

ПРАКТИКА

ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ

СЪДЪРЖАНИЕ

1	ВЪВЕДЕНИЕ.....	9
1.1	ПРЕГЛЕД.....	9
1.2	ИЗИСКВАНИЯ КЪМ ПРАКТИКАТА.....	11
1.3	НОРМАТИВНИ ПОЗОВАВАНИЯ	13
1.4	ИМЕ И ИДЕНТИФИКАЦИЯ НА ДОКУМЕНТА	15
1.5	УЧАСТНИЦИ В ИНФРАСТРУКТУРАТА НА ЕВРОТРЪСТ	20
1.5.1	УДОСТОВЕРЯВАЩИ ОРГАНИ	21
1.5.2	РЕГИСТРИРАЩ ОРГАН	28
1.5.3	ПОТРЕБИТЕЛИ	29
1.5.4	ДОВЕРЯВАЩИ СЕ СТРАНИ	30
1.5.5	ДРУГИ УЧАСТНИЦИ.....	31
1.6	УПОТРЕБА И ПРИЛОЖИМОСТ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ.....	31
1.7	УПРАВЛЕНИЕ НА ПРАКТИКАТА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНА УДОСТОВЕРИТЕЛНА УСЛУГА.....	32
2	ОТГОВОРНОСТ ЗА ПУБЛИКУВАНЕ И ХРАНИЛИЩЕ	32
2.1	ХРАНИЛИЩЕ.....	32
2.2	ИНФОРМАЦИЯ, ПУБЛИКУВАНА ОТ ЕВРОТРЪСТ	34
2.3	ЧЕСТОТА НА ПУБЛИКУВАНЕ	35
2.4	ДОСТЪП ДО ПУБЛИКАЦИИ	35
3	ИДЕНТИФИКАЦИЯ И УДОСТОВЕРЯВАНЕ НА САМОЛИЧНОСТ/ ИДЕНТИЧНОСТ	36
3.1	ИМЕНА	37
3.1.1	ВИДОВЕ ИМЕНА.....	38
3.1.2	НЕОБХОДИМОСТ ОТ СМИСЛЕНИ ИМЕНА	38
3.1.3	АНОНИМНОСТ НА ПОТРЕБИТЕЛИТЕ	39
3.1.4	ПРАВИЛА ЗА ТЪЛКУВАНЕ НА РАЗЛИЧНИ ФОРМИ НА ИМЕНА	39
3.1.5	УНИКАЛНОСТ НА ИМЕНАТА.....	39
3.1.6	ПОВЕРКА НА ИМЕНА И СПОРОВЕ ПО ПОВОД НА ТЯХ.....	40
3.2	ПЪРВОНАЧАЛНА РЕГИСТРАЦИЯ	40
3.2.1	ПРОВЕРКА ЗА ПРИТЕЖАНИЕ НА ЧАСТЕН КЛЮЧ	42
3.2.2	УСТАНОВЯВАНЕ НА ИДЕНТИЧНОСТ НА ЮРИДИЧЕСКО ЛИЦЕ	42
3.2.3	УСТАНОВЯВАНЕ НА САМОЛИЧНОСТ НА ФИЗИЧЕСКО ЛИЦЕ.....	44
3.2.4	УСТАНОВЯВАНЕ НА САМОЛИЧНОСТ НА ФИЗИЧЕСКО ЛИЦЕ, УПЪЛНОМОЩЕН ПРЕДСТАВИТЕЛ НА ЮРИДИЧЕСКО ЛИЦЕ	45
3.2.5	ОСОБЕНИ АТРИБУТИ.....	45
3.2.6	НЕПОТВЪРДЕНА ИНФОРМАЦИЯ.....	46
3.2.7	ДЕЙСТВИЯ НА УДОСТОВЕРЯВАЩИЯ ОРГАН	46
3.2.8	ПРОВЕРКА НА ПРИТЕЖАНИЕ НА ДОМЕЙН	46
3.2.9	КРИТЕРИИ ЗА СЪОТВЕТСТВИЕ.....	47
3.3	ИДЕНТИФИКАЦИЯ И ПРОВЕРКА ЗА САМОЛИЧНОСТ/ИДЕНТИЧНОСТ ПРИ ПОДНОВЯВАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ.....	47
3.4	ИДЕНТИФИКАЦИЯ И ПРОВЕРКА НА САМОЛИЧНОСТ/ИДЕНТИЧНОСТ ПРИ СПИРАНЕ НА ДЕЙСТВИЕТО НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ	49
3.5	ИДЕНТИФИКАЦИЯ И ПРОВЕРКА НА САМОЛИЧНОСТ/ИДЕНТИЧНОСТ ПРИ ПРЕКРАТЯВАНЕ НА ДЕЙСТВИЕТО НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ.....	49
3.6	ИДЕНТИФИКАЦИЯ И ПРОВЕРКА ЗА САМОЛИЧНОСТ/ИДЕНТИЧНОСТ СЛЕД ПРЕКРАТЯВАНЕ ДЕЙСТВИЕТО НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ	50
4	ОПЕРАТИВНИ ИЗИСКВАНИЯ	50

4.1	ПОДАВАНЕ НА ИСКАНЕ ЗА ИЗДАВАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ	51
4.1.1	ЛИЦА, ПОДАВАЩИ ИСКАНЕ ЗА ИЗДАВАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ	51
4.1.2	ОБРАБОТКА НА ИСКАНЕТО ЗА ИЗДАВАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ	52
4.2	ОБРАБОТКА НА ИСКАНЕТО	58
4.2.1	ИДЕНТИФИКАЦИЯ И ПРОВЕРКА ЗА САМОЛИЧНОСТ	59
4.2.2	ПРИЕМАНЕ ИЛИ ОТХВЪРЛЯНЕ НА ИСКАНЕ	59
4.2.3	ИЗЧАКВАНЕ ИЗДАВАНЕТО НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ	60
4.3	ИЗДАВАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ	61
4.3.1	ОБРАБОТКА	61
4.3.2	ПРЕДОСТАВЯНЕ НА ИНФОРМАЦИЯ	62
4.4	ПРИЕМАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ	62
4.4.1	ПОТВЪРЖДЕНИЕ ЗА ПРИЕМАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ	62
4.4.2	ПУБЛИКУВАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ	63
4.4.3	ИНФОРМАЦИЯ ЗА ДРУГИ СТРАНИ	63
4.5	УПОТРЕБА НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ И НА ДВОЙКАТА КЛЮЧОВЕ	63
4.5.1	ОТ СТРАНА НА ТИТУЛЯРИТЕ/СЪЗДАТЕЛИТЕ	63
4.5.2	ОТ ДОВЕРЯВАЩИТЕ СЕ СТРАНИ	64
4.6	ПОДНОВЯВАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ	64
4.7	ИЗДАВАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ С ГЕНЕРИРАНЕ НА НОВА ДВОЙКА КЛЮЧОВЕ	64
4.7.1	ОБСТОЯТЕЛСТВА, ПРИ КОИТО СЕ ПРИЛАГА ИЗДАВАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ С ГЕНЕРИРАНЕ НА НОВА ДВОЙКА КЛЮЧОВЕ	65
4.7.2	КОЙ МОЖЕ ДА ПОИСКА АКТУАЛИЗАЦИЯ НА КЛЮЧОВА ДВОЙКА	65
4.7.3	АКТУАЛИЗАЦИЯ НА КЛЮЧОВА ДВОЙКА И ОБРАБОТКА НА ИСКАНЕТО	66
4.7.4	ИНФОРМАЦИЯ ЗА ТИТУЛЯРЯ/СЪЗДАТЕЛЯ	66
4.7.5	ПОТВЪРЖДЕНИЕ ЗА ПРИЕМАНЕ НА НОВО УДОСТОВЕРЕНИЕ	67
4.7.6	ПУБЛИКУВАНЕ НА НОВО КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ	67
4.7.7	ИНФОРМАЦИЯ ЗА ДОВЕРЯВАЩИ СЕ СТРАНИ	67
4.8	ПРОМЯНА В КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ	67
4.8.1	ОБСТОЯТЕЛСТВА ЗА ПРОМЯНА В КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ	67
4.8.2	КОЙ МОЖЕ ДА ПОИСКА ПРОМЯНА НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ	68
4.8.3	ОБРАБОТКА НА ИСКАНЕТО	68
4.8.4	ИНФОРМАЦИЯ ЗА ПОТРЕБИТЕЛЯ	69
4.8.5	ПОТВЪРЖДЕНИЕ ЗА ПРИЕМАНЕ НА НОВО КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ	69
4.8.6	ПУБЛИКУВАНЕ НА НОВО КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ	70
4.8.7	ИНФОРМАЦИЯ ЗА ДОВЕРЯВАЩИТЕ СЕ СТРАНИ	70
4.9	СПИРАНЕ И ПРЕКРАТЯВАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ	70
4.9.1	ОСНОВАНИЯ ЗА ПРЕКРАТЯВАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ	71
4.9.2	ОСНОВАНИЯ ЗА ПРЕКРАТЯВАНЕ НА УДОСТОВЕРЕНИЕ НА УДОСТОВЕРЯВАЩ ОРГАН	73
4.9.3	ЛИЦА, ЛЕГИТИМИРАНИ ДА ПОИСКАТ ПРЕКРАТЯВАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ	73
4.9.4	ПРОЦЕДУРА ЗА ПРЕКРАТЯВАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ	74
4.9.5	ГРАТИСЕН ПЕРИОД НА ПРЕКРАТЯВАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ	76
4.9.6	СРОК ЗА ОБРАБОТКА НА ИСКАНЕТО ЗА ПРЕКРАТЯВАНЕ	77
4.9.7	ПРОВЕРКА НА СПИСЪКА СЪС СПРЕНИ И ПРЕКРАТЕНИ УДОСТОВЕРЕНИЯ (CRL)	77
4.9.8	ЧЕСТОТА НА ИЗДАВАНЕ НА СПИСЪКА СЪС СПРЕНИ И ПРЕКРАТЕНИ УДОСТОВЕРЕНИЯ (CRL)	78
4.9.9	МАКСИМАЛНО ЗАБАВЯНЕ НА ПУБЛИКУВАНЕТО НА CRL	78
4.9.10	ОНЛАЙН ПРОВЕРКА НА СЪСТОЯНИЕТО НА УДОСТОВЕРЕНИЕ	78
4.9.11	ИЗИСКВАНИЯ ЗА ОНЛАЙН ПРОВЕРКА НА СЪСТОЯНИЕТО НА УДОСТОВЕРЕНИЕ	79

4.9.12 СПЕЦИАЛНИ ИЗИСКВАНИЯ ПО ОТНОШЕНИЕ НА НАРУШЕНИЕ НА СИГУРНОСТТА НА КЛЮЧА	79
4.9.13 ОСНОВАНИЯ ЗА СПИРАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ	79
4.9.14 ЛИЦА, ЛЕГИТИМИРАНИ ДА ПОИСКАТ СПИРАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ	80
4.9.15 ПРОЦЕДУРА ЗА СПИРАНЕ И ВЪЗОБНОВЯВАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ	80
4.9.16 ГРАТИСЕН ПЕРИОД НА СПИРАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ	81
4.9.17 ВЪЗОБНОВЯВАНЕ ДЕЙСТВИЕТО НА СПРЯНО УДОСТОВЕРЕНИЕ	81
4.9.18 ПРОЦЕДУРА ЗА ВЪЗОБНОВЯВАНЕ НА ДЕЙСТВИЕТО НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ	81
4.10 ПРОВЕРКА НА АКТУАЛНОТО СЪСТОЯНИЕ (СТАТУСА) НА КВАЛИФИЦИРАНИТЕ УДОСТОВЕРЕНИЯ	82
4.10.1 ХАРАКТЕРИСТИКИ	82
4.10.2 ДОПЪЛНИТЕЛНИ ФУНКЦИИ	82
4.11 ПРЕКРАТЯВАНЕ НА ДОГОВОР ЗА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ ОТ ПОТРЕБИТЕЛ	83
4.12 ДОВЕРИТЕЛНО СЪХРАНЕНИЕ НА ЧАСТЕН КЛЮЧ (ЕСКРОУ)	83
5 КОНТРОЛ НА ФИЗИЧЕСКАТА И ОРГАНИЗАЦИОННА СИГУРНОСТ	84
5.1 КОНТРОЛ НА ФИЗИЧЕСКАТА СИГУРНОСТ	84
5.1.1 ПОМЕЩЕНИЯ И КОНСТРУКЦИЯ НА ПОМЕЩЕНИЯТА	86
5.1.2 ФИЗИЧЕСКИЯТ ДОСТЪП	86
5.1.3 КОНТРОЛ ДА ДОСТЪП	87
5.1.4 ЕЛЕКТРИЧЕСКО ЗАХРАНВАНЕ И КЛИМАТИЧНИ УСЛОВИЯ	88
5.1.5 НАВОДНЕНИЕ	89
5.1.6 ПРЕДОТВРАТЯВАНЕ НА ПОЖАР И ЗАЩИТА ОТ ПОЖАР	89
5.1.7 РАБОТА С НОСИТЕЛИ	89
5.1.8 ИЗХВЪРЛЯНЕ НА ОТПАДЪЦИТЕ	90
5.1.9 СРОК НА УПОТРЕБА НА ТЕХНИЧЕСКИ КОМПОНЕНТИ	90
5.2 ОРГАНИЗАЦИОНЕН КОНТРОЛ	90
5.2.1 ДОВЕРЕНИ РОЛИ	93
5.2.2 ИЗИСКВАНИЯ ЗА РАЗДЕЛЯНЕ НА ОТГОВОРНОСТИТЕ	94
5.2.3 ИДЕНТИФИКАЦИЯ И ПРОВЕРКА ЗА САМОЛИЧНОСТ ЗА ВСЯКА РОЛЯ	95
5.3 КОНТРОЛ НА ПЕРСОНАЛА	95
5.3.1 КВАЛИФИКАЦИЯ НА ПЕРСОНАЛА	96
5.3.2 ПРОЦЕДУРИ ЗА ПРОВЕРКА НА ПЕРСОНАЛА	96
5.3.3 ИЗИСКВАНИЯ ЗА ОБУЧЕНИЕ НА ПЕРСОНАЛА НА ЕВРОТРЪСТ	97
5.3.4 ЧЕСТОТА НА ОБУЧЕНИЯТА И ИЗИСКВАНИЯ ЗА НАДГРАЖДАНЕ НА КВАЛИФИКАЦИЯТА НА СЛУЖИТЕЛИТЕ	98
5.3.5 СМЯНА НА РАБОТАТА	98
5.3.6 САНКЦИИ ЗА ИЗВЪРШВАНЕ НА НЕРАЗРЕШЕНИ ДЕЙСТВИЯ	98
5.3.7 ДОГОВОР С ПЕРСОНАЛА	98
5.3.8 ДОКУМЕНТАЦИЯ, ПРЕДОСТАВЕНА НА ПЕРСОНАЛА	98
5.4 ЗАПИСИ НА СЪБИТИЯ И ПОДДЪРЖАНЕ НА ЖУРНАЛИ	99
5.4.1 ВИДОВЕ ЗАПИСИ	99
5.4.2 СЪБИРАНЕ НА ДОКАЗАТЕЛСТВА	101
5.4.3 ЧЕСТОТА НА СЪЗДАВАНЕ НА ЗАПИСИ	102
5.4.4 ПЕРИОД НА СЪХРАНЕНИЕ НА ЗАПИСИ	102
5.4.5 ЗАЩИТА НА АРХИВА	102
5.4.6 ПОДДЪРЖАНЕ НА РЕЗЕРВНИ КОПИЯ НА ЗАПИСИ НА СЪБИТИЯ	103
5.4.7 СИСТЕМА ЗА УВЕДОМЯВАНЕ СЛЕД АНАЛИЗ НА ЗАПИСИ	103
5.4.8 УЯЗВИМОСТ И ОЦЕНКА НА РИСКА	104

5.5	АРХИВИРАНЕ.....	105
5.5.1	ВИДОВЕ АРХИВИ	105
5.5.2	ПЕРИОД НА СЪХРАНЕНИЕ НА АРХИВА	105
5.5.3	ЗАЩИТА НА АРХИВНА ИНФОРМАЦИЯ.....	105
5.5.4	ВЪЗСТАНОВЯВАНЕ НА АРХИВИРАНА ИНФОРМАЦИЯ.....	106
5.5.5	ИЗИСКВАНИЯ ЗА ОТБЕЛЯЗВАНЕ НА ВРЕМЕТО НА АРХИВИРАНЕ	106
5.5.6	СЪХРАНЯВАНЕ НА АРХИВА	106
5.5.7	ПРОЦЕДУРИ ЗА ДОСТЪП И ПРОВЕРКА НА АРХИВИРАНАТА ИНФОРМАЦИЯ	106
5.6	УПРАВЛЕНИЕ НА АКТИВИ	107
5.7	ПРОМЯНА НА КЛЮЧ НА ДОСТАВЧИКА.....	107
5.8	КОМПРОМЕТИРАНЕ НА КЛЮЧОВЕ И ВЪЗСТАНОВЯВАНЕ СЛЕД АВАРИИ	108
5.8.1	ДЕЙСТВИЯ ПРИ АВАРИИ.....	108
5.8.2	ИНЦИДЕНТИ, СВЪРЗАНИ СЪС СРИВОВЕ В ХАРДУЕРА, СОФТУЕРА И/ИЛИ ДАННИТЕ.....	109
5.8.3	КОМПРОМЕТИРАНЕ ИЛИ СЪМНЕНИЕ ЗА КОМПРОМЕТИРАНЕ НА ЧАСТЕН КЛЮЧ НА УДОСТОВЕРЯВАЩИЯ ОРГАН НА ЕВРОТРЪСТ	110
5.8.4	НЕПРЕКЪСНАТОСТ НА БИЗНЕСА И ВЪЗСТАНОВЯВАНЕ СЛЕД АВАРИИ	111
5.9	ПРЕКРАТЯВАНЕ НА ДЕЙНОСТТА НА ЕВРОТРЪСТ	113
5.9.1	ПЛАН ЗА ПРЕКРАТЯВАНЕ НА ДЕЙНОСТТА	113
5.9.2	ИЗИСКВАНИЯ, СВЪРЗАНИ С ПРЕХОДА ДО ПРЕКРАТЯВАНЕ НА ДЕЙНОСТТА НА ДОСТАВЧИКА	114
5.9.3	ПРЕКРАТЯВАНЕ НА ДЕЙНОСТТА НА УДОСТОВЕРЯВАЩ ОРГАН	115
5.9.4	ПРЕХВЪРЛЯНЕ НА ДЕЙНОСТ КЪМ ДРУГ ДОСТАВЧИК НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ.....	116
5.9.5	ОТНЕМАНЕ НА КВАЛИФИЦИРАН СТАТУТ НА ЕВРОТРЪСТ ИЛИ НА КВАЛИФИЦИРАНИЯ СТАТУТ НА СЪОТВЕТНА УСЛУГА	116
6	УПРАВЛЕНИЕ И КОНТРОЛ НА ТЕХНИЧЕСКАТА СИГУРНОСТ	117
6.1	ГЕНЕРИРАНЕ И ИНСТАЛИРАНЕ НА ДВОЙКА КЛЮЧОВЕ	118
6.1.1	ГЕНЕРИРАНЕ НА ДВОЙКА КЛЮЧОВЕ НА УДОСТОВЕРЯВАЩ ОРГАН.....	119
6.1.2	ГЕНЕРИРАНЕ НА ДВОЙКА КЛЮЧОВЕ НА ТИТУЛЯР/СЪЗДАТЕЛ.....	121
6.1.3	ДОСТАВКА НА ЧАСТЕН КЛЮЧ НА ПОТРЕБИТЕЛЯ	122
6.1.4	ДОСТАВКА НА ПУБЛИЧЕН КЛЮЧ ОТ ПОТРЕБИТЕЛ НА ДОСТАВЧИК	123
6.1.5	ДОСТАВКА НА ПУБЛИЧЕН КЛЮЧ НА ДОСТАВЧИКА НА ДОВЕРЯВАЩИТЕ СЕ СТРАНИ.....	124
6.1.6	ДЪЛЖИНА НА КЛЮЧОВЕ.....	124
6.1.7	КРИПТОГРАФСКИ АЛГОРИТМИ.....	126
6.1.8	ПАРАМЕТРИ НА ПУБЛИЧЕН КЛЮЧ	127
6.1.9	ИЗПОЛЗВАНЕ НА КЛЮЧА.....	127
6.2	ЗАЩИТА НА ЧАСТЕН КЛЮЧ И КОНТРОЛ НА КРИПТОГРАФСКИЯ МОДУЛ.....	128
6.2.1	СТАНДАРТИ ЗА КРИПТОГРАФСКИ МОДУЛИ.....	129
6.2.2	КОНТРОЛ НА ИЗПОЛЗВАНЕ И СЪХРАНЕНИЕ НА ЧАСТЕН КЛЮЧ	129
6.2.3	ДОВЕРИТЕЛНО СЪХРАНЯВАНЕ НА ЧАСТЕН КЛЮЧ (ЕСКРОУ).....	130
6.2.4	СЪХРАНЯВАНЕ НА ЧАСТЕН КЛЮЧ	130
6.2.5	АРХИВИРАНЕ НА ЧАСТНИЯ КЛЮЧ	131
6.2.6	ТРАНСФЕР НА ЧАСТЕН КЛЮЧ В КРИПТОГРАФСКИ МОДУЛ	132
6.2.7	СЪХРАНЯВАНЕ НА ЧАСТЕН КЛЮЧ В КРИПТОГРАФСКИЯ МОДУЛ	132
6.2.8	МЕТОД ЗА АКТИВИРАНЕ НА ЧАСТЕН КЛЮЧ.....	132
6.2.9	МЕТОД ЗА ДЕАКТИВИРАНЕ НА ЧАСТЕН КЛЮЧ.....	133
6.2.10	МЕТОД ЗА УНИЩОЖАВАНЕ НА ЧАСТЕН КЛЮЧ.....	133
6.2.11	ОЦЕНКА НА КРИПТОГРАФСКИЯ МОДУЛ	133
6.3	ДРУГИ АСПЕКТИ НА УПРАВЛЕНИЕТО НА ДВОЙКАТА КЛЮЧОВЕ	133
6.3.1	АРХИВИРАНЕ НА ПУБЛИЧЕН КЛЮЧ	134

6.3.2	ПЕРИОД НА ВАЛИДНОСТ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ И УПОТРЕБА НА КЛЮЧОВЕ	134
6.4	ДАННИ ЗА АКТИВИРАНЕ	135
6.4.1	ГЕНЕРИРАНЕ И ИНСТАЛИРАНЕ НА ДАННИ ЗА АКТИВИРАНЕ	136
6.4.2	ЗАЩИТА НА ДАННИ ЗА АКТИВИРАНЕ	137
6.4.3	ДРУГИ АСПЕКТИ НА ДАННИТЕ ЗА АКТИВИРАНЕ	137
6.5	СИГУРНОСТ НА КОМПЮТЪРНИТЕ СИСТЕМИ	137
6.5.1	СТЕПЕН НА КОМПЮТЪРНА СИГУРНОСТ	138
6.5.2	УПРАВЛЕНИЕ НА ИНЦИДЕНТИ И МОНИТОРИНГ	139
6.5.3	ПОЛИТИКАТА ЗА ИНФОРМАЦИОННА СИГУРНОСТ	140
6.6	СИГУРНОСТ НА ЖИЗНЕНИЯ ЦИКЪЛ НА ТЕХНОЛОГИЧНАТА СИСТЕМА.....	143
6.6.1	КОНТРОЛИ ЗА РАЗВИТИЕ НА ТЕХНОЛОГИЧНАТА СИСТЕМА	143
6.6.2	КОНТРОЛИ ЗА УПРАВЛЕНИЕ НА СИГУРНОСТТА НА ТЕХНОЛОГИЧНАТА СИСТЕМА	143
6.6.3	КРИПТОГРАФСКИ КОНТРОЛИ	144
6.6.4	ОЦЕНКА НА ЖИЗНЕНИЯ ЦИКЪЛ НА СИГУРНОСТТА НА ТЕХНОЛОГИЧНАТА СИСТЕМА.....	145
6.7	МРЕЖОВА СИГУРНОСТ	145
7	ПРОФИЛИ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ, CRL И НА OCSP	147
7.1	ПРОФИЛ НА БАЗОВ УДОСТОВЕРЯВАЩ ОРГАН „EVROTRUST RSA ROOT“	147
7.2	ПРОФИЛ НА УДОСТОВЕРЯВАЩИ ОРГАНИ ЗА ПРОВЕРКА НА СТАТУС	148
7.2.1	ПРОФИЛ НА УДОСТОВЕРЯВАЩ ОРГАН „EVROTRUST RSA VALIDATION“	151
7.2.2	ПРОФИЛ НА УДОСТОВЕРЯВАЩ ОРГАН „EVROTRUST RSA QS VALIDATION“	152
7.2.3	ПРОФИЛ НА УДОСТОВЕРЯВАЩ ОРГАН „EVROTRUST SERVICES VALIDATION“	153
7.2.4	ПРОФИЛ НА УДОСТОВЕРЯВАЩ ОРГАН „EVROTRUST RSA QOPERATIONAL CA 2024 OCSP“ ...	155
7.3	ПРОФИЛ НА ОПЕРАТИВЕН УДОСТОВЕРЯВАЩ ОРГАН „EVROTRUST RSA OPERATIONAL CA“	156
7.4	ПРОФИЛ НА ОПЕРАТИВЕН УДОСТОВЕРЯВАЩ ОРГАН „EVROTRUST SERVICES CA“ ..	158
7.5	ПРОФИЛИ НА CRL-И	160
7.5.1	CRL ПРОФИЛ НА БАЗОВИЯ УДОСТОВЕРЯВАЩ ОРГАН „EVROTRUST RSA ROOT CA“	161
7.5.2	CRL ПРОФИЛ НА ОПЕРАТИВНИЯ УДОСТОВЕРЯВАЩ ОРГАН „EVROTRUST RSA OPERATIONAL CA“	162
7.5.3	CRL ПРОФИЛ НА ОПЕРАТИВНИЯ УДОСТОВЕРЯВАЩ ОРГАН „EVROTRUST SERVICES CA“	162
7.5.4	CRL ПРОФИЛ НА ОПЕРАТИВНИЯ УДОСТОВЕРЯВАЩ ОРГАН „EVROTRUST RSA QOPERATIONAL CA 2024“	163
7.5.5	CRL ПРОФИЛ НА ОПЕРАТИВНИЯ УДОСТОВЕРЯВАЩ ОРГАН „EVROTRUST RSA REG.KE OPERATIONAL CA 2025“	163
7.6	ПРОФИЛИ НА ПОТРЕБИТЕЛСКИ УДОСТОВЕРЕНИЯ	164
7.6.1	ПРОФИЛ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ ЗА КВАЛИФИЦИРАН ЕЛЕКТРОНЕН ПОДПИС НА ФИЗИЧЕСКО ЛИЦЕ „EVROTRUST QUALIFIED NATURAL PERSON CERTIFICATE FOR QES“	170
7.6.2	ПРОФИЛ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ ЗА УСЪВЪРШЕНСТВАН ЕЛЕКТРОНЕН ПОДПИС НА ФИЗИЧЕСКО ЛИЦЕ „EVROTRUST QUALIFIED NATURAL PERSON CERTIFICATE FOR AES“	177
7.6.3	ПРОФИЛ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ ЗА КВАЛИФИЦИРАН ЕЛЕКТРОНЕН ПЕЧАТ НА ЮРИДИЧЕСКО ЛИЦЕ „EVROTRUST QUALIFIED LEGAL PERSON CERTIFICATE FOR QESEAL“	185
7.6.4	ПРОФИЛ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ ЗА УСЪВЪРШЕНСТВАН ЕЛЕКТРОНЕН ПЕЧАТ НА ЮРИДИЧЕСКО ЛИЦЕ „EVROTRUST QUALIFIED LEGAL PERSON CERTIFICATE FOR AESEAL“	191
7.6.5	ПРОФИЛ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ ПО PSD2 ЗА УСЪВЪРШЕНСТВАН ЕЛЕКТРОНЕН ПЕЧАТ НА ЮРИДИЧЕСКО ЛИЦЕ „EVROTRUST QUALIFIED PSD2 LEGAL PERSON	

CERTIFICATE FOR AESEAL"	196
7.6.6 ПРОФИЛ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ ЗА АВТЕНТИЧНОСТ НА УЕБСАЙТ ЗА ОРГАНЗИАЦИЯ „EVROTRUST SSL ORGANIZATION VALIDATED CERTIFICATE"	202
7.6.7 ПРОФИЛ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ ЗА АВТЕНТИЧНОСТ НА УЕБСАЙТ С РАЗШИРЕНО ВАЛИДИРАНЕ „EVROTRUST SSL EV CERTIFICATE"	207
7.6.8 ПРОФИЛ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ ЗА АВТЕНТИЧНОСТ НА PSD2 УЕБСАЙТ „EVROTRUST SSL PSD2 CERTIFICATE"	213
7.6.9 ПРОФИЛ НА КВАЛИФИЦИРАНО АТРИБУТИВНО УДОСТОВЕРЕНИЕ ЗА КВАЛИФИЦИРАН ЕЛЕКТРОНЕН ПОДПИС НА ФИЗИЧЕСКО ЛИЦЕ „EVROTRUST QUALIFIED NATURAL PERSON ATTRIBUTE CERTIFICATE FOR QES"	219
7.6.10 ПРОФИЛ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ ЗА АВТЕНТИЧНОСТ НА УЕБСАЙТ ЗА ДОМЕЙН „EVROTRUST SSL DOMAIN VALIDATED CERTIFICATE"	230
7.6.11 ПРОФИЛ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ ЗА КВАЛИФИЦИРАН ЕЛЕКТРОНЕН ПОДПИС НА ФИЗИЧЕСКО ЛИЦЕ „EVROTRUST REG.KE QUALIFIED NATURAL PERSON CERTIFICATE FOR QES"	233
7.6.12 ПРОФИЛ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ ЗА УСЪВЪРШЕНСТВАН ЕЛЕКТРОНЕН ПОДПИС НА ФИЗИЧЕСКО ЛИЦЕ „EVROTRUST REG.KE QUALIFIED NATURAL PERSON CERTIFICATE FOR AES"	237
7.6.13 ПРОФИЛ НА КВАЛИФИЦИРАНО АТРИБУТИВНО УДОСТОВЕРЕНИЕ ЗА КВАЛИФИЦИРАН ЕЛЕКТРОНЕН ПОДПИС НА ФИЗИЧЕСКО ЛИЦЕ „EVROTRUST REG.KE QUALIFIED NATURAL PERSON ATTRIBUTE CERTIFICATE FOR QES"	241
7.7 ПРОФИЛ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ НА ПОДПИСВАЩ МОДУЛ ЗА ВРЕМЕ „TIMESTAMP SIGNING UNIT"	246
7.8 ПРОФИЛ НА ОПЕРАТИВЕН УДОСТОВЕРЯВАЩ ОРГАН „EVROTRUST RSA OPERATIONAL CA 2024"	248
7.9 ПРОФИЛ НА ОПЕРАТИВЕН УДОСТОВЕРЯВАЩ ОРГАН „EVROTRUST RSA REG.KE OPERATIONAL CA 2025"	250
8 ОДИТ	252
8.1 ЧЕСТОТА НА ОДИТА	253
8.2 КВАЛИФИКАЦИЯ НА ПРОВЕРЯВАЩИТЕ ЛИЦА	253
8.3 ОТНОШЕНИЯ НА ПРОВЕРЯВАЩИТЕ ЛИЦА С ЕВРОТРЪСТ	253
8.4 ОБХВАТ НА ОДИТА	254
8.5 ДЕЙСТВИЯ, ПРЕДПРИЕТИ В РЕЗУЛТАТ НА ИЗВЪРШЕНИЯ ОДИТ	254
8.6 СЪХРАНЕНИЕ НА РЕЗУЛТАТИТЕ ОТ ОДИТИТЕ	254
9 ДРУГИ БИЗНЕС И ПРАВНИ ВЪПРОСИ	255
9.1 ЦЕНИ И ТАКСИ	255
9.1.1 ВЪЗНАГРАЖДЕНИЯ	255
9.1.2 ВЪЗНАГРАЖДЕНИЯ ЗА УДОСТОВЕРИТЕЛНИ, КРИПТОГРАФСКИ, ИНФОРМАЦИОННИ И КОНСУЛТАНТСКИ УСЛУГИ	256
9.1.3 ФАКТУРИРАНЕ	257
9.1.4 ВРЪЩАНЕ НА УДОСТОВЕРЕНИЕ И ВЪЗСТАНОВЯВАНЕ НА ПЛАЩАНЕ	257
9.1.5 БЕЗПЛАТНИ УСЛУГИ	258
9.2 ФИНАНСОВИ ОТГОВОРНОСТИ	258
9.2.1 ЗАСТРАХОВКА НА ДЕЙНОСТТА	258
9.2.2 ЗАСТРАХОВАТЕЛНО ПОКРИТИЕ	259
9.3 КОНФИДЕНЦИАЛНОСТ НА БИЗНЕС ИНФОРМАЦИЯ	259
9.3.1 ОБХВАТ НА КОНФИДЕНЦИАЛНАТА ИНФОРМАЦИЯ	260
9.3.2 НЕКОНФИДЕНЦИАЛНА ИНФОРМАЦИЯ	260
9.3.3 ЗАЩИТА НА КОНФИДЕНЦИАЛНАТА ИНФОРМАЦИЯ	261

9.4	НЕПРИКОСНОВЕНОСТ НА ЛИЧНИТЕ ДАННИ	261
9.4.1	ДЕКЛАРАЦИЯ ЗА ПОВЕРИТЕЛНОСТ	262
9.4.2	ИНФОРМАЦИЯ ТРЕТИРАНА КАТО ЛИЧНА.....	262
9.4.3	ИНФОРМАЦИЯ, КОЯТО НЕ СЕ СЧИТА ЗА ЛИЧНА	262
9.4.4	ОТГОВОРНОСТ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ	262
9.4.5	СЪГЛАСИЕ ЗА ИЗПОЛЗВАНЕ НА ЛИЧНИ ДАННИ.....	263
9.4.6	ДРУГИ ОБСТОЯТЕЛСТВА ЗА РАЗКРИВАНЕ НА ИНФОРМАЦИЯ	263
9.5	ПРАВА ВЪРХУ ИНТЕЛЕКТУАЛНА СОБСТВЕНОСТ	263
9.5.1	ПРАВО НА СОБСТВЕНОСТ НА ДАННИ В КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ	264
9.5.2	ПРАВО НА СОБСТВЕНОСТ НА ИМЕНА И ТЪРГОВСКИ МАРКИ	264
9.5.3	ПРАВО НА СОБСТВЕНОСТ НА ДВОЙКА КЛЮЧОВЕ	264
9.6	ОБЩИ ПОЛОЖЕНИЯ	264
9.6.1	ЗАДЪЛЖЕНИЯ, ОТГОВОРНОСТ И ГАРАНЦИИ НА ЕВРОТРЪСТ	265
9.6.2	ЗАДЪЛЖЕНИЯ, ОТГОВОРНОСТ И ГАРАНЦИИ НА РЕГИСТРИРАЩИЯ ОРГАН	269
9.6.3	ЗАДЪЛЖЕНИЯ НА ПОТРЕБИТЕЛИТЕ	270
9.6.4	ДЪЛЖИМА ГРИЖА НА ДОВЕРЯВАЩА СЕ СТРАНА.....	272
9.6.5	ЗАДЪЛЖЕНИЯ НА ДРУГИ СТРАНИ.....	273
9.7	ОСВОБОЖДАВАНЕ ОТ ОТГОВОРНОСТ	276
9.8	ОГРАНИЧЕНИЯ НА ОТГОВОРНОСТТА	278
9.9	ОТГОВОРНОСТ НА ТИТУЛЯРЯ/СЪЗДАТЕЛЯ	278
9.9.1	ОТГОВОРНОСТ НА ТИТУЛЯРЯ/СЪЗДАТЕЛЯ КЪМ ЕВРОТРЪСТ	278
9.10	СРОК И ПРЕКРАТЯВАНЕ НА „ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ“	278
9.10.1	СРОКОВЕ	278
9.10.2	ПРЕКРАТЯВАНЕ	279
9.10.3	ЕФЕКТ НА ПРЕКРАТЯВАНЕ И ОЦЕЛЯВАНЕ.....	279
9.11	БЕЛЕЖКИ И СЪОБЩЕНИЯ МЕЖДУ СТРАНИТЕ	279
9.12	ИЗМЕНЕНИЯ В „ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ“	279
9.13	РЕШАВАНЕ НА СПОРОВЕ	280
9.14	ПРИЛОЖИМО ПРАВО	281
9.15	СЪОТВЕТСТВИЕ С ПРИЛОЖИМОТО ПРАВО	281
9.16	ДРУГИ РАЗПОРЕДБИ	282
10	ИЗПОЛЗВАНИ ТЕРМИНИ И СЪКРАЩЕНИЯ	282
10.1	ПРИЛОЖЕНИЕ 1: ТЕРМИНИ И СЪКРАЩЕНИЯ НА БЪЛГАРСКИ ЕЗИК.....	282
10.2	ПРИЛОЖЕНИЕ 2: ТЕРМИНИ И СЪКРАЩЕНИЯ НА АНГЛИЙСКИ ЕЗИК	289

1 ВЪВЕДЕНИЕ

„Евротръст Технолъджис“ АД (Евротръст) е юридическо лице, регистрирано в Търговския регистър към Агенцията по вписванията с ЕИК 203397356 със седалище и адрес на управление: 1766 София, ул. Околовръстен път 251Г, ММ Бизнес център. Телефон за контакт: +359 2 4485858. Интернет адрес: <http://www.evrotrust.com>.

Дружеството осъществява публични функции по смисъла на Закона за електронния документ и електронни удостоверителни услуги (ЗЕДЕУУ).

Евротръст е доставчик на квалифицирани удостоверителни услуги. Той предоставя на потребители срещу възнаграждение квалифицирани удостоверителни услуги и продукти с висока степен на сигурност. Доставчикът предоставя своите услуги, както на територията на Република България, така и в държавите-членки на Европейския съюз и останалите страни по света.

Иновативен в своята дейност, Евротръст предоставя на своите потребители създаването на електронни подписи/печати от разстояние. В този икономически изгоден метод на работа средата на създаване на електронен подпис/печат се управлява от доставчика от името на Титуляря/Създателя на електронния подпис/печат. Евротръст гарантира, че прилага стандартизирани процедури за сигурност на управление и използва надеждни системи и продукти, включително сигурни електронни канали на комуникация, с цел да се гарантира надеждността на средата на създаване на електронния подпис/печат и да се гарантира, че тази среда е използвана единствено под контрола на Титуляря/Създателя на електронния подпис/печат.

1.1 ПРЕГЛЕД

„Практика при предоставяне на квалифицирани удостоверителни услуги“ (Практиката/Certification Practice Statement/CPS) на Евротръст е публичен документ. Той може да бъде променян по всяко време от Евротръст и всяка нова редакция се съобщава на заинтересованите лица, като актуализираният документ се публикува на интернет страницата на Евротръст.

Практиката на Евротръст описва общите изисквания при предоставяне на квалифицирани удостоверителни услуги. Документът съдържа правила и процедури, които трябва да се изпълняват при издаване и управление (спиране, прекратяване и възобновяване)

действието на квалифицирани удостоверения за електронни подписи/печати, квалифицирани електронни времеви печати и квалифицирани удостоверения за уебсайт. В хода на обслужване на заявките се събират необходими документи при приемане и проверка на заявление за издаване на квалифицирани удостоверения. В Практиката се описва реализирането на мерките за сигурност при предоставяне на предлаганите от Евротръст квалифицирани удостоверителни услуги. Този документ определя правата и задълженията, както на участниците в инфраструктурата на публичния ключ (PKI) на доставчика, така и на външни лица (ако има такива), участващи в дейността по предоставяне на квалифицирани удостоверителни услуги.

Описват се отговорностите, правата и задълженията на Титуляря/Създателя на квалифициран електронен подпис/печат при ползване на удостоверителни услуги, предоставяни от Евротръст.

Настоящият документ съдържа описание на следните предлагани от Евротръст услуги:

- Издаване и управление на квалифицирани удостоверения за усъвършенствани и квалифицирани електронни подписи/печати;
- Издаване и управление на квалифицирани удостоверения за уебсайт;

Евротръст може да предоставя криптографски, информационни и консултантски услуги свързани с приложимостта на удостоверителните услуги, следвайки общоприетите препоръки, спецификации и стандарти. За тези услуги, Евротръст може да публикува отделно общи условия.

Практиката се отнася за всички участници в инфраструктурата на публичния ключ на Евротръст по целия свят, включително, удостоверяващи органи, регистриращи органи, търговски агенти, клиенти, крайни потребители и всички доверяващи се страни.

Удостоверителните услуги се предоставят в съответствие с Интегрираната система за управление, прилагана от Евротръст, която включва изискванията на ISO 9001¹, ISO 27001²,

¹ ISO 9001 Системи за управление на качеството

² ISO 27001 Информационни технологии. Методи за сигурност. Системи за управление на сигурността на информацията

ISO 27701³, ISO 22301:⁴, ISO 20000-1⁵, Регламент (ЕС) № 910/2014 г.⁶, Регламент (ЕС) 2016/679⁷ (GDPR), Директива (ЕС) 2015/2366⁸ (PSD2) и приложимото законодателство в Република България.

Настоящият документ е структуриран в съответствие с рамката, определена в препоръката IETF RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.

Евротръст поддържа редица документи, свързани с прилагането на Практиката. Част от тях не са публично достъпни. Те са част от сигурността на системата за управление на информацията в Евротръст.

1.2 ИЗИСКВАНИЯ КЪМ ПРАКТИКАТА

Евротръст прилага следните изисквания:

- а) Евротръст прилага набор от политики и практики, подходящи за услугата за отдалечено подписване с електронен подпис. Приложимите политики и практики са вписани, със своите обектни идентификатори в издадените удостоверения при използване на услугата. За всяка предоставяна услуга и всяко издадено удостоверение Евротръст е публикувал на страницата си в интернет политика и практика с включени обектни идентификатори;
- б) Ръководството на Евротръст одобрява наборът от политики и практики, след което те се публикуват и съобщават на служителите и доверяващите се страни, когато е уместно;
- в) В настоящия документ са описани практиките и процедурите, използвани за изпълнение на всички изисквания на приложимата политика за удостоверителни услуги на Евротръст;

³ ISO 27701 Управление на неприкосновеността на информацията. Разширява ISO/IEC 27001 и ISO/IEC 27002 за управление на информацията за поверителност

⁴ ISO 22301 Сигурност на обществото. Системи за управление на непрекъснатостта на дейността

⁵ ISO 20000-1 Система за управление на качеството на ИТ-услугите

⁶ Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета от 23 юли 2014 г. относно електронната идентификация и удостоверителните услуги при електронни транзакции на вътрешния пазар и за отмяна на Директива 1999/93/ЕО

⁷ Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните)

⁸ ДИРЕКТИВА (ЕС) 2015/2366 НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА за платежните услуги във вътрешния пазар, за изменение на директиви 2002/65/ЕО, 2009/110/ЕО и 2013/36/ЕС и Регламент (ЕС) № 1093/2010 и за отмяна на Директива 2007/64/ЕО

d) В настоящия документ в т. 1.5.5 е разгледана възможността да има външни организации, поддържащи услугите на Евротръст. В случай на наличие на външни организации техните задължения и приложими политики и практики се описват в договорни споразумения;

e) Евротръст предоставя на потребителите и доверяващите се страни своята удостоверителна практика и друга документация, ако е необходимо, за да демонстрира съответствие с политиката за удостоверителни услуги;

f) Когато Евротръст възнамерява да направи промени в своята Практика, които биха могли да повлияят на приемането на услугата от титуляря или доверяващите се страни, Евротръст уведомява надлежно за промените потребителите и доверяващите се страни чрез публикуване на актуализираната Практика;

g) Евротръст има управителен орган, който е окончателно одобрява настоящия документ;

h) Ръководството на Евротръст управлява прилагането на приложимите политики и практики;

i) Евротръст определя процеса на преглед на практиките, което се извършва поне веднъж годишно и определя отговорностите за тяхното поддържане, което възлага на оторизирани служители;

j) Евротръст своевременно актуализира практиките и политиките, като всяка нова версия на документите се одобрява от ръководството и публикува на страницата на дружеството в интернет;

k) Евротръст публикува всяка нова редакция на приложимите си практики и политики незабавно;

l) В т. 5.9 от настоящият документ се посочват разпоредбите, предвидени за прекратяване на услугата. Друга възможност за прекратяване на услугата е при прекратяване или изтичане на давността на договора за удостоверителни услуги между потребителите и Евротръст.

1.3 НОРМАТИВНИ ПОЗОВАВАНИЯ

Съдържанието на настоящия документ е в съответствие със следните нормативни документи, стандарти, стандартизационни документи и препоръки:

- RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework;
- RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile;
- RFC 3739 Internet X.509 Public Key Infrastructure: Qualified Certificates Profile;
- RFC 6960 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP;
- RFC 3161 Internet X.509 Public Key Infrastructure: Time Stamp Protocol (TSP);
- RFC 5816 ESSCertIDv2 Update for RFC 3161;
- RFC 3279 Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List Profile;
- RFC 4055 Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile;
- ITU-T X.509 | ISO/IEC 9594-8: The Directory: Authentication framework; Public-key and attribute certificate frameworks;
- ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers;
- ETSI EN 319 411-1 Policy and security requirements for Trust Service Providers issuing certificates: General requirements;
- ETSI EN 319 411-2 Policy and security requirements for Trust Service Providers issuing certificates Requirements for trust service providers issuing EU qualified certificates;
- EN 319 421 Policy and Security Requirements for Trust Service Providers issuing Electronic Timestamps;
- ETSI EN 319 412-1 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures;
- ETSI EN 319 412-2 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons;
- ETSI EN 319 412-3 Electronic Signatures and Infrastructures (ESI); Certificate Profiles;

Part 3: Certificate profile for certificates issued to legal persons;

- ETSI EN 319 412-4 Electronic Signatures and Infrastructures (ESI); Certificate Profiles;

Part 4: Certificate profile for web site certificates;

- ETSI EN 319 412-5 Electronic Signatures and Infrastructures (ESI); Certificate Profiles;

Part 5: QCStatements;

- EN 319 422 Time-stamping protocol and electronic time-stamp profiles;
- TS 119 312 Cryptographic Suites;
- EN 319 521 Policy and Security Requirements for Electronic Registered Delivery Service Providers;

Providers;

- EN 319 522 Electronic Registered Delivery Services;
- EN 319 531 Policy and Security Requirements for Electronic Registered Electronic Mail Service Providers;

Service Providers;

- EN 319 532 Registered Electronic Mail (REM) Services;
- ETSI TR 119 460 Electronic Signatures and Infrastructures (ESI); Survey of technologies and regulatory requirements for identity proofing for trust service subjects;

➤ ETSI TS 119 461 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects;

➤ ETSI TS 119 471 Electronic Signatures and Trust Infrastructures (ESI); Policy and Security requirements for Providers of Electronic Attestation of Attributes Services;

➤ ETSI TS 119 495 Electronic Signatures and Infrastructures (ESI); Sector Specific Requirements; Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive (EU) 2015/2366;

➤ ДИРЕКТИВА (ЕС) 2015/2366 (PSD2) НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА от 25 ноември 2015 година за платежните услуги във вътрешния пазар, за изменение на директиви 2002/65/ЕО, 2009/110/ЕО и 2013/36/ЕС и Регламент (ЕС) № 1093/2010 и за отмяна на Директива 2007/64/ЕО;

➤ Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета от 23 юли 2014 година относно електронната идентификация и удостоверителните услуги при електронни трансакции на вътрешния пазар и за отмяна на Директива 1999/93/ЕО;

- Регламент (ЕС) 2024/1183 на Европейския парламент и на Съвета от 11 април 2024 година за изменение на Регламент (ЕС) № 910/2014 по отношение на създаването на европейска рамка за цифрова самоличност;
- Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните);
- Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).
- CA/Browser Forum Network and certificate system security requirements;
- ETSI EN 301 549 Accessibility requirements for ICT products and services;
- ISO/IEC 27701:2019 Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines;
- ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection - information security controls;
- ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection - Guidance on managing information security risks.

1.4 ИМЕ И ИДЕНТИФИКАЦИЯ НА ДОКУМЕНТА

Настоящият документ е с пълно наименование „Практика при предоставяне на квалифицирани удостоверителни услуги“ и е публично достъпен в електронна версия на интернет страницата на Евротръст: [CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED TRUST SERVICES](#) или се предоставя по предварително поискване, изпратено на електронен адрес: office@evrotrust.com.

Практиката е с присвоен уникален идентификатор на обект (OID – Object Identifier) 1.3.6.1.4.1.47272.3.1.1.

Практиката е свързана с Политиките при предоставяне на квалифицирани удостоверения за електронни подписи/печати и квалифицирани удостоверителни услуги.

Политиките включват:

- описание на условията, които Евротръст спазва и следва при издаване на квалифицирани удостоверения, както и приложимостта на тези удостоверения с оглед на нивото на сигурност и ограниченията при използването им;
- съвкупност от конкретни процедури, които се спазват в процеса на издаване и поддържане на квалифицирани удостоверения, изисквания при идентификация, условията и необходимите нива на сигурност при създаване на електронния подпис/печат и съхраняване на частния ключ;
- определя приложимостта и степента на доверие в приложената информация в квалифицираните удостоверения.

Практиката изпълнява общите изискванията за удостоверителни политики, посочени в ETSI EN 319 411-1:

1. **NCP** - Нормализирана политика за удостоверяване, която отговаря на общопризнатите най-добри практики на доставчици, издаващи удостоверения, използвани в подкрепа на всякакъв вид транзакции;
2. **NCP+** - Разширена нормализирана политика за удостоверяване, която предлага качеството на NCP, но включва и изискванията за защитено криптографско устройство;
3. **EVCP** - Разширена политика за валидиране на TLS/SSL удостоверения, предлагаща нивото на сигурност, изисквано от CAB Forum. Изискванията се основават на изискванията на NCP удостоверения, но допълнени с изискванията на EVCG;
4. **DVCP** - Политика за удостоверяване на домейн (DVCP) за TLS/SSL удостоверения, предлагаща нивото на сигурност, изисквано от CAB Forum. Изискванията на политиката се основават на изискванията на BRG;
5. **OVCP** - Политика за удостоверяване на TLS/SSL удостоверения за организации, предлагаща нивото на сигурност, изисквано от CAB Forum. Изискванията на политиката се основават на BRG;
6. **IVCP** - Индивидуална политика за валидиране на сертификати (IVCP) за TLS/SSL удостоверения, предлагаща нивото на сигурност, изисквано от CAB Forum. Изискванията на политиката се основават на изискванията на BRG;
7. **WEB** - Изисквания на политика за издаване на сертификати за уеб удостоверяване за общо предназначение.

Политиките за удостоверяване на Евротръст са съобразени с правилата посочени в ETSI EN 319 411-1 и идентификаторите за всяка политика. Евротръст издава удостоверения прилагайки следните политики:

- a) нормализирана политика за сертифициране (**NCP**);
- b) подобрена нормализирана политика за сертифициране (**NCP +**); и
- c) разширена политика за валидиране на сертификати (**EVCP**).

Евротръст прилага в своята дейност по издаване на удостоверения следните политики на ЕС за квалифицирани удостоверения:

1. Политика за удостоверения, издадени на **физически лица (QCP-n)**, отговарящи на изискванията на ЕС (политика за NCP, NCP+ и допълнителни изисквания за квалифицирани удостоверения, както е посочено в Регламент (ЕС) № 910/2014). Удостоверенията, издадени съгласно тези изисквания, поддържат усъвършенствани електронни подписи, основани на квалифициран сертификат, определен в членове 26 и 27 от Регламент (ЕС) № 910/2014;

2. Политика за удостоверения, издадени на **юридически лица (QCP-l)**, отговарящи на изискванията на ЕС (политика за NCP, NCP + и допълнителни изисквания, за квалифицирани удостоверения, както е посочено в Регламент (ЕС) № 910/2014). Удостоверенията, издадени съгласно тези изисквания, поддържат усъвършенствани електронни печати, базирани на квалифицирано удостоверение, определени в членове 36 и 37 от Регламент (ЕС) № 910/2014;

3. Политика за квалифицирани удостоверения (**QCP-n-qscd**), издадени на **физически лица** с използване на устройство за създаване на подпис (**QSCD**) (включва политика за QCP-n, NCP + и допълнителни изисквания, както е посочено в Регламент (ЕС) № 910/2014). Такава политика изисква частният ключ, да се намира в QSCD, отговарящи на изискванията на Регламент (ЕС) № 910/2014. Удостоверенията, издадени съгласно тези изисквания, поддържат квалифицирани електронни подписи, определени в член 3 (12) от Регламент (ЕС) № 910/2014;

4. Политика за квалифицирани удостоверения (**QCP-l-qscd**), издадени на **юридически лица**, с използване на устройство за създаване на подпис (**QSCD**) (включва политика за QCP-n, NCP + и допълнителни изисквания, както е посочено в Регламент (ЕС) № 910/2014). Такава политика изисква частният ключ, свързан със сертифицирания публичен

ключ, да се намира в QSCD. Удостоверенията, издадени съгласно тези изисквания, поддържат квалифицирани електронни печати, определени в член 3 (27) от Регламент (ЕС) № 910/2014;

5. Политика за квалифицирани удостоверения **за уебсайтове (QEVCp-w)**, отговарящи на изискванията на EVCG, предлагайки най-малкото ниво на сигурност „Extended Validated“, както е определено от CA/Browser Forum и ниво на качество, определено в Регламент (ЕС) № 910/2014 за квалифицирани удостоверения, използвани в подкрепа на удостоверяване на уебсайтове. Изискванията за **QEVCp-w** включват всички изисквания на EVCP, издадени на **юридически лица** и допълнителни разпоредби, подпомагащи издаването и управлението на квалифицирани удостоверения, както е посочено в Регламент (ЕС) № 910/2014;

6. Политика за квалифицирани удостоверения за уебсайтове (**QNCP-w**), които отговарят на BRG, като предлагат най-малко нивото на сигурност „Organization Validated“ или „Individual Validated“, както е определено от CA/Browser Forum и ниво на сигурност, определено в Регламент (ЕС) № 910/2014 за квалифицирани удостоверения, използвани в подкрепа на удостоверяване на уебсайтове. Изискванията за QNCP-w включват всички изисквания на NCP за удостоверения, издадени на физически или юридически лица и допълнително изискванията на IVCP/OVCP и управлението на квалифицирани удостоверения, както е посочено в Регламент (ЕС) № 910/2014;

7. Политика за квалифицирани удостоверения за уебсайтове (**QNCP-w-gen**), предлагащи нивото на сигурност, определено в Регламент (ЕС) № 910/2014. Политиката подкрепя удостоверения за квалифицирано удостоверяване на уебсайт с общо предназначение. Изискванията за QNCP-w-gen включват всички изисквания на NCP за удостоверения, издадени на физически или юридически лица, допълнително избрани изисквания от BRG, обозначени като **[WEB]** в ETSI EN 319 411-1, и допълнителни разпоредби, подходящи за подпомагане на издаването и управлението на квалифицирани удостоверения, както е посочено в Регламент (ЕС) № 910/2014.

Квалифицираните удостоверенията, издадени от Евротръст, съдържат идентификатори на политиките им: Certificate Policies extension. На всяка от политиките, с които се издават квалифицираните удостоверения се присвоява идентификатор на обект (OID – Object Identifier), като Евротръст специфицира в политиката и идентификаторите

според EN 319 411-1/ EN 319 411-2. Стойностите на Евротръст идентификаторите са:

Квалифициран орган/услуга	Идентификатор на обект (OID), Policy identifier
Evrotrust RSA Root CA	1.3.6.1.4.1.47272.1
Evrotrust RSA Validation (OCSP service)	1.3.6.1.4.1.47272.1.1
Evrotrust TSA	1.3.6.1.4.1.47272.1.2
Evrotrust TST	1.3.6.1.4.1.47272.1.2.1
Evrotrust RSA Operational CA	1.3.6.1.4.1.47272.2
Evrotrust RSA QS Validation (OCSP service)	1.3.6.1.4.1.47272.2.1
Evrotrust Qualified Natural Person Certificate for QES	1.3.6.1.4.1.47272.2.2
Evrotrust Qualified Natural Person Attribute Certificate for QES	1.3.6.1.4.1.47272.2.2.1
Evrotrust Qualified Legal Person Certificate for QESeal	1.3.6.1.4.1.47272.2.3
Evrotrust SSL Domain Validated Certificate	1.3.6.1.4.1.47272.2.4.1
Evrotrust SSL Organization Validated Certificate	1.3.6.1.4.1.47272.2.4.2
Evrotrust SSL EV Certificate	1.3.6.1.4.1.47272.2.5
Evrotrust SSL PSD2 Certificate	1.3.6.1.4.1.47272.2.5.1
Evrotrust Qualified Natural Person Certificate for AES	1.3.6.1.4.1.47272.2.7
Evrotrust Qualified Legal Person Certificate for AESeal	1.3.6.1.4.1.47272.2.8
Evrotrust Qualified PSD2 Legal Person Certificate for AESeal	1.3.6.1.4.1.47272.2.8.1
Evrotrust Services CA	1.3.6.1.4.1.47272.2.14
Evrotrust Services Validation (OCSP service)	1.3.6.1.4.1.47272.2.14.1
Evrotrust RSA QOperational CA 2024	1.3.6.1.4.1.47272.2.19
Evrotrust RSA QOperational CA 2024 OCSP	1.3.6.1.4.1.47272.2.19.1
Evrotrust RSA REG.KE Operational CA 2025	1.3.6.1.4.1.47272.2.23
Evrotrust REG.KE Qualified Natural Person Certificate for	1.3.6.1.4.1.47272.2.24

QES	
Evrotrust REG.KE Qualified Natural Person Certificate for AES	1.3.6.1.4.1.47272.2.25
Evrotrust REG.KE Qualified Natural Person Attribute Certificate for QES	1.3.6.1.4.1.47272.2.26
Evrotrust QEAA SU 2026 <i>/ Signing Unit for Evrotrust QEAA Signing Service /</i>	1.3.6.1.4.1.47272.3.1.3.1
Evrotrust QEAA Status SU 2026 <i>/ Signing Unit for Evrotrust QEAA Status Service /</i>	1.3.6.1.4.1.47272.3.1.3.2

Евротръст си запазва правото да разширява поддържаните Политики на издавани удостоверения, чрез оперативните Удостоверяващи органи.

Евротръст гарантира, че не променя обектния идентификатор на настоящия документ, както и обектните идентификатори на политиките, практиките и другите рефериращи документи. Ако има разширяване/промяна в политиката и практиката, която не засяга вече издадени удостоверения, Евротръст презентира нов обектен идентификатор, който описва новите удостоверения или разширените/променените такива. Евротръст следва вътрешна процедура за управление на OID.

1.5 УЧАСТНИЦИ В ИНФРАСТРУКТУРАТА НА ЕВРОТРЪСТ

Практиката регулира най-важните отношения между участниците в структурата на Евротръст, неговите консултантски и одиторски екипи, както и отношенията между доставчика, потребителите на квалифицирани удостоверителни услуги и доверяващи се страни. Изискванията и правилата описани в Практиката се прилагат за:

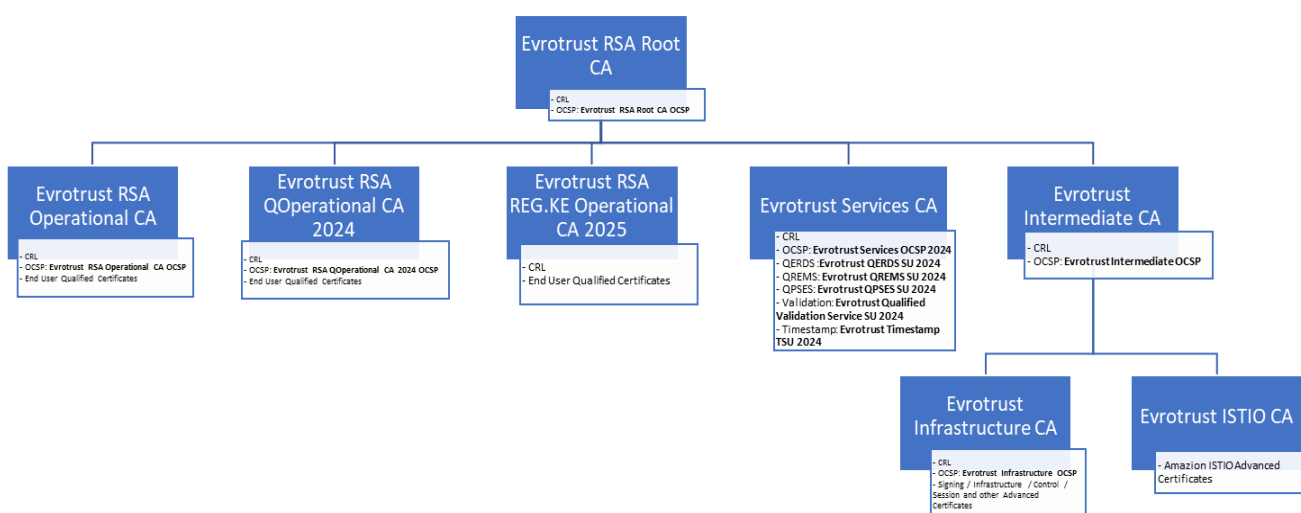
- Удостоверяващи органи;
- Регистриращи органи;
- Потребители (клиенти/Титуляри/Създатели и т.н.);
- Доверяващи се страни;
- Други участници.

Евротръст предоставя квалифицирани удостоверителни услуги на всички физически и юридически лица, които приемат правилата на този документ. Целта на Практиката е

клиентите да бъдат убедени в сигурността на предоставяните квалифицирани удостоверителни услуги.

1.5.1 УДОСТОВЕРЯВАЩИ ОРГАНИ

1.5.1.1 ЙЕРАРХИЯ НА УДОСТОВЕРЯВАЩИЯ ОРГАН



1.5.1.2 БАЗОВ УДОСТОВЕРЯВАЩ ОРГАН (EVROTRUST RSA ROOT CA)

Evrotrust RSA Root CA издава квалифицирани електронни удостоверения, които са йерархично зависими в инфраструктурно отношение в домейна на Евротръст. Базовото удостоверение на Евротръст е самоиздадено и самоподписано с базовия частен ключ на Евротръст. С базовия частен ключ доставчикът подписва удостоверения за публични ключове на свои оперативни Удостоверяващи органи.

1.5.1.3 ОПЕРАТИВНИ УДОСТОВЕРЯВАЩИ ОРГАНИ

Evrotrust RSA Operational CA, Evrotrust RSA QOperational CA 2024 и **Evrotrust RSA REG.KE Operational CA 2025** издават потребителски квалифицирани удостоверения, съгласно Практиката и Политиката за предоставяне на квалифицирани удостоверителни услуги.

Потребителските квалифицирани удостоверения, които издават **Evrotrust RSA Operational CA** и **Evrotrust RSA QOperational CA 2024** са :

- **Evrotrust Qualified Natural Person Certificate for QES/AES (E-Sign)** - издава се на физическо лице (Титуляр). Има характер на квалифицирано удостоверение за квалифициран електронен подпис/ усъвършенстван електронен подпис (КЕП/УсЕП). Може да се използва за идентифициране и установяване на самоличност при достъп до интернет приложения, защитени комуникации и електронно подписване на документи от всякакъв тип. В удостоверението може да се вписват и данни за юридическо лице, асоциирано с физическото лице, от името на което Титулярят ще подписва.

- **Evrotrust Qualified Legal Person Certificate for QESeal/AESeal (E-Seal)** - издава се на юридическо лице (Създател). Има характер на квалифицирано удостоверение за квалифициран електронен печат/усъвършенстван електронен печат (КЕПечат/УсЕПечат). Може да се използва за да се гарантира произход и интегритет на изходящи от юридическото лице данни, например: електронни документи, снимки, архитектурни проекти, софтуер и други.

- **Evrotrust Qualified PSD2 Legal Person Certificate for AESeal (E-Seal)** - издава се на Доставчик на платежни услуги (PSP) според PSD2. Има характер на квалифицирано удостоверение за УсЕПечат. Използва се за изпълнение на изискванията на PSD2.

- **Evrotrust SSL Domain Validated/Organization Validated/EV Certificate (Website authentication)** - издава се целите на удостоверяването на уебсайт, свързан с конкретно физическото или юридическото лице. Има характера на квалифицирано удостоверение за уебсайт по смисъла на Регламент (ЕС) N° 910/2014 и се използва за създаване на увереност у посетител, че уебсайта е на реален и легитимен субект. Чрез технологията се обезпечават надеждна свързаност по сигурен протокол за обмен на информацията.

- **Evrotrust SSL PSD2 Certificate (Website authentication)** - издава се за целите на удостоверяването на уебсайт, свързан с Доставчик на платежни услуги (PSP) според PSD2. Използва се за изпълнение на изискванията на PSD2. Има характера на квалифицирано

удостоверение за уебсайт по смисъла на Регламент (ЕС) № 910/2014 и се използва за създаване на увереност у посетител, че уебсайта е на реален и легитимен субект. Чрез технологията се обезпечават надеждна свързаност по сигурен протокол за обмен на информацията.

- **Evrotrust Qualified Natural Person Attribute Certificate for QES** - издава се с цел идентифициране на физическо лице (Титуляр) с конкретни, описани в удостоверението атрибути. Има характер на квалифицирано удостоверение за КЕП. Всички процедури и правила за неговото издаване и управление съвпадат с тези на Evrotrust Qualified Natural Person Certificate for QES/AES (E-Sign). Разликата между двете удостоверения е в срока на действие, обема и вида на удостоверените в тях данни.

Потребителските квалифицирани удостоверения, които издава **Evrotrust RSA REG.KE Operational CA 2025** са:

- **Evrotrust REG.KE Qualified Natural Person Certificate for QES/AES (E-Sign)** - издава се на физическо лице (Титуляр) за региона Кения. Има характер на квалифицирано удостоверение за квалифициран електронен подпис/усъвършенстван електронен подпис (КЕП/УсЕП). Може да се използва за идентифициране и установяване на самоличност при достъп до интернет приложения, защитени комуникации и електронно подписване на документи от всякакъв тип. В удостоверението може да се вписват и данни за юридическо лице, асоциирано с физическото лице, от името на което Титулярят ще подписва.

- **Evrotrust REG.KE Qualified Natural Person Attribute Certificate for QES** - издава се с цел идентифициране на физическо лице (Титуляр) с конкретни, описани в удостоверението атрибути. Има характер на квалифицирано удостоверение за КЕП. Всички процедури и правила за неговото издаване и управление съвпадат с тези на Evrotrust REG.KE Qualified Natural Person Certificate for QES/AES (E-Sign). Разликата между двете удостоверения е в срока на действие, обема и вида на удостоверените в тях данни.

Квалифицираните оперативни удостоверяващи органи на Евротръст изпълняват следните специфични задължения, включени в рамките на Политиката и Практиката на Евротръст:

➤ Приемане на електронно искане за квалифицирани удостоверения или

квалифицирани удостоверителни услуги;

- Издаване на квалифицирано удостоверение за квалифицирана удостоверителна услуга въз основа на исканията след идентификация на потребителите;
- Публикуване и поддържане на издадени квалифицирани удостоверения в съответствие с процедурите, описани в Политиките и Практиките на Евротръст;
- Приемане и изпълнение на искане за отмяна на квалифицирана удостоверителна услуга в съответствие с процедурите, посочени в Политиките и Практиките на Евротръст;
- Издаване на Списък със спрените и прекратени удостоверения (CRL);
- Публикуване на издадения CRL;
- Съхраняване записите (логовете) по процеса на издаване на квалифицирани удостоверения и от другите удостоверителни услуги, които подлежат на одит;
- Други дейности и услуги, свързани с дейността на Евротръст.

Евротръст запазва правото да разширява или променя инфраструктурата си с друга йерархия или с разширение на текущата.

1.5.1.4 ОПЕРАТИВЕН УДОСТОВЕРЯВАЩ ОРГАН (EVROTRUST SERVICES CA)

Evrotrust Services CA издава специализирани квалифицирани удостоверения, съгласно Практиката и Политиката за предоставяне на квалифицирани удостоверителни услуги.

Специализираните квалифицирани удостоверения, които издава Evrotrust Services CA в инфраструктурата на Евротръст са:

- **Evrotrust Timestamp TSU 2024** – Удостоверението е издадено на подписващия модул за време (Timestamp Signing Unit/TSU) на услугата за удостоверяване на време „Evrotrust TSA“ и има за цел да удостовери точна дата и час на електронно подписване или друго събитие. Пълното описание на услугата и профила на издаденото удостоверение се намират в документа „Политика и практика на услуга за предоставяне на квалифицирани електронни времеви печати“;
- **Evrotrust QERDS SU 2024** – Удостоверението е издадено на подписващия модул (Signing Unit/SU) на квалифицираната услуга за електронна препоръчана поща (QERDS) и има за цел да удостовери всички издадени доказателства/удостоверения от страна на услугата. Пълното описание на услугата и профила на издаденото удостоверение се намират в

документа "Политика и практика при предоставяне на квалифицирана услуга за електронна препоръчана поща";

- **Evrotrust QREMS SU 2024** – Удостоверението е издадено на подписващия модул (Signing Unit/SU) на квалифицирана услуга за имейл препоръчана поща (QREMS) и има за цел да удостовери всички издадени доказателства/удостоверения от страна на услугата. Пълното описание на услугата и профила на издаденото удостоверение се намират в документа "Политика и практика при предоставяне на квалифицирана услуга за имейл препоръчана поща";

- **Evrotrust QPSES SU 2024** – Удостоверението е издадено на подписващия модул (Signing Unit/SU) на услуга по квалифицирано съхраняване на квалифицирани електронни подписи/печати (QPSES) и има за цел да удостовери всички издадени доказателства/удостоверения от страна на услугата. Пълното описание на услугата и профила на издаденото удостоверение се намират в документа "Политика и практика при предоставяне на услуга по квалифицирано съхраняване на квалифицирани електронни подписи/печати";

- **Evrotrust Qualified Validation Service SU 2024** – Удостоверението е издадено на подписващия модул (Signing Unit/SU) на услуга за валидиране на подписи (QSVSP) и има за цел да удостовери всички издадени доказателства/удостоверения от страна на услугата. Пълното описание на услугата и профила на издаденото удостоверение се намират в документа "Политика и практика на услуга по квалифицирано валидиране на квалифицирани електронни подписи/печати".

- **Evrotrust QEAA SU 2026** – Удостоверението е издадено на подписващия модул (Signing Unit/SU) на услуга за Издаване на Квалифицирани Електронни Удостоверения за Атрибути (QEAA). Това удостоверение е предназначена да доказва всички издадени от услугата удостоверения (assertions). Пълното описание на услугата и профилът на издаденото удостоверение са описани в документа „Qualified Electronic Attestation of Attributes (QEAA) Policy and Practice Statement“.

- **Evrotrust QEAA Status SU 2026** – Удостоверението е издадено на подписващия модул (Signing Unit/SU) на услуга за Удостоверяване на статус на Квалифицирани Електронни Удостоверения за Атрибути (QEAA). Това удостоверение е предназначена да доказва всички издадени от услугата удостоверения (assertions) за статус. Пълното описание на услугата и

профилът на издаденото удостоверение са описани в документа „Qualified Electronic Attestation of Attributes (QEAA) Policy and Practice Statement“.

Квалифицираният оперативен удостоверяващ орган на Евротръст **“Evrotrust Services CA”** изпълнява следните специфични задължения, включени в рамките на Политиката и Практиката на Евротръст:

- Приемане на електронно искане за квалифицирани удостоверения на предоставяна удостоверителна услуга;
- Издаване на квалифицирано удостоверение за квалифицирана удостоверителна услуга;
- Публикуване и поддържане на издадени квалифицирани удостоверения в съответствие с процедурите, описани в Политиките и Практиките на Евротръст;
- Приемане и изпълнение на искане за отмяна на квалифицирано удостоверение в съответствие с процедурите, посочени в Политиките и Практиките на Евротръст;
- Издаване на Списък със спрените и прекратени удостоверения (CRL);
- Публикуване на издадения CRL;
- Съхраняване записите (логовете) по процеса на издаване на квалифицирани удостоверения и от другите удостоверителни услуги, които подлежат на одит;
- Други дейности и услуги, свързани с дейността на Евротръст.

Евротръст запазва правото да разширява или променя инфраструктурата си с друга йерархия или с разширение на текущата.

1.5.1.5 ОРГАНИ ЗА ПРОВЕРКА НА СТАТУС НА УДОСТОВЕРЕНИЯ (OCSP SERVICE)

Квалифицираните удостоверения в инфраструктурата на Евротръст, които се използват за подписване на заявката за валидиране, биват:

- **Evrotrust RSA Validation** – Използва се за валидиране на базовия подпис и се издава директно от Базовия удостоверяващ орган “Evrotrust RSA Root CA”;
- **Evrotrust RSA QS Validation** – Използва се за валидиране на квалифицирани удостоверения и е издаден от Оперативния удостоверяващ орган “Evrotrust RSA Operational CA”

- **Evrotrust Services Validation** – Използва се за валидиране на квалифицирани удостоверения и е издаден от Оперативния удостоверяващ орган "Evrotrust Services CA".
- **Evrotrust RSA QOperational CA 2024 OCSP** – Използва се за валидиране на квалифицирани удостоверения и е издаден от Оперативния удостоверяващ орган "Evrotrust RSA QOperational CA 2024".

В процеса на валидиране на квалифициран електронен подпис/печат Органът за валидиране на Евротръст потвърждава валидността на квалифицирания електронен подпис/печат, при условие че:

- удостоверението, придружаващо подписа/печата към момента на подписването е било квалифицирано удостоверение за електронен подпис/печат, отговарящо на изискванията на Регламент (ЕС) 910/2014 г.;
- квалифицираното удостоверение, издадено от Евротръст е било валидно към момента на подписването;
- данните за валидиране на подписа/печата съответстват на данните, предоставени от доверяващата се страна;
- уникалният набор от данни, представящи Титуляря/Създателя на електронния подпис/печат в удостоверението, е надлежно предаден на доверяващата се страна;
- ако към момента на подписването е бил използван псевдоним, то това е ясно указано на доверяващата се страна;
- електронният подпис/печат е създаден от устройство за създаване на електронен подпис/печат;
- целостта на подписаните данни не е застрашена;
- изискванията на настоящия документ са били изпълнени към момента на подписването.

Използваната за валидиране на квалифицирания електронен подпис/печат система на Евротръст предоставя на доверяващата се страна правилния резултат от процеса на валидиране и ѝ позволява да открие евентуални проблеми, свързани със сигурността.

Всяка доверяващата се страна, когато приема квалифицирано удостоверение, може да заяви проверка на статуса на удостоверенията в реално време през OCSP сървър (On-line

Certificate Status Protocol/Протокол за онлайн проверка на статуса на удостоверение).

Проверката на статуса на удостоверение в реално време не е задължителна функция за Доверяващите се страни, но Доставчикът препоръчва да се използва тази услуга. За постигане на по-голяма сигурност при използване на електронни подписи/печати, е препоръчително интегриране на услугата в процеса на създаване или приемане на електронно подписани документи.

1.5.2 РЕГИСТРИРАЩ ОРГАН

Функциите на Регистриращ орган се извършват от обособена структура на Евротръст или от външни лица, на които Евротръст възлага осъществяването им, в рамките на разрешеното от закона. Функциите са:

- Приемане на искане за квалифицирана удостоверителна услуга;
- Евротръст събира и валидира или преки доказателства, или удостоверение от подходящ и оторизиран източник за самоличност (например име) и, ако е приложимо, всякакви специфични атрибути на субектите, на които е издадено удостоверение. Представените доказателства могат да бъдат под формата на хартиена или електронна документация;
- Проверката на самоличността на субекта се извършва в момента на регистрация чрез подходящи средства. Събирането на доказателства може да включва копие на лични данни, като лична карта или паспорт;
- Идентифициране на лицето подало искане съгласно установените от Евротръст правила и процедури;
- Удостоверяване на верността и допустимостта на подадено искане за квалифицирано удостоверение;
- Уведомяване на потребителите за издадено квалифицирано удостоверение;
- Осигуряване на надеждна среда за получаване на издадено квалифицирано удостоверение или използване на квалифицирана удостоверителна услуга;
- Инициране и предаване на удостоверяващия орган в хартиена или електронна форма на заявки за управление (спиране, възобновяване или прекратяване) на издадени удостоверения;
- Извършване на одобрение на заявки за продължаване действието на

квалифицирано удостоверение от името на Евротръст;

- Сключване на договори за предоставяне на удостоверителни и други криптографски, информационни и консултантски услуги с потребители от името на Евротръст;
- Други функции, които осигуряват функционирането на квалифицирана удостоверителна услуга на Евротръст.

Регистриращият орган може да бъде обособено звено в рамките на юридическо лице, различно от Евротръст, на което са делегирани права да осъществява тези дейности или на част от тях от името на Евротръст. Отношенията между Евротръст и Регистриращия орган се уреждат с договор.

1.5.3 ПОТРЕБИТЕЛИ

Всяко физическо, юридическо или друго лице, което има сключен договор с Евротръст за удостоверителна услуга е потребител на тази предоставена от Евротръст услуга.

Когато това е практически осъществимо, предоставяните удостоверителни услуги и използваните при предоставянето на тези услуги продукти са достъпни и за хора с увреждания.

1.5.3.1 ТИТУЛЯР

Титулярят (Titular) на електронен подпис е физическо лице, което създава електронния подпис.

Титулярят осъществява от свое име или от името на друго лице, което той представлява, електронни изявления, които електронно подписва в съответствие с предоставената му представителна власт. В удостоверението може се посочи и лицето, което Титуляря представлява.

Титулярят на електронния подпис може да възлага обслужването на устройствата за създаване на квалифицирани електронни подписи на трета страна, при условие, че са въведени подходящи механизми и процедури, гарантиращи, че Титулярят разполага с едноличен контрол върху използването на данните, свързани със създаването на електронния му подпис, и че при използването на устройството са изпълнени изискванията по отношение на квалифицирания електронен подпис.

Единствено Титулярят на квалифицираното удостоверение, има право на достъп до

частния ключ за подписване на електронни изявления, чрез които създава усъвършенстван или квалифициран електронен подпис.

1.5.3.2 СЪЗДАТЕЛ НА ПЕЧАТ

Създателят (Creator) на печат е юридическо лице, което създава електронен печат.

Създателят може да подписва електронни обекти, независимо от тяхната същност (софтуер, снимки, музика, филми, книги, архитектурни проекти, бази данни, дизайн и др.), с което огласява, че той е легитимния източник на този електронен обект, както и обекта е с ненарушена цялост (интегритет). Електронният печат не гарантира права върху електронния обект (авторски и други).

Юридическото лице е посочено в издаденото удостоверение за електронен печат като Създател.

Единствено Създателят като Потребител на квалифицирано удостоверение, има право на достъп до частния ключ за подписване на електронни изявления, чрез които той създава усъвършенстван или квалифициран електронен печат.

1.5.3.3 КЛИЕНТ

Клиент (Subscriber) е лицето, което ползва квалифицираната удостоверителна услуга. Той може да е юридическо, физическо или друго лице и може да съвпада с Титуляря/Създателя.

Клиентът може да действа от името на един или няколко различни Титуляри/Създатели, с които той е свързан. Клиентът е например компания, която изисква удостоверения за своите служители, за да им позволи да участват в електронните бизнес процеси от името на компанията и може да не присъства в данните, вписани в издаденото удостоверение. Клиентът може да е и лице, което например ползва удостоверителна услуга на Евротръст за удостоверяване на време.

1.5.4 ДОВЕРЯВАЩИ СЕ СТРАНИ

Доверяваща се страна означава физическо или юридическо лице, което разчита на удостоверителна услуга.

Доверяващите се страни следва да имат познания и умения относно използването на квалифицирано удостоверение и да се доверяват на удостоверените обстоятелства в тях само с оглед на приложимата Политика, особено по отношение на нивото на сигурност при проверка на самоличността на Титулярите и идентичността на Създателите на тези квалифицирани удостоверения, както и по отношение на вписаните в удостоверението ограничения за използването му.

Доверяващите се страни имат постоянен достъп до регистрите на Евротръст за проверка на валидността на квалифицираните удостоверения, за установяване на електронната идентичност на Титулярите/Създателите или на други обстоятелства и данни, отразени в удостоверенията или вписани в тези регистри.

Доверяващите се страни, установени извън територията на Република България, могат да разчитат на надеждно, сигурно, лесно и удобно квалифицирано валидиране по автоматизиран начин на квалифицирани електронни подписи и електронни печати, удостоверенията за които са издадени от Евротръст.

1.5.5 ДРУГИ УЧАСТНИЦИ

За определени дейности, съгласно Регламент (ЕС) № 910/2014, Евротръст може да привлича външни лица. Отношенията по повод на тези дейности се уреждат с договор. Договорът определя правата и задълженията, на външните лица, участващи в дейността по предоставяне на удостоверителни услуги. Евротръст използва подизпълнители и доставчици на услуги като специализирани дейта центрове за надеждна и сигурна колокация на сървърното и мрежово оборудване, доставчици на облачни системи и услуги, доставчици на услуги по автоматизирана идентификация, IT услуги и др. При работата си с подизпълнители и доставчици Евротръст изисква от тях стриктно да бъдат спазвани неговите инструкции, в съответствие с настоящата Политика и Практика.

1.6 УПОТРЕБА И ПРИЛОЖИМОСТ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ

Квалифицирано удостоверение за електронен подпис/печат, за квалифициран електронен времеви печат или за автентичност на уебсайт се издава от „Евротръст Технолъджис“ АД като квалифициран доставчик на квалифицирани удостоверителни услуги и

отговаря на определените в Регламент (ЕС) 910/2014 г. изисквания за употреба и приложимост.

Контекста на приложимост на удостоверенията може да варира в зависимост от целта, за която се използват в Република България и други европейски страни, като освен средство за подписване, те биват използвани и в ролята им на средство за идентифициране, установяване на криптирана TLS връзка, криптиране на данни и други.

Описание на употребата и приложимостта на квалифицираните удостоверения има в документа Политика при предоставяне на квалифицирано удостоверение за квалифициран електронен подпис/печат.

1.7 УПРАВЛЕНИЕ НА ПРАКТИКАТА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНА УДОСТОВЕРИТЕЛНА УСЛУГА

Всяка версия на Практиката при предоставяне на квалифицирана удостоверителна услуга е в сила (има актуално състояние) до момента на одобрение и публикуване на нова версия. Всяка нова версия се разработва от служители на Евротръст и след одобрение от Съвета на директорите се публикува.

Абонатите са длъжни да се съобразяват само с валидната версия на Практиката към момента на ползване на услугите на Евротръст.

Контактното лице за управление на документа „Практика при предоставяне на квалифицирани удостоверителни услуги“ от „Евротръст Технолджис“ АД е изпълнителния директор на Евротръст.

Допълнителна информация може да бъде получена на следния адрес:

гр. София, 1766

бул. „Околовръстен път“ № 251 Г, „ММ БИЗНЕС ЦЕНТЪР“, ет. 5

телефон, факс: + 359 2 448 58 58

електронен адрес: office@evrotrust.com

2 ОТГОВОРНОСТ ЗА ПУБЛИКУВАНЕ И ХРАНИЛИЩЕ

2.1 ХРАНИЛИЩЕ

Евротръст поддържа хранилище, в което са разположени актуални и предишни версии

на електронни документи. Евротръст управлява и контролира уеб сайта на дружеството, където публикува всички актуални версии на електронните документи и осигурява сигурен и непрекъснат достъп до тях на заинтересованите страни. Регистърът на удостоверенията е база данни, в която се публикуват всички издадени удостоверения, които Евротръст използва в дейността си, потребителски удостоверения и списъци на прекратени удостоверения. Относно хранилището Евротръст изпълнява следните изисквания:

- в регистъра на удостоверенията се съдържат удостоверенията на инфраструктурата на публичния ключ (PKI/Public Key Infrastructure) и клиентски удостоверения на разположение на клиенти и доверяващи се страни;
- гарантира, че всички удостоверения, публикувани в регистъра на удостоверенията принадлежат на посочените в тях потребители или на упълномощени от тях представители;
- удостоверенията са на разположение само в случаите, за които е получено съгласието на титуляря. Ако субектът е устройство или система, трябва да се получи съгласието от физическото или юридическото лице, отговорно за експлоатацията на устройството или системата, вместо субекта;
- гарантира, че удостоверенията на удостоверителните органи, принадлежащи на Евротръст и удостоверенията на потребителите са публикувани в регистъра на удостоверенията;
- публикува на уеб сайта си (<https://www.evrotrust.com>) актуални „Политика при предоставяне на квалифицирани удостоверителни услуги“, „Практика при предоставяне на квалифицирани удостоверителни услуги“, Общи условия, образци на документи, предназначени за потребителите и споразумения между страните, както и архивни версии;
- дава достъп до информация относно статуса на удостоверенията, чрез публикуване на CRL или чрез използване на протокола OCSP;
- Всички потребители и доверяващи се страни имат постоянен достъп 24/7/365 до информацията на уеб сайта на доставчика на адрес: <https://www.evrotrust.com>. Достъпността до тази информация няма географски ограничения;
- осигурява достъп до информацията в регистъра на удостоверенията за удостоверяващите органи, регистриращия орган, потребителите и доверяващите се страни;
- публикува друга информация бързо и в съответствие със сроковете, определени в този документ;

➤ осигурява безопасен и контролиран достъп до информацията в регистъра на удостоверенията.

Всички потребители, имат неограничен достъп до цялата информация на уеб сайта.

2.2 ИНФОРМАЦИЯ, ПУБЛИКУВАНА ОТ ЕВРОТРЪСТ

Уеб сайта на Евротръст е достъпен на адрес: <https://www.evrotrust.com>.

Достъп до уеб сайта може да се осъществява по протокол HTTP/HTTPS.

Информацията, публикувана от Евротръст включва документи, които описват:

- Условието и реда за издаване на електронно удостоверение, включително за правилата за установяване идентичност на Титуляр на удостоверение;
- Процедури за сигурност при издаване и управление на удостоверенията;
- Начин на използване на удостоверенията;
- Условие и ред за използване на квалифицирани удостоверения, включително изисквания за съхраняване на частен ключ;
- Условие за достъп до удостоверение и начин на проверка на квалифицирано удостоверение;
- Цена за получаване и използване на удостоверение, както и цени на останалите предоставяни услуги;
- Отговорност на Евротръст и на Титуляр/Създател на квалифициран електронен подпис/печат;
- Условие и ред, по които Титулярят/Създателят прави искане за прекратяване
- действието на квалифициран електронен подпис/печат.
- Доклади от одити, извършени от упълномощена институция;
- Допълнителна информация, например съобщения и известия.

Част от цитираната информацията се съдържа в този документ и в Практиките за предоставяне на други квалифицирани удостоверителни услуги.

Освен посочената документация, Евротръст публикува и:

- Базовото си удостоверение (Evrotrust RSA Root CA);
- Оперативните си удостоверения на Удостоверяващите органи;
- Удостоверенията за време;

- Издадените от Евротръст удостоверения;
- Списъкът на спрените и отменени удостоверения (CRL), издадени от Евротръст.

2.3 ЧЕСТОТА НА ПУБЛИКУВАНЕ

Евротръст публикува информация със следната честота:

- „Политика при предоставяне на квалифицирани удостоверителни услуги“ и „Практика при предоставяне на квалифицирани удостоверителни услуги“ подлежи на незабавно публикуване при всяка актуализация;
- Оперативните удостоверения - при всяко издаване на ново удостоверение;
- Актуализация в регистъра на издадените удостоверения се осъществява автоматично и незабавно след публикуване на всяко новоиздадено валидно удостоверение;
- Актуализация на текущия Списък със спрени и прекратени удостоверения (CRL) се осъществява автоматично на не повече от 3 (три) часа или незабавно след прекратяване или спиране/възобновяване на валидно удостоверение. Във всички Списъци със спрени и прекратени удостоверения (CRL) Евротръст указва времето за следващото издание. Ефективният период на валидност на публикувания актуален Списък е посочен в него, освен ако не се извърши актуализация;
- Допълнителна информация - при всяко настъпило събитие.

2.4 ДОСТЪП ДО ПУБЛИКАЦИИ

Евротръст предлага достъп до публикации, които са достъпни на неговия уеб сайт чрез използване на HTTP/HTTPS базиран достъп.

Цялата информация в на уеб сайта, публикувана от Евротръст, е общодостъпна. Достъпът до регистъра на удостоверенията също не се ограничава от Евротръст, освен по искане на Титуляря и само по отношение на негово удостоверение.

Информацията, публикувана в на уеб сайта на Евротръст, е достъпна постоянно (24/7/365), освен в случаите на събития, извън контрола на Евротръст и в случаи на краткотрайни временни прекъсвания за профилактика.

Доставчикът осигурява свободен достъп до всички базови и оперативни удостоверения на своите активни удостоверителни органи, както и свободен достъп до тези на всички неактивни такива за срок не по-малък от 2 (две) години след изтичане на срока на

валидност на тези удостоверения.

Комуникациите между потребителите и защитените уеб страници на Евротръст се осъществяват чрез използване на HTTPS протокол.

Евротръст е предприел мерки, логически и физически механизми за защита срещу неоторизирано добавяне, премахване и промяна на информацията публикувана на уеб сайта на доставчика.

При откриване на нарушения в информацията Евротръст предприема подходящи действия, за да възстанови целостта на информацията. При необходимост Евротръст налага законови санкции, уведомява засегнатите субекти и компенсира загубите им.

3 ИДЕНТИФИКАЦИЯ И УДОСТОВЕРЯВАНЕ НА САМОЛИЧНОСТ/ИДЕНТИЧНОСТ

Тази част от Практиката представя общите правила за проверка на самоличността/идентичността на потребителите, прилагани от Евротръст при издаване на квалифицирани удостоверения. Правилата са базирани на определени видове информация, която се включва в удостоверенията. По този начин се гарантира, че включената информация е точна и достоверна в момента на издаване на удостоверение. Проверката на данни задължително се извършва в етапа на регистрация на потребителя и по искане на Евротръст за всички квалифицирани удостоверителни услуги.

Регистриращият орган на доставчика извършва следните действия по идентификация:

- приема искания за издаване на квалифицирани удостоверения;
- осъществява проверка за установяване на самоличността на Титуляря, съответно идентичността на Създателя и на специфични данни за тях с допустими средства;
- утвърждава след успешна проверка или отхвърля регистрираните искания;
- уведомява Удостоверяващия орган да издаде исканото удостоверение.

Евротръст, съответно Регистриращият орган събира и получава необходимата информация за идентификация и проверка на самоличността на Титуляря/Създателя.

Евротръст е разработило специализирана система за отдалечена видео идентификация чрез мобилно приложение, инсталирано на смарт устройство на потребителя. Същото гарантира идентификация на потребителя в реално време чрез автоматична видео идентификация въз основа на получени данни и снимка от национална база данни от

документи за самоличност или чрез видеоконферентна връзка в реално време от оператор, въз основа на предоставен по електронен път документ за самоличност и по специална методология. Проверката на самоличност и идентичност на физически и юридически лица и, при необходимост специфични атрибути, свързани с лицата се извършва чрез система за отдалечена видео идентификация. Услугата предоставя сигурен метод за идентификация на потребителя по смисъла на чл. 24, ал. 1а, буква в) от Регламент (ЕС) № 910/2014 г., изменен с Регламент (ЕС) № 2024/1183 г., който гарантира идентифицирането на лицето с висока степен на надеждност и чието съответствие е потвърдено от орган за оценяване на съответствието.

Автоматизираната отдалечена идентификация на юридическите лица, които ще бъдат вписвани в издаваните квалифицирани удостоверения, както и законната представителна власт на Титуляря спрямо тях, се установява в реално време, чрез проверка на актуалния статус и вписванията в търговски и други регистри, в които са вписани.

Когато справка не може да се извърши, идентификацията на юридическите лица и проверката на представителна власт се извършва на място, въз основа на представени документи от служител на Евротръст или Регистриращ орган.

Евротръст гарантира, че физическите и юридическите лица са правилно идентифицирани, тяхната самоличност е проверена и че исканията за издаване на квалифицирани удостоверения са напълно, акуратно и надлежно проверени и одобрени, включително пълното име/наименование и правния статус на съответното физическо/юридическо лице и връзката между удостоверените данни и физическото/юридическото лице.

Идентификацията и проверката на самоличността на Титуляря/Създателя се извършва преди да бъде издадено квалифицирано удостоверение. Тя се извършва чрез системата за отдалечена идентификация или чрез лично явяване на Титуляря/Създателя, или на упълномощено от него лице пред служител на Евротръст, или пред Регистриращ орган.

3.1 ИМЕНА

В квалифицираните удостоверения се използват всички приложими имена или други идентификатори, включвайки ASN.1 идентификатори на обект. Изискванията за имената в удостоверенията са както е посочено в Препоръка ITU-T X.509 или IETF RFC 5280 и на ETSI EN 319 412. Допуска се имената да бъдат в съответствие с Domain Name Service (DNS), описан в

RFC 2247.

Регистриращите органи проверяват и гарантират, че имената в исканията за издаване на удостоверения отговарят на стандарта X.509.

Полето „Subject“ в удостоверението съдържа наименованието на Титуляря/Създателя.

Името и другите индивидуализиращи белези на Титуляря/Създателя в съответните полета за всеки тип удостоверение са в съответствие с DN (Distinguished Name), формиращо се съобразно стандарта X.500 и X.520.

Оперативните удостоверения на Евротръст съдържат в полето „Subject“ и поле „Issuer“ атрибут DN, формиращ неговото уникалното име.

Детайлна спецификация на издаваните от Евротръст удостоверения се съдържа в последващите части на настоящия документ.

3.1.1 ВИДОВЕ ИМЕНА

Изискванията за имена в издаваните удостоверения са както е посочено в Препоръка ITU-T X.509 или IETF RFC 5280 и на ETSI EN 319 412. Допуска се имената да бъдат в съответствие с Domain Name Service (DNS), описан в RFC 2247. По този начин се позволява на абонатите да използват два вида имена: DN и DNS едновременно.

За да се осигури по-лесен начин за електронна комуникация с потребителя, може да се използва и алтернативно име (псевдоним). Доставчикът може да издава квалифицирано удостоверение като използва „псевдоним“ за да именува потребителя, само след като за същото е събрана необходимата информация за самоличността му и е успешно идентифициран. Името може да съдържа и адрес на електронна поща на потребителя, който е в съответствие с препоръка RFC 822.

3.1.2 НЕОБХОДИМОСТ ОТ СМИСЛЕНИ ИМЕНА

Имената, включени в Distinguished Name (DN) на потребителя имат своето значение в българския или в друг чужд език. Структурата DN зависи от вида на удостоверението и потребителя. DN се състои от следните области (описанията са в съответствие с препоръка RFC 3280 и X.520):

- поле C - международно съкращение на името на страната (BG за България);
- поле CN - пълно/често използване име на физическото лице или на организацията;
- поле GN - име на физическото лице;
- поле SN - фамилия на физическото лице;
- поле O - име на институцията, която лицето представлява;
- поле E - имейл адрес на Титуляря/Създателя;
- поле SerialNumber - уникален идентификатор на физическото лице,
- Други полета, които се подробно описани в политиките за съответните профили на квалифицираните удостоверения.

DN трябва да бъде потвърдено от оператор на Регистрацията орган и одобрено от Удостоверяващия орган.

3.1.3 АНОНИМНОСТ НА ПОТРЕБИТЕЛИТЕ

Евротръст не публикува удостоверения и други идентификационни данни, за да се гарантира анонимността на данните на потребителите (например ЕГН), освен ако лицето изрично не заяви своето желание за това.

3.1.4 ПРАВИЛА ЗА ТЪЛКУВАНЕ НА РАЗЛИЧНИ ФОРМИ НА ИМЕНА

Тълкуването на полетата, предвидени в удостоверенията, издадени от Евротръст са в съответствие със удостоверенията на потребителския профил, описан по-долу в този документ.

Във всички удостоверения, в които се вписва Титуляря, полето за име (Common Name, CN) съдържа общоприето име на физическото лице.

В удостоверение, в което се вписва лице, от името на което действа Титуляря, атрибутът за уникално име (DN) съдържа информация и за самоличността, съответно идентичността на това лице.

Името, което е използвано в удостоверението на един потребител, никога няма да бъде използвано в удостоверение на друг потребител.

3.1.5 УНИКАЛНОСТ НА ИМЕНАТА

Полето „Subject“ в удостоверението се формира от информацията за Титуляря/Създателя, която се предоставя онлайн или на хартия от лицето подало заявка или от упълномощен представител при регистрация на първоначално искане за издаване на удостоверение и която се проверява от Регистриращия орган въз основа на представени документи, видео идентификация и проверки в първични държавни регистри.

Евротръст гарантира уникалност на „DN“ на Титуляря/Създателя в неговия домейн, чрез добавяне на реквизит, който гарантира такава уникалност.

Титуляр/Създател с уникален DN в домейна на Евротръст може да има повече от едно издадени действителни квалифицирани удостоверения.

Всяко издадено удостоверение има уникален сериен номер („SerialNumber“) в домейна на Евротръст. Комбинацията на полета „Issuer“ и „SerialNumber“ гарантират уникалността на издаденото удостоверение в публичния домейн.

3.1.6 ПОВЕРКА НА ИМЕНА И СПОРОВЕ ПО ПОВОД НА ТЯХ

Имената, които не са собственост на лице подало искане не могат да бъдат използвани в неговите приложения. В случай на съмнение, лицето е длъжно да приложи документи, доказващи собствеността на имената.

Извън дължимата грижа на Евротръст е да проверява дали потребителят има право да използва името поставено в искането за регистрация, нито може да играе роля на арбитър за разрешаване на спорове. Евротръст не носи отговорност, когато използваните имена в удостоверението, нарушават чужди права върху търговско име, търговска марка, домейни, авторски права и др.

В случай на възникнал спор по отношение на използвани имена, Евротръст си запазва правото да не издаде удостоверение или едностранно и без предизвестие да прекрати договора за поддържане на такова.

Евротръст не носи отговорност, когато използвани от потребители имена в удостоверения нарушават чужди субективни права.

3.2 ПЪРВОНАЧАЛНА РЕГИСТРАЦИЯ

Първоначалната регистрация на потребителя се извършва, когато той подава искане за регистрация за първи път в Евротръст.

Регистрацията включва процедури, които позволяват преди да се издаде удостоверение на потребител, да се съберат данни за неговата самоличност/идентичност и същият да се идентифицира. Потвърждението на тези данни изисква физическо присъствие пред служител на Евротръст или негов Регистриращ орган, нотариус или друго оправомощено лице, потвърждаващи неговата самоличност/идентичност. Тази процедура може да се осъществи отдалечено и при възможност и автоматизирано по реда, посочен по-горе, чрез система за отдалечена идентификация, отговаряща на изискванията на Регламент (ЕС) № 910/2014.

Потребителят, физическото лице е длъжно да предостави пред представител на Регистриращия орган следната информация за еднозначно идентифициране и проверка на самоличността му:

- Имена;
- Документ за самоличност – личната карта, международен паспорт или друг документ за самоличност;
- Национален идентификационен номер, ако има такъв;
- Данни за контакт – мобилен телефон, +

След успешна проверка на самоличността на Титуляря, оторизираният оператор в Регистриращия орган:

- предлага договор за квалифицирани удостоверителни услуги подписан от името на Евротръст и съхранява всички представени документи към договора;
- потвърждава искането за издаване и изпраща електронно искане за издаване на удостоверение до оперативния Удостоверяващ орган на Евротръст;
- записва издаденото удостоверение на устройство за създаване на електронен подпис (QSCD/Secure Signature Creation Device) и го предава на Титуляря или на упълномощеното лице.

При използване на системата за отдалечена идентификация чрез специално разработено мобилно приложение, Титулярят заявява отдалечено предоставянето на услугата, като предоставя документ за самоличност и данни от него, както и данни за мобилен номер и електронна поща. В този случай, Титулярят заявява сключване на договор и издаване на квалифицирано удостоверение за квалифициран електронен подпис и незабавно

автоматизирано подписва договора с Евротръст.

За всяко лице в системите на Евротръст се поддържа регистрационен профил.

3.2.1 ПРОВЕРКА ЗА ПРИТЕЖАНИЕ НА ЧАСТЕН КЛЮЧ

За издаване или продължаване на действието на удостоверение е необходимо Евротръст да получи електронно искане във формат PKCS#10. Спецификацията на този формат на искане за издаване на удостоверение изисква искането да бъде подписано от Титуляря/Създателя, притежаващ частния ключ.

Евротръст извършва проверка на валидността на електронния подпис/печат, придружаващ искането. Установяването на валидност на поставения електронен подпис/печат е достатъчно основание да се счита, че Титулярят/Създателят е подал електронно искане и че притежава частния ключ, който е технически годен и кореспондира на публичния ключ, съдържащ се в искането.

Двойката ключове, съответстваща на издаването от Евротръст квалифицирано удостоверение, задължително се генерира в устройство за създаване на електронен подпис/печат.

Когато се заявява отдалечено издаване на квалифицирано удостоверение за електронен подпис/печат, Евротръст предоставя на Титуляря/Създателя услугата отдалечено, чрез генериране на двойката ключове в хардуерен криптомодул, отговарящ на изискванията за устройство за сигурно създаване на подпис. Частният ключ се съхранява в криптиран вид, като за криптиране се използва ПИН кодът на Титуляря/Създателя.

Контролът на достъпа до частния ключ се осъществява само от Титуляря/Създателя.

3.2.2 УСТАНОВЯВАНЕ НА ИДЕНТИЧНОСТ НА ЮРИДИЧЕСКО ЛИЦЕ

Установяването на идентичността на юридическо лице (Създател), се осъществява от представител на Регистриращия орган, чрез проверка в съответните регистри по предоставен ЕИК, БУЛСТАТ или друг идентификационен номер на лицето. За юридически лица, за които не може да се извърши автоматизирана проверка се представят:

- Съдебно решение или друг документ, удостоверяващи възникването на юридическото лице;
- Документ, удостоверяващ актуалното състояние на лицето;
- Уникален национален идентификатор.

След копиране на всички изискуеми документи, със съгласието на лицето подало искането, копията остават в архива на Евротръст.

Когато вместо юридическо лице се явява негов упълномощен представител, удостоверяването на информацията, която се съдържа в представените документи става чрез:

- Заверка „Вярно с оригинала“ и саморъчен подпис върху документите пред служител на Регистриращия орган, в случай на лично предаване на документите;
- Нотариална заверка на документите, които се изпращат по поща до Регистриращия орган;
- Подписване на приложените електронни формати на документите с валидно удостоверение за квалифициран електронен подпис/печат;
- Преглед и потвърждение, чрез използване на специализирано мобилно или друго приложение и след извършена надлежна идентификация на представляващото лице и/или юридическото лице от служител на Евротръст.

Удостоверяване на идентичността на юридическо лице има две цели. Първата цел е да се докаже, че по време на разглеждане на искането юридическото лице съществува. Втората цел е да се докаже, че представителното лице, което кандидатства за удостоверение е получил разрешение от юридическото лице да го представлява.

Служителят на Регистриращия орган може да провери регистрацията посредством всички достъпни публични услуги съгласно приложимото законодателство.

При идентифициране на лица, за които се издават удостоверения за целите на изпълнение на изискванията по PSD2, Евротръст проверява специфичните атрибути, които получава от лицето и които вписва в издаваните удостоверения, чрез използване на автентична информация от Компетентен национален орган (NCA) (напр. публичен регистър). В случай, че NCA е определил правила за проверка на тези атрибути, Евротръст ги изпълнява и прилага.

Ако субектът е устройство или система, управлявана от или от името на юридическо

лице или друг организационен субект, идентифициран във връзка с юридическо лице, доказателства на самоличността се проверяват надлежно чрез упълномощено лице (subscriber), директно, чрез физическо присъствие на лице, или трябва да се проверяват непряко, като се използват средства, осигуряващи еквивалентна сигурност физическо присъствие.

3.2.3 УСТАНОВЯВАНЕ НА САМОЛИЧНОСТ НА ФИЗИЧЕСКО ЛИЦЕ

Установяването и проверката на самоличността на физическото лице (Титуляр) се осъществява от представител на Регистриращия орган. Идентификацията може да се извърши и автоматизирано, чрез отдалечена проверка.

За установяване и проверка на самоличността на физическо лице се изисква то да представи документ за самоличност.

Физическото лице, което заявява издаване или управление на квалифицирано удостоверение, попълва и предава на Евротръст документи в съответствие с политиката на доставчика за издаване и управление на квалифицирани удостоверения. Данните за лицето могат да включват номер на мобилен телефон, имейл адрес, адрес по местоживеене и други. Физическото лице потвърждава достоверността на данните, чрез:

- Саморъчно поставен подпис върху документите пред служител на Регистриращия орган, в случай на лично предаване на документите;
- Нотариална заверка на документите, които се изпращат по поща до Регистриращия орган;
- Подписване на приложените електронни документите с валидно удостоверение за квалифициран електронен подпис по смисъла на Регламент (ЕС) № 910/2014;

Евротръст може да установи самоличността на физическо лице по реда, посочен по-горе, чрез използване на специализирано мобилно или друго приложение и след извършена автоматизирана идентификация на физическото лице или от служител на Евротръст. Когато се използва мобилното приложение на Евротръст се осъществява проверка на самоличност на физическите лица чрез система за автоматизирана видео идентификация чрез проверка на сканиран документ за самоличност и получаване на данни за неговата валидност от национална база данни с български документи за самоличност, както и чрез биометричен анализ на лицето със снимков материал, получен от националната база данни. При неуспешна

проверка се извършва идентификация от оператор по специална методология чрез видеоконферентен разговор. Проверката на представителната власт на едно физическо лице спрямо юридическо се извършва чрез проверка на данните за вписванията в съответните регистри към Агенцията по вписванията.

Евротръст извършва проверка на достоверността на информацията в попълнените документи, с всички законово позволени средства в съответните публични регистри.

Списък с изискуемите документи за физическо лице при издаване и управление на квалифицирано удостоверение се поддържа на сайта на Евротръст в интернет.

3.2.4 УСТАНОВЯВАНЕ НА САМОЛИЧНОСТ НА ФИЗИЧЕСКО ЛИЦЕ, УПЪЛНОМОЩЕН ПРЕДСТАВИТЕЛ НА ЮРИДИЧЕСКО ЛИЦЕ

За издаване на квалифицирано удостоверение на физическо лице (Титуляр), което е упълномощено от юридическо лице, упълномощеният представител се явява пред Регистриращия орган. Удостоверяването на информацията, която се съдържа в представените документи става чрез:

- заверка „Вярно с оригинала“ и саморъчен подпис върху документите пред служител на Регистриращия орган, в случай на лично предаване на документите;
- нотариална заверка на документите, които се изпращат по поща до Регистриращия орган;
- подписване на приложените електронни формати на документите с валидно удостоверение за квалифициран електронен подпис/печат;
- преглед и потвърждение, чрез използване на специализирано мобилно или друго приложение и след извършена надлежна идентификация на представляващото лице и/или юридическото лице от служител на Евротръст, както и чрез проверка на вписванията на представителната власт в официални регистри (към Агенцията по вписванията).

С проверката на идентичността на юридическо лице се цели да се докаже, че по време на разглеждане на заявката юридическото лице съществува и че представляващото лице, което кандидатства за квалифицирано удостоверение притежава представителна власт да поиска издаването.

3.2.5 ОСОБЕНИ АТРИБУТИ

Доставчикът може да включва в издаваното удостоверение особени атрибути, свързани с Титуляря, ако удостоверението се издава за конкретна цел по съответната политика.

Тази информация подлежи на проверка от Регистриращия орган.

Евротръст издава по искане на лице за нуждите на идентификация пред доверяваща се страна атрибутивно квалифицирано удостоверение за квалифициран електронен подпис „Eurotrust Qualified Natural Person Attribute Certificate for QES“ с кратък срок на валидност, съдържащо всички текстови реквизити от документа за самоличност, доколкото същите са предоставени от лицето към момента на регистрацията му като потребител.

3.2.6 НЕПОТВЪРДЕНА ИНФОРМАЦИЯ

Всяка информация извън задължително проверяваната, е непотвърдена информация.

Доставчикът може да включва в издаваното удостоверение и непотвърдена информация за Титуляря/Създателя, която не подлежи на проверка от Регистриращия орган. В този случай Евротръст не носи никаква отговорност за тази информация.

3.2.7 ДЕЙСТВИЯ НА УДОСТОВЕРЯВАЩИЯ ОРГАН

След успешна идентификация и проверка от Регистриращия орган на условията за издаване или управление на квалифицирано удостоверение, представител на Регистриращия орган потвърждава данните пред Удостоверяващия орган. Удостоверяващият орган публикува незабавно издаденото удостоверение в регистъра на удостоверенията и съответно информация за управлението му в Списъка със спрени и прекратени удостоверения (CRL).

В Евротръст единствено оперативният Удостоверяващ орган, издал квалифицирано удостоверение за електронен подпис/печат, може да прекрати действието на това удостоверение.

3.2.8 ПРОВЕРКА НА ПРИТЕЖАНИЕ НА ДОМЕЙН

При издаване на квалифицирани удостоверения за автентичност на уебсайт, Евротръст извършва проверка дали регистрацията и притежанието на домейна в публичните WhoIs бази данни съответства на лицето, което го е заявило. При липса на такава публична информация, потребителят сам предоставя информация, с която доказва притежанието на домейна и която

Евротръст проверява.

3.2.9 КРИТЕРИИ ЗА СЪОТВЕТСТВИЕ

Квалифицираните удостоверения издадени от Евротръст отговарят на изискванията на Регламент (ЕС) 910/2014 и се признават в Европейския съюз. Предвид трансграничната оперативна съвместимост на въведените с Регламент (ЕС) № 910/2014 формати на квалифицираните електронни подписи и печати квалифицираните удостоверения не надвишават задължителните изисквания, предвидени в Регламент (ЕС) № 910/2014. На национално равнище в квалифицираните удостоверения са включени специфични данни, като например ЕГН и други специфични данни при подадено искане от потребител, но Евротръст гарантира, че те не възпрепятстват трансграничната оперативна съвместимост и признаването на квалифицираните удостоверения и електронните подписи/печати в Европейската общност.

3.3 ИДЕНТИФИКАЦИЯ И ПРОВЕРКА ЗА САМОЛИЧНОСТ/ИДЕНТИЧНОСТ ПРИ ПОДНОВЯВАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ

Евротръст може да поднови валидно квалифицирано удостоверение, което не е прекратено в срока му на валидност, като генерира нова двойка ключове (Re-key). Евротръст не поддържа подновяване със запазване на съществуващата двойка ключове (Renewal) или със запазване на серийния номер.

Евротръст подновява текущо удостоверение на Титуляря/Създателя с нова двойка ключове (Re-key), само ако няма настъпили промени в удостоверената информация. Подновеното удостоверение има вписани в него нов сериен номер, нов публичен ключ, нов период на валидност и нов електронен подпис/печат от Удостоверяващия орган, като удостоверената в него информация се запазва.

След подновяване текущото квалифицирано удостоверение не се прекратява и остава валидно в срока му на валидност.

Съществуващите доказателства могат да бъдат използвани за повторно за потвърждаване на самоличността в зависимост от приложимото законодателство и предвид факта, че събраните доказателствата са останали валидни предвид изминалото време.

За идентификация и проверка на самоличност/идентичност на Титуляря/Създателя на квалифицираното удостоверение, което се подновява, не се изисква неговото лично явяване пред Регистриращия орган на Евротръст.

При настъпили промени в информацията за Титуляря/Създателя на квалифицирано удостоверение, текущото удостоверение не се подновява. Доставчикът издава ново квалифицирано удостоверение, като следва първоначална идентификация и проверка на самоличност/идентичност и прекратява незабавно текущото квалифицирано удостоверение.

Доставчикът съблюдава следните времеви ограничения и изисквания за идентификация при подновяване на квалифицирано удостоверение:

Период	Подновяване	Изисквания
До 30 дни преди изтичане срока на валидност на квалифицираното удостоверение, което не е прекратено и което няма промяна в удостоверената в него информация	чрез Re-key	➤ Да няма промяна в „DN“ на удостоверението ➤ Заявката за подновяване може да бъде извършена отдалечено
До 30 дни след изтичане срока на валидност на квалифицираното удостоверение, което не е прекратено и което няма промяна в удостоверената в него информация	чрез Re-key	➤ Да няма промяна в „DN“ на удостоверението ➤ Заявката за подновяване се подава на място (в Регистриращ орган)
Повече от 30 дни след срока на валидност на квалифицираното удостоверение	Не се подновява	

При отдалечено издаване и подновяване на квалифицирани удостоверения през мобилно приложение, подновяването е винаги с Re-key, като задължително се издава ново удостоверение. В този случай проверка за самоличност и идентификация не се извършва, но се прави автентификация на лицата.

Във връзка с изпълнение на изискванията на PSD2, при подновяване на удостоверение, в което има вписана информация, според изискванията на PSD2, Евротръст отново я

проверява, като при това той може да я поиска отново от съответния NCA. В случай, че NCA е определил правила за проверка на тези атрибути, Евротръст ги изпълнява и прилага.

3.4 ИДЕНТИФИКАЦИЯ И ПРОВЕРКА НА САМОЛИЧНОСТ/ИДЕНТИЧНОСТ ПРИ СПИРАНЕ НА ДЕЙСТВИЕТО НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ

Спиране на валидността на квалифицирани удостоверения е установена оперативна практика на Евротръст и се различава от прекратяване по това, че води до временно преустановяване на удостоверителната сила на дадено удостоверение. От съображения за правна сигурност Евротръст винаги ясно отбелязва статута на спиране на валидността на удостоверенията.

Евротръст е длъжен, чрез Регистриращия орган, да спре действието на валидно удостоверение при постъпило искане за спиране. Времето в системите, свързани със спиране и прекратяване на удостоверения се синхронизира спрямо UTC поне веднъж на 24 часа.

Доставчикът, чрез Регистриращия орган, не извършва идентификация и проверка за самоличност/идентичност на Титуляря/Създателя и спира незабавно действието на удостоверението.

При издадено отдалечено квалифицирано удостоверение, същото може да бъде спряно от мобилното приложение незабавно от потребителя, чрез предвидената за това функционалност.

3.5 ИДЕНТИФИКАЦИЯ И ПРОВЕРКА НА САМОЛИЧНОСТ/ИДЕНТИЧНОСТ ПРИ ПРЕКРАТЯВАНЕ НА ДЕЙСТВИЕТО НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ

Когато Евротръст прекрати действието на квалифицирано удостоверение, той отразява това в поддържаните от него бази данни своевременно, но не по-късно от 24 часа след като бъде получено искането. Отмяната става валидна веднага след като бъде публикувана.

Евротръст прекратява действието на удостоверение само след успешна идентификация и проверка за самоличност/идентичност на Титуляря/Създателя и уточнена причина за прекратяване. В противен случай удостоверението се възобновява.

При прекратяване през мобилното приложение, проверка за идентичност и самоличност не се извършва, предвид наличието на достъп на Титуляря до съответната

функционалност.

Евротръст предоставя на всяка доверяваща се страна информация относно прекратяване на действието на издадените от него квалифицирани удостоверения, при заявено желание за това. Тази информация се предоставя на разположение по всяко време и дори след срока на валидност на удостоверението.

3.6 ИДЕНТИФИКАЦИЯ И ПРОВЕРКА ЗА САМОЛИЧНОСТ/ИДЕНТИЧНОСТ СЛЕД ПРЕКРАТЯВАНЕ ДЕЙСТИЕТО НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ

Политиката и Практиката при предоставяне на квалифицирани удостоверителни услуги на Евротръст не допускат подновяване на квалифицирано удостоверение след прекратяването му.

Титулярят/Създателят на прекратено удостоверение може да поиска издаване на ново удостоверение.

Доставчикът, чрез Регистриращия орган, изпълнява първоначална идентификация и проверка за самоличност/идентичност на Титуляря/Създателя, ако той заяви ново удостоверение. Такава проверка не се извършва, ако потребителят заявява издаването на ново квалифицирано удостоверение от мобилното приложение, в което има активен профил.

4 ОПЕРАТИВНИ ИЗИСКВАНИЯ

Евротръст, чрез Регистриращия орган, в рамките на сключен Договор за квалифицирани удостоверителни услуги, предоставя следните оперативни процедури за квалифицирани удостоверителни услуги, приложими към квалифицираните удостоверения за електронни подписи/печати:

- регистрация на искане за издаване на квалифицирано удостоверение;
- обработка на искане за издаване на квалифицирано удостоверение;
- издаване на квалифицирано удостоверение;
- предаване на издаденото квалифицирано удостоверение;
- употреба на двойката ключове и на квалифицирано удостоверение;
- подновяване на квалифицирано удостоверение;
- спиране/възобновяване действие на квалифицирано удостоверение;
- прекратяване на квалифицирано удостоверение;

- статус на квалифицирано удостоверение.

Доставчикът, чрез Регистриращия орган, допуска Титуляря/Създателя да прекрати Договора за квалифицирани удостоверителни услуги между тях.

Времето в системите, свързани със спиране и прекратяване на удостоверения се синхронизира спрямо UTC поне веднъж на 24 часа.

4.1 ПОДАВАНЕ НА ИСКАНЕ ЗА ИЗДАВАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ

Подаване на искане за издаване на квалифицирано удостоверение е процес, при който потребителят подава до Регистриращ орган на Евротръст, в писмена или електронна форма, искане за издаване на квалифицирано удостоверение съгласно политиката на издаване на съответното удостоверение.

Искането може да се направи от Титуляря/Създателя или упълномощен представител на Създателя.

Потребителят регистрира искане за издаване на квалифицирано удостоверение в онлайн режим или чрез оператор в Регистриращия орган на Евротръст.

В онлайн режим исканията се подават, чрез мрежови протоколи като HTTP/HTTPS, S/MIME или TCP/IP.

Искане за издаване на квалифицирано удостоверение може да се подава и чрез мобилното приложение на Евротръст. В този случай, горните изисквания не се прилагат.

4.1.1 ЛИЦА, ПОДАВАЩИ ИСКАНЕ ЗА ИЗДАВАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ

Всяко лице, попадащо към една от следните категории лица, може да подава искане за издаване на квалифицирано удостоверение:

- физическо лице, което като потребител ще използва квалифицирано удостоверение;
- упълномощен представител на юридическо лице;
- служител на Евротръст, овластен със функции към Удостоверяващия орган на Евротръст;
- овластено лице към Регистриращи орган, независимо дали е външна организация

или е организационно обособено звено към инфраструктурата на Евротръст.

4.1.2 ОБРАБОТКА НА ИСКАНЕТО ЗА ИЗДАВАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ

4.1.2.1 ПОТРЕБИТЕЛСКИ УДОСТОВЕРЕНИЯ

Всички потребители на квалифицирани удостоверения със сключването на договор за удостоверителни услуги трябва да приемат задълженията и гаранциите, определени в него, както и в Политиката за предоставяне на квалифицирани услуги и тази Практика. За всеки потребител на квалифицирано удостоверение се извършва процес на регистрация, която включва следните стъпки:

- подаване на искане за издаване на квалифицирано удостоверение, което съдържа вярна и точна информация. Искането може да включва и допълнителна, непроверяема информация, част от която се удостоверява, а друга част улеснява контакта на Евротръст с Титуляря/Създателя;

- генерира се двойка криптографски ключове от Евротръст или потребителят сам осъществява това. Двойката криптографски ключове за квалифицирани удостоверения за КЕП/КЕПечат задължително се генерира в устройство за сигурно създаване на електронен подпис/печат, отговарящо на изискванията за ниво на сигурност, определено в Регламент (ЕС) № 910/2014;

- електронният формат на искането за издаване на квалифицирано удостоверение с информацията, която ще се включи в удостоверението е структура, подписана с частния ключ от генерираната двойка ключове в устройство за създаване на електронен подпис/печат, освен ако заявяването не се извършва отдалечено, през мобилното приложение на Евротръст;

- когато е необходимо, Регистриращият орган предоставя на Титуляря/Създателя или на упълномощено от него лице в защитен вид информация/код за достъп до частния ключ в устройство за създаване на електронен подпис/печат;

- в случай на самостоятелно отдалечено генериране на двойка ключове от потребителя, същият трябва да предостави публичния ключ на Евротръст чрез органа за регистрация и да докаже притежание на съответния частен ключ съответстващ на публичния ключ;

➤ Въз основа на одобрените искания за издаване и управление на квалифицирано удостоверение се осъществява сключването на договора с Евротръст.

4.1.2.2 УДОСТОВЕРЕНИЯ НА УДОСТОВЕРЯВАЩ И РЕГИСТРИРАЩ ОРГАН

Регистриращите органи, които предоставят квалифицирани услуги, които не са в организационната структура на Евротръст (външни Регистриращи органи), е необходимо преди да осъществяват тази дейност, да сключат съответен договор с Евротръст. В споразумението, освен правата и задълженията на двете страни, трябва да се включва и информация за самоличността на лицата участващи в Регистриращия орган и тяхното разрешение да представляват и двете страни по време на изпълнението на договора. Лицата, упълномощени да извършват тази дейност, следва да определят вида и предназначението на удостоверенията, преди тяхното издаване.

Ключовете и удостоверенията на Удостоверяващия орган могат да бъдат генерирани само по време на церемония по генериране на ключове, в която участват единствено лица, оправомощени от Евротръст.

4.1.2.3 ИСКАНЕ ЗА РЕГИСТРАЦИЯ НА ПОТРЕБИТЕЛИ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ

Искането за регистрация на потребители на квалифицирани удостоверителни услуги се подава до Регистриращия орган от физически, юридически или упълномощени лица и включва следната информация:

- пълно наименование на Титуляря/Създателя или на упълномощено лице;
- доказателства за представителна власт на Титуляря спрямо Създателя и на упълномощеното лице на Създателя;
- идентификатори: ЕИК (персонален идентификационен номер) и др.;
- пощенски адрес на лицето (страна, област, пощенски код, град или село, номер на сграда, име на улица или квартал, номер на факс);
- имейл адрес;
- вид на исканото квалифицирано удостоверение, вземайки предвид предназначението му;
- идентификатор на политиката за удостоверяване, въз основа на която се издава

удостоверението;

- наличие на частен ключ, съответстващ на публичен ключ;
- публичен ключ;
- допълнителна информация, заявена за включване в удостоверението, както и допустима непотвърдена такава;
- подписване на Договор за квалифицирани удостоверителни услуги и съгласие с условията на Политиката и Практиката при предоставяне на квалифицирани удостоверителни услуги от Евротръст.

В зависимост от съдържанието на удостоверението и неговия вид, някои от данните, посочени по-горе, може да отсъстват.

Ако двойката криптографски ключове е генерирана при Титуляря/Създателя, Регистриращият орган следва да провери предоставеното електронно искане за регистрация и изискванията за нивото на сигурност на устройството за създаване на електронен подпис/печат.

След успешна идентификация, проверка на самоличност на лицето, подало искане за квалифицирано удостоверение и при получаване на потвърждение от Регистриращия орган, искането за регистрация се изпраща на Удостоверяващия орган за издаване на удостоверение.

4.1.2.4 ПОДНОВЯВАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ, ГЕНЕРИРАНЕ НА НОВА ДВОЙКА КЛЮЧОВЕ И ПРОМЯНА НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ

Титулярят/Създателят или упълномощеното лице може да заяви подновяване на квалифицирано удостоверение при съблюдаване на времевите ограничения, изисквания и условия за подновяване.

Подновяването на квалифицирано удостоверение запазва информацията за Титуляря/Създателя или упълномощеното лице от текущото удостоверение, като в подновеното удостоверение се променя периода на валидност и серийния му номер.

Подновяване на квалифицирано удостоверение, което не е било прекратено в периода му на валидност, може да се изпълни чрез генериране на нова двойка ключове (Re-key). Евротръст не поддържа подновяване със запазване на съществуващата двойка ключове (Renewal) или със запазване на серийния номер.

Подновяването на квалифицирано удостоверение се предхожда от регистриране на искане за подновяване пред Регистриращия орган или онлайн.

Когато квалифицираното удостоверение е с изтекъл срок на валидност и искането за подновяване е съгласно посочените времеви ограничения и изисквания за идентификация при подновяване, Титулярят/Създателят или упълномощеното лице трябва да посети Регистриращия орган на Евротръст или да се идентифицира отдалечено.

Титулярят/Създателят или упълномощеното лице може да поднови многократно свое квалифицирано удостоверение.

Доставчикът не допуска използване на двойка ключове за електронен подпис/печат за период, по-голям от 3 (три) години.

Регистриращият орган ще поднови едно квалифицирано удостоверение за електронен подпис/печат, чрез Re-key при следните условия:

- удостоверението не е прекратено в срока му на валидност;
- Титулярят/Създателят или упълномощеното лице декларира, че няма промяна в удостоверената информация в текущото му удостоверение;
- искане за подновяване е направена до 30 дни преди или след изтичане на срока на валидност на удостоверението;
- строго изпълнява идентификацията и проверка за самоличност на потребителя и посочените времеви ограничения при подновяване;

Във всички случаи, когато има промяна в удостоверената информация за Титуляря/Създателя или упълномощеното лице на текущото удостоверение, последното не подлежи на подновяване, а Евротръст издава ново квалифицирано удостоверение.

Искането за подновяване на квалифицирано удостоверение, трябва да съдържа най-малко следното:

- уникалното име на Титуляря/Създателя или упълномощеното лице;
- вид на квалифицираното удостоверение/предназначение;
- идентификатор на политиката за удостоверяване въз основа на която удостоверението се издава;
- публичен ключ, който трябва да бъде удостоверен.

Една част или цялата част на данните, която се съдържа по-горе в искането за подновяване на квалифицирано удостоверение може да бъде удостоверена, чрез полагане на

електронен подпис/печат при условие, че абонатът притежава валиден към момента частен ключ за създаване на подпис/печат.

Доставчикът не допуска промяна в профила на удостоверенията за електронен подпис/печат.

Подновяване на квалифицирано удостоверение, заявено отдалечено през мобилното приложение на Евротръст не се подновява. След изтичането му се издава ново удостоверение. В този случай допълнителна идентификация не се извършва, а само проверка на актуалността на данните за самоличност.

4.1.2.5 ИСКАНЕ ЗА СПИРАНЕ И ПРЕКРАТЯВАНЕ НА УДОСТОВЕРЕНИЕ

Искане за прекратяване на квалифицирано удостоверение се подава от Титуляря/Създателя или упълномощено лице на място при Регистриращия орган или по електронен път.

В момента на прекратяване на квалифицирано удостоверение, Регистриращият орган уведомява потребителя за този факт (например по електронната поща).

Евротръст прекратява издадено от него удостоверение при:

- смърт или поставяне под запрещение на Титуляря/Създателя с прекратяване на представителната власт на Създателя;
- прекратяване на представителната власт на Титуляря спрямо Създателя;
- установяване на неверни данни при издаване на удостоверението;
- станала впоследствие невярна удостоверена информация;
- при промяна в удостоверена вече информация на Титуляря/Създателя;
- компрометиране на частния ключ;
- забавяне в заплащането на дължимо възнаграждение;
- искане за прекратяване от страна на Титуляря/Създателя, след като Доставчикът се увери в самоличността им и в представителната власт на Създателя. Когато се заявява спиране или прекратяване на квалифицирано удостоверение през мобилното приложение на Евротръст, проверка на самоличността не се извършва.

Доставчикът предприема незабавно прекратяване на действието на издадено удостоверение при всяко едно от посочените по-горе обстоятелства.

Доставчикът прекратява издадени от него удостоверения, ако прекрати дейността си

без да я прехвърлил на друг доставчик. В този случай същият уведомява потребителите си и прекратява удостоверенията с едномесечно предизвестие. В едномесечен срок от уведомяването, Евротръст възстановява на потребителите платената от тях сума, в размер съобразен с оставащия срок на договора за квалифицирана удостоверителна услуга. Когато е заявено квалифицирано удостоверение през мобилното приложение на Евротръст, абонаментът на потребителя се прекратява от момента, в който настъпи следващия период за подновяване.

Доставчикът може да спре и прекрати удостоверение на Удостоверяващ орган от инфраструктурата, ако са налице основателни съмнения за компрометиране на частния ключ на този орган.

При прекратяване на удостоверение на оперативния Удостоверяващ орган за издаване и поддържане на квалифицирани удостоверения за електронен подпис/печат, действието на всички издадени от него и валидни удостоверения се прекратява.

Само оперативният Удостоверяващ орган, издал квалифицирано удостоверение за електронен подпис/печат, може да прекрати действието на това удостоверение.

Ако прекратяването е следствие от операторска грешка или следствие от компрометиране на оперативен частен ключ на Евротръст, Доставчикът ще издаде за своя сметка еквивалентно потребителско удостоверение.

Услугите по управление на прекратяване и спиране на действието на удостоверение са на разположение денонощно, 7 дни в седмицата.

При срив в системата, услугите или други фактори, които са извън контрола на Удостоверяващия орган, Евротръст полага максимални усилия, за да гарантира, че услугата ще е достъпна максимум до 3 (три) часа.

Времето в системите, свързани със спиране и прекратяване на удостоверения се синхронизира спрямо UTC поне веднъж на 24 часа.

Във връзка с изпълнение на изискванията на PSD2, искане за спиране и прекратяване на удостоверение може да бъде подадено и от страна на NCA за издадени удостоверения с вписан в тях идентификационния код на платежната институция (authorisation number of the payment institution) на Доставчик на платежни услуги (Payment service provider/PSP), регистриран от същия NCA. При това NCA специфицира конкретния сериен номер на удостоверение, както и причината за искането за спиране или прекратяване. Възможните

причини за прекратяването са:

- прекратена е авторизацията на PSP;
- има промяна в идентификационния код на платежната институция на PSP;
- има промяна в името или идентификатора на NCA;
- прекратена е една или повече от ролите, удостоверени в издадено удостоверение.

Вменяването на нова роля на PSP не е причина за прекратяване на издадено удостоверение;

- прекратяването е изисквано по закон;
- други причини.

Ако NCA е собственик на специфична информация по PDS2 и съобщава на Евротръст, че тази информация е променена и че тя има отношение към валидността на издадено от Евротръст удостоверение, Евротръст проверява тази информация, независимо от съдържанието и формата ѝ, без да има задължението това да се случи в рамките на 24 часа.

Евротръст проверява автентичността и верността на информацията и исканията, отправени от NCA и при необходимост може да изпълни или откаже тяхното изпълнение, без да има задължението да информира за причината за приемането или отказа им.

4.2 ОБРАБОТКА НА ИСКАНЕТО

Евротръст приема искания за квалифицирани удостоверителни услуги, подадени индивидуално. Исканията могат да се подават онлайн през публично достъпно уеб базирано приложение и на място при Регистриращия орган. В случай, че документите се изпращат по пощата е необходима нотариална заверка на подписите. Искания могат да се приемат и през мобилното приложение на Евротръст.

Онлайн подаване през публично достъпно уеб базирано приложение се извършва с помощта на интернет страницата на доставчика на адрес: <https://www.evrotrust.com>. Потребителят, който е посетил подходящото място на сайта, попълва (в съответствие с инструкциите на този сайт) подходяща форма за кандидатстване и го изпраща на Регистриращия орган онлайн. Исканията за квалифицирани удостоверителни услуги се обработват от служител на Евротръст.

При подаване на искане при Регистриращ орган се изисква присъствие Титуляр/Създател или упълномощено лице. В случай на овластяване се изискват документи доказващи автентичност.

При подаване на искане през мобилното приложение на Евротръст, то се генерира автоматизирано, в удобен за потребителите диалогов режим.

4.2.1 ИДЕНТИФИКАЦИЯ И ПРОВЕРКА ЗА САМОЛИЧНОСТ

Дейностите по идентификация и проверка за самоличност на потребителите на Евротръст се осъществява от Регистриращия орган в съответствие с условията, посочени в настоящия документ.

4.2.2 ПРИЕМАНЕ ИЛИ ОТХВЪРЛЯНЕ НА ИСКАНЕ

4.2.2.1 ОБРАБОТКА НА ИСКАНЕ ОТ РЕГИСТРИРАЩИЯ ОРГАН

Всяко искане, подадено по електронен път или на хартия на Регистриращия орган, се обработва по следния начин:

- Регистриращият орган получава искането на Титуляря/Създателя или упълномощеното лице (на хартиен носител или в електронен формат);
- Регистриращият орган проверява дали лицето е заплатило такса за разглеждането на искането за издаване на квалифицирано удостоверение, при условие, че заплащането е предвидено в ценовата листа на Евротръст. При липса на такава такса, искането се отхвърля;
- Регистриращият орган проверява данните, посочени в искането, например личните данни на лицето и проверява за притежание на частен ключ;
- при положителна проверка Регистриращият орган потвърждава искането;
- ако оригиналното приложение съдържа невярна информация, то се отхвърля или коригира;
- в резултат на потвърждаването се издава удостоверение;
- Регистриращият орган може също така да провери и други данни, които не са посочени в искането, но се изискват от Евротръст.

Когато искането се подава през мобилно приложение, горните процедури не се прилагат. В този случай се проверява наличие на проверена самоличност на лицето и осъществена идентификация – автоматично или от оператор. При наличие на технологична възможност се извършва автоматизирана проверка в национални бази данни от документи за самоличност или в регистри на населението. Ако проверките са удовлетворителни Евротръст генерира двойката ключове отдалечено, в свой хардуерен криптомодул, криптира частния

ключ на потребителя с неговия ПИН и издава квалифицираното удостоверение.

4.2.2.2 ЗАЯВКА КЪМ УДОСТОВЕРЯВАЩИЯ ОРГАН ЗА ИЗДАВАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ

Евротръст може да откаже издаване на квалифицирано удостоверение на всяко лице без да има задължения или отговорност, ако потребителят посочва неверни данни в искането за издаване на удостоверение.

Евротръст може да направи отказ за издаване на квалифицирано удостоверение:

- ако потребителят не може да докаже, своите права върху предложения DN;
- в случай на съмнение, че потребителят фалшифицира данни или посочва неверни данни;
- ако потребителят ангажира значителни ресурси от Евротръст за обработка на повече искания отколкото са му необходими;
- потребителят не направи плащане за издаване на удостоверение, при условие че плащането е предвидено в ценовата листа на Евротръст;
- ако са налице други важни причини, които не са посочени по-горе.

Кандидатите, чиито искания са отхвърлени, впоследствие могат отново да подадат искане за издаване на квалифицирано удостоверение.

4.2.3 ИЗЧАКВАНЕ ИЗДАВАНЕТО НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ

Регистриращият орган на Евротръст незабавно, в присъствието на потребителя – Титуляр/Създател или упълномощено от него лице, изпълнява всички функции по проверка на направеното искане за издаване на квалифицирано удостоверение.

Удостоверяващият орган на Евротръст издава незабавно квалифицирано удостоверение след утвърждаване от Регистриращия орган на електронното искане за издаване.

Евротръст гарантира, че при получаване на искане за издаване или управление на удостоверение, Регистриращия орган ще разглежда искането и издаването на удостоверение незабавно, а при по-специални случаи в срок не по-дълъг от 3 дни от деня на подаването му.

Този период зависи главно от вида на квалифицираното удостоверение, пълнотата на подаденото искане и от технологичното време за координация в обслужването между

административни структури на доставчика, както и от времето за общуване между Евротръст и потребителя.

Когато се издава квалифицирано удостоверение през мобилното приложение на Евротръст, горните процедури не се прилагат и изчакване не се прави. В този случай удостоверението се издава незабавно, при наличие на успешни проверки за идентичност и самоличност.

4.3 ИЗДАВАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ

4.3.1 ОБРАБОТКА

След получаване на искане за издаване на квалифицирано удостоверение и съответно неговата обработката, същото се издава от Удостоверяващия орган.

Всички удостоверения се издават в реално време. Процедурата за издаване е следната:

- всяко искане за издаване на квалифицирано удостоверение, се записва и проверява от Регистриращия орган;
- само лицата, извършващи доверени роли имат достъп до оперативните действия на Регистриращия орган. Използването на акаунти защитава оперативните действия на много нива и позволява сигурно обработване на искането за издаване на квалифицирано удостоверение, включително за създаване на подходящо форматирана заявка за издаване на удостоверение от Удостоверяващия орган;
- обработената и форматирана заявка за удостоверение се изпраща на сървър за издаване на квалифицирано удостоверение съгласно избрания профил;
- Удостоверяващият орган генерира исканото удостоверение, подписва го с електронния подпис на Евротръст и го публикува незабавно в Публичния си регистър;
- Удостоверяващият орган подготвя отговор, съдържащ издаденото удостоверение и го предоставя на потребителя;
- Евротръст не издава удостоверения, чийто живот надвишава този на издаващия го удостоверяващ орган за подписване.

При отдалечено заявяване на удостоверение през мобилното приложение на Евротръст, същото се издава в реално време незабавно, в рамките на сесията по регистрация на потребителя.

4.3.2 ПРЕДОСТАВЯНЕ НА ИНФОРМАЦИЯ

Оторизиран представител на Регистриращия орган на Евротръст, незабавно известява Титуляря/Създателя или упълномощеното от Създателя лице за издаденото и публикувано удостоверение.

Оторизиран представител на Регистриращия орган на Евротръст изпраща до Титуляря/Създателя електронно известие по имейл с информация за името на Титуляря, вида на издаденото удостоверение за електронен подпис/печат уникалния сериен номер на квалифицираното удостоверение и периода му на валидност, освен в случаите, когато липсва имейл адрес.

Доставчикът доставя издаденото удостоверение на Титуляря/Създателя, респективно на упълномощеното от него лице, чрез Регистриращия орган.

В случаите когато Евротръст управлява частния ключ от името на потребителя пълното и точно удостоверение е налично за използване от титуляря, ако е необходимо. Не е необходимо удостоверението да е налично за използване веднага след издаването.

Оторизиран оператор на Регистриращия орган записва удостоверението на устройство за създаване на електронен подпис/печат, където е била генерирана двойката криптографски ключове за това удостоверение.

Тези правила се прилагат и при отдалечено издаване на квалифицирано удостоверение чрез мобилното приложение на Евротръст. В този случай уведомяването на Титуляря/Създателя става чрез изпращане на съобщение в самото мобилно приложение.

4.4 ПРИЕМАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ

4.4.1 ПОТВЪРЖДЕНИЕ ЗА ПРИЕМАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ

При получаване на квалифицирано удостоверение, потребителят е длъжен да провери съдържанието му, по отношение на точността на данните и наличието на публичен ключ съответстващ на частния ключ, който той притежава. Ако в удостоверението са вписани неверни данни, удостоверението трябва да бъде незабавно прекратено.

Ако Титулярят/Създателят възрази, че издаденото квалифицирано удостоверение съдържа грешки или непълноти в 3 (тридневен) срок от публикуването му в регистъра, Евротръст ги отстранява чрез издаване на ново удостоверение без заплащане на възнаграждение, освен ако се дължат на предоставяне на неверни данни. При липса на

възражение се смята, че съдържанието на удостоверение е прието.

Правилата в настоящата точка се прилагат както при издаване на удостоверение, така и при подновяване на удостоверение.

След процедура по приемане на квалифицирано удостоверение се приема, че потребителят е бил запознат с процедурите за издаване на удостоверение, описани в този документ.

С приемане на квалифицираното удостоверение, потребителят приема Практиката и Политиката при предоставяне на квалифицирани удостоверителни услуги.

4.4.2 ПУБЛИКУВАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ

Всяко издадено и прието удостоверение се публикува незабавно в регистъра на удостоверенията на Евротръст.

4.4.3 ИНФОРМАЦИЯ ЗА ДРУГИ СТРАНИ

След публикуването на издаденото удостоверение в регистъра на удостоверенията, то става достъпно без ограничение за всички заинтересовани страни след изпълнение на приложимите процедури за проверка на достъпа до него.

4.5 УПОТРЕБА НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ И НА ДВОЙКАТА КЛЮЧОВЕ

4.5.1 ОТ СТРАНА НА ТИТУЛЯРИТЕ/СЪЗДАТЕЛИТЕ

Титулярите/Създателите трябва да използват частните ключове и квалифицираните удостоверения:

- в съответствие с тяхното предназначение, посочено в настоящата Практика и в съответствие с ограниченията и целите за използване, вписани в самото приложение, както във връзка с атрибутите на самото удостоверение;
- в съответствие с допълнително споразумение между потребителя и Евротръст;
- само в рамките на срока на тяхната валидност;
- когато удостоверението е спряно, потребителят не трябва да използва частния ключ за създаване на електронен подпис/печат.

Титулярят/Създателят няма право да прави достояние частния си ключ на трети лица,

нито да предоставя носителя, върху който е персонализиран или начина на идентификация. Отговорността за опазването на тайната на частния ключ е на Титуляря/Създателя.

4.5.2 ОТ ДОВЕРЯВАЩИТЕ СЕ СТРАНИ

Доверяващите се страни, включително операторите в Регистриращия орган, трябва да полагат дължимата грижа при използване на публичните ключове и съответните им удостоверения:

- в съответствие с тяхното предназначение и вписани ограничения за използване, посочено в настоящата Практика, както и с оглед атрибутите на самото удостоверение;
- само след проверка на техния статус и проверка на електронния подпис на Удостоверяващия орган, издал удостоверението;
- до прекратяване на удостоверение;
- когато удостоверението е спряно, доверяващата се страна не трябва да приема публичния ключ.

4.6 ПОДНОВЯВАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ

Подновяване на квалифицирано удостоверение означава подмяна на валидно удостоверение с ново, без да се променя съществуващата информация в него, освен нов сериен номер, нова двойка ключове, нов срок на валидност и нов електронен подпис/печат на Удостоверяващия орган. То трябва да бъде предшествано от регистриране на искане за подновяване в подходяща форма, приета и одобрена от оператор в Регистриращ орган, проверена идентичност и коректност на подаденото искане.

4.7 ИЗДАВАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ С ГЕНЕРИРАНЕ НА НОВА ДВОЙКА КЛЮЧОВЕ

Нова двойка ключове се генерира от Евротръст, в случаите когато вече регистриран потребител поиска да му се генерира нова двойка ключове или нов потребител подаде искане за генериране на двойка ключове. Генерирането на нова двойка ключове се съпътства с

издаване ново квалифицирано удостоверение, потвърждаващо притежанието на новосъздадената ключова двойка.

Издаване и подновяване с Re-key трябва да се тълкува по следния начин:

- издаването на нова двойка ключове не се свързва с никакви валидни удостоверения и се използва от потребителите, за да получат удостоверение от всякакъв вид;
- отнася се до конкретно валидно удостоверение, посочено в искането. В следствие на това, новото удостоверение включва същото съдържание, като разликите са: нов сериен номер, нов публичен ключ, нов срок на валидност и нов електронен подпис/печат от Удостоверяващия орган.

Евротръст информира предварително потребителите си по имейл най-малко 14 дни преди изтичане срока на валидност на издадено удостоверение, когато това е възможно.

Процедурата по издаване на квалифицирано удостоверение с генериране на нова двойка ключове може да се прилага и към Удостоверяващия орган и към Регистриращия орган.

Процедурите по тази точка не се прилагат за квалифицирани удостоверения, издадени отдалечено, чрез мобилното приложение на Евротръст.

4.7.1 ОБСТОЯТЕЛСТВА, ПРИ КОИТО СЕ ПРИЛАГА ИЗДАВАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ С ГЕНЕРИРАНЕ НА НОВА ДВОЙКА КЛЮЧОВЕ

Едно потребителско искане за издаване на квалифицирано удостоверение с генериране на нова двойка ключове, предоставено пред Евротръст, може да се прилага ако:

- потребителят е същия;
- удостоверението е валидно в момента на подава на искането и не е отменяно преди това;
- потребителят изисква допълнително удостоверение от същия тип или от различен тип, но само в рамките на политиката за удостоверяване на валидното квалифицирано удостоверение.

4.7.2 КОЙ МОЖЕ ДА ПОИСКА АКТУАЛИЗАЦИЯ НА КЛЮЧОВА ДВОЙКА

Искането за издаване на квалифицирано удостоверение с генериране на нова двойка ключове се извършва единствено от Титуляр/Създател или упълномощено от него

лице.

4.7.3 АКТУАЛИЗАЦИЯ НА КЛЮЧОВА ДВОЙКА И ОБРАБОТКА НА ИСКАНЕТО

Издаване на квалифицирано удостоверение с генериране на нова двойка ключове за електронен подпис/печат се предхожда от регистриране на искане за подновяване пред Регистриращия орган на Евротръст.

Искането за подновяване на квалифицирано удостоверение, чрез електронна заявка се удостоверява с електронен подпис/печат, съответстващ на валидното удостоверение на Титуляря/Създателя или упълномощено от него лице.

В случай, че удостоверението, което се подновява е с изтекъл срок на валидност, Титулярят/Създателят или упълномощено от него лице трябва да посети Регистриращия орган на Евротръст или да се идентифицира отдалечено. Упълномощен оператор на Регистриращия орган строго следва изискванията за идентификация и установяване на идентичност и на условията за подновяване.

След успешна идентификация и проверка на условията за подновяване, Регистриращият орган потвърждава искането за подновяване пред оперативния Удостоверяващ орган на Евротръст.

След успешна електронна автентификация на Регистриращия орган, чрез оторизирания оператор, оперативния Удостоверяващ орган изпълнява потвърденото искане за подновяване на удостоверението.

При неуспешна идентификация и проверка на условията за подновяване, Регистриращият орган отхвърля искането за подновяване на удостоверението и известява потребителя за това свое действие. В такъв случай потребителя с отхвърлено искане за подновяване може да заяви издаване на ново удостоверение.

Подновяване по тази точка не се прилага за квалифицирани удостоверения, издадени отдалечено, чрез мобилното приложение на Евротръст.

4.7.4 ИНФОРМАЦИЯ ЗА ТИТУЛЯРЯ/СЪЗДАТЕЛЯ

Оторизиран представител на Регистриращия орган на Евротръст незабавно известява Титуляря/Създателя или упълномощено от него лице за подновения и публикувано удостоверение.

В случаите, когато искането е подадено по електронен път през публично достъпно уеб базирано приложение, Евротръст изпраща по електронен път (чрез електронна поща) информация за новото квалифицирано удостоверение: името на потребителя, типа квалифицирано удостоверение, уникален сериен номер и срока на валидност на подновеното удостоверение. Изпраща се и електронния адрес, от който може да се свали новото квалифицирано удостоверение.

Когато искането се подава на място, при Регистриращия орган, Титулярят/Съзателят или упълномощеното от него лице получава подновеното квалифицирано удостоверение, чрез оторизиран оператор на Регистриращия орган. Операторът го записва на устройство за създаване на електронен подпис/печат, в което е генерирана двойката криптографски ключове за квалифицираното удостоверение.

4.7.5 ПОТВЪРЖДЕНИЕ ЗА ПРИЕМАНЕ НА НОВО УДОСТОВЕРЕНИЕ

При получаване на ново квалифицирано удостоверение, Титулярят/Съзателят е длъжен да спазва изискванията по-горе.

4.7.6 ПУБЛИКУВАНЕ НА НОВО КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ

Евротръст, чрез оперативния Удостоверяващ орган публикува незабавно подновеното удостоверение в регистъра на удостоверенията.

4.7.7 ИНФОРМАЦИЯ ЗА ДОВЕРЯВАЩИ СЕ СТРАНИ

След незабавното публикуване на издаденото удостоверение в регистъра на удостоверенията, то става достъпно без ограничение за всички доверяващи се страни при изпълнение на съответните процедури за достъп до него.

4.8 ПРОМЯНА В КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ

4.8.1 ОБСТОЯТЕЛСТВА ЗА ПРОМЯНА В КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ

Промяна в квалифицирано удостоверение означава промяна в съдържанието на данните във вече издадено и публикувано квалифицирано удостоверение за електронен подпис/печат. При промяна в квалифицирано удостоверение се изисква задължително генериране на нова двойка ключове.

Промяната се третира по същия начин, както и издаването на ново квалифицирано удостоверение.

Евротръст не допуска промяна в профила на квалифицираните удостоверения за електронен подпис/печат.

Промяна не се допуска за квалифицирани удостоверения, издадени отдалечено, чрез мобилното приложение на Евротръст. Същите се прекратяват и на тяхно място се издават нови.

4.8.2 КОЙ МОЖЕ ДА ПОИСКА ПРОМЯНА НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ

Титуляр/Създател, упълномощено от него лице, друго свързано с тях лице или лице, което е източник или има връзка с вписани в удостоверението данни, може да поиска промяна на квалифицирано удостоверение при условие, че са изпълнени изискванията и условията, описани в този документ.

4.8.3 ОБРАБОТКА НА ИСКАНЕТО

Промяната на квалифицирано удостоверение за електронен подпис/печат се предхожда от подаване на искане за промяна от Титуляря/Създателя или упълномощено от него лице при Регистриращия орган на Евротръст.

Искането за промяна, чрез електронна заявка се удостоверява с електронен подпис/печат на Титуляря/Създателя, съответстващ на валидно квалифицирано удостоверение.

В случай, че удостоверението, което се променя е с изтекъл срок на валидност, Титулярят/Създателят или упълномощено от него лице трябва да посети Регистриращия орган на Евротръст или да се идентифицира отдалечено. Регистриращият орган строго следва изискванията за идентификация и установяване на идентичност и на условията за промяна на квалифицирано удостоверение.

След успешна идентификация и проверка на условията за промяна, Регистриращият орган потвърждава искането пред оперативния Удостоверяващ орган на Евротръст.

След успешна електронна автентификация на оторизирания оператор на Регистриращия орган пред оперативния Удостоверяващ орган, последният изпълнява

потвърденото искане за промяна на квалифицираното удостоверение.

При неуспешна идентификация и проверка на условията за промяна, Регистриращият орган отхвърля искането и незабавно известява потребителя за причината. В такъв случай потребителя с отхвърлено искане за промяна, може да поиска издаване на ново квалифицирано удостоверение за електронен подпис/печат.

4.8.4 ИНФОРМАЦИЯ ЗА ПОТРЕБИТЕЛЯ

Оторизиран служител на Регистриращия орган на Евротръст, незабавно известява Титуляря/Създателя или упълномощено от него лице за промененото и публикувано квалифицирано удостоверение.

Доставчикът изпраща до Титуляря/Създателя електронно известие (имейл) с името на Титуляря/Създателя, типа на квалифицираното удостоверение за електронен подпис/печат, уникалния сериен номер и срока на валидност на промененото удостоверение. Потребителят получава и електронна препратка, от която може да си свали промененото квалифицирано удостоверение.

Когато Титулярят/Създателят или упълномощеното от него лице посещава Регистриращия орган, потребителят получава новото удостоверение на място. Оторизиран служител на Регистриращия орган записва новото квалифицирано удостоверение на устройство за създаване на подпис/печат, в което е и генерирана двойката криптографски ключове за удостоверението.

4.8.5 ПОТВЪРЖДЕНИЕ ЗА ПРИЕМАНЕ НА НОВО КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ

При получаване на променено квалифицирано удостоверение, потребителят се ангажира да провери съдържанието му, особено за точността на данните и наличието на публичен ключ съответстващ на частния ключ, който той притежава. Ако удостоверението има някакви грешки, които не могат да бъдат приети от потребителя, удостоверението трябва да бъде незабавно прекратено.

Титулярят/Създателят или упълномощеното от него лице, може да възрази, ако издаденото удостоверение съдържа грешки или непълноти, в 3 (тридневен) срок от публикуването му в регистъра. Евротръст ги отстранява, чрез издаване на ново

квалифицирано удостоверение без заплащане на възнаграждение, освен ако се дължат на предоставяне на неверни данни. При липса на възражение се смята, че съдържанието на удостоверението е прието.

4.8.6 ПУБЛИКУВАНЕ НА НОВО КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ

Евротръст, чрез оперативния Удостоверяващ орган публикува незабавно промененото квалифицирано удостоверение в регистъра на удостоверенията.

4.8.7 ИНФОРМАЦИЯ ЗА ДОВЕРЯВАЩИТЕ СЕ СТРАНИ

Публичният ключ в квалифицираното удостоверение, съответстващ на държания от Титуляря частен ключ, е публично достъпен за всички доверяващи се страни.

Всяка доверяваща се страна, включително оператор в Регистриращ орган следва да използва публичния ключ и удостоверението на Титуляря/Създателя в съответствие с изискванията на означената в удостоверението политика.

Доверяващите се страни трябва да използват публичния ключ само след проверка на статуса на удостоверението и проверка на електронния подпис на Евротръст.

От особена важност е доверяващите се страни да не използват публичния ключ след прекратяване на удостоверението или в момент, когато то е спряно.

4.9 СПИРАНЕ И ПРЕКРАТЯВАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ

Спиране и прекратяване на валидността на квалифицирано удостоверение е установена оперативна практика на Евротръст. Те се изпълняват само през периода на валидност на удостоверението. Спирането води до временно спиране на действието на удостоверението. Прекратяването води до безвъзвратно спиране на действието на удостоверението и е необратим процес.

Ако удостоверението бъде прекратено след първоначалното активиране, то губи валидността си от момента на прекратяване и неговият статус не може да бъде възстановен при никакви обстоятелства.

Ако Евротръст спре или прекрати удостоверение, той регистрира тази промяна в своята база данни с удостоверения и публикува отменения статус на удостоверението своевременно, но във всички случаи в срок до 24 (двадесет и четири) часа след като бъде

получено искането. Спирането или прекратяването стават валидни веднага след като бъдат публикувани в регистъра на удостоверенията. Те винаги са ясно отбелязани с точна дата и час на промяна на статуса в съответния Списък със спрени и преустановени удостоверения (Certificate revocation list/CRL) и в Оργανа за валидация на издателя на удостоверението (Online Certificate Status Protocol/OCSP).

При прекратяване на удостоверението на оперативния Удостоверяващ орган за издаване и поддържане на квалифицирани удостоверения за електронни подписи/печати, действието на всички издадени от него и валидни удостоверения се прекратява.

Само оперативният Удостоверяващ орган, издал квалифицирано удостоверение за електронен подпис/печат, може да прекрати действието на това удостоверение.

Ако прекратяването е следствие от операторска грешка или следствие от компрометиране на оперативен частен ключ на Евротръст, довели до прекратяване на действието на удостоверението на оперативния Удостоверяващ орган, Доставчикът ще издаде за своя сметка еквивалентно квалифицирано удостоверение.

Услугите по управление на прекратяване и спиране на действието на квалифицирано удостоверение са на разположение денонощно, 7 дни в седмицата.

При срив в системата, услугите или други фактори, които са извън контрола на Удостоверяващия орган, Евротръст полага максимални усилия, за да гарантира, че услугата не липсва за период, по-дълъг от максималния период от време, който в случая е 3 (три) часа.

Евротръст предоставят на всички доверяващи се страни информация относно валидността или не на издадените от него квалифицирани удостоверения. Тази информация се предоставя на разположение по всяко време и дори след срока на валидност на удостоверението по автоматизиран надежден начин.

Времето в системите, свързани със спиране и прекратяване на удостоверения се синхронизира спрямо UTC поне веднъж на 24 часа.

4.9.1 ОСНОВАНИЯ ЗА ПРЕКРАТЯВАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ

Основна причина за прекратяване на квалифицирано удостоверение на потребител е загубата на контрол върху частния ключ или носителя, върху който е записан или дори съмнение за такава загуба. Обстоятелства съществуват, когато притежавания от потребителя частен ключ е извън неговия обег на сигурност, когато има съществено нарушение на

задълженията на Титуляря/Създателя, описани в договора между него и Евротръст, или изискванията на политиката и практиката при предоставяне на квалифицирани удостоверителни услуги не е спазена от потребителя.

Евротръст прекратява издадено от него квалифицирано удостоверение, при наличие на следните обстоятелства:

- когато информацията, вписана в удостоверението се е променила;
- когато има подозрение, че частният ключ, свързан с публичния ключ, съдържащ се в удостоверението е компрометиран - възникнал е неоторизиран достъп до частния ключ или има причина да се подозира за такъв достъп, загуба на частен ключ или наличие на причина да се подозира за такава загуба, кражба на частен ключ или наличие на причина да се подозира за такава кражба, случайно изтриване на частен ключ;
- потребителят реши да прекрати договора с Евротръст;
- смърт или поставяне под запрещение на Титуляря/Създателя с прекратяване на юридическо лице на Създателя;
- прекратяване на представителната власт на Титуляря спрямо Създателя;
- когато потребителят не отговаря на изискванията на приетата политика за удостоверяване;
- ако Удостоверяващия орган прекрати дейността си;
- ако потребителят дължи неизплатени такси за предоставяни квалифицирани удостоверителни услуги;
- когато надеждността и сигурността на частния ключ на Удостоверяващия орган е нарушена;
- когато потребител, който е служител на една организация прекрати договора си за работа и не върне използваната криптографска карта, на която се съхранява удостоверението и съответния частен ключ;
- други обстоятелства, свързани с неизпълнение на изискванията на Практиката при предоставяне на квалифицирани удостоверителни услуги.

При удостоверения, издадени за целите на изпълнение на изискванията по PSD2, искането за прекратяване на действието при промяна на регистрацията на лицето се отправя от и е отговорност на NCA. Евротръст проверява автентичността на това искане. В

допълнение Евротръст изисква NCA за използва имейл адрес: support@evrotrust.com, на който да изпраща исканията, свързани с промяната да срока на действие и прекратяване на тези удостоверения. Независимо от използвания от NCA формат на имейл съобщението, Евротръст винаги го проверява.

4.9.2 ОСНОВАНИЯ ЗА ПРЕКРАТЯВАНЕ НА УДОСТОВЕРЕНИЕ НА УДОСТОВЕРЯВАЩ ОРГАН

Удостоверение, което принадлежи на Удостоверяващия орган, може да бъде прекратено от неговия издаващ орган. Подобно прекратяване може да се появи в следната ситуация:

- когато Удостоверяващият орган има основания да смята, че информацията в издаденото удостоверение е невярна;
- когато частният ключ на Удостоверяващия орган или неговата информационна система са нарушени по начин, засягащ доверието на удостоверенията, издадени от този орган;
- когато Удостоверяващия орган съществено е нарушил задължение, произлизащо от настоящата „Практика при предоставяне на квалифицирани удостоверителни услуги“.

4.9.3 ЛИЦА, ЛЕГИТИМИРАНИ ДА ПОИСКАТ ПРЕКРАТЯВАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ

Следните субекти могат да подадат искане за прекратяване на квалифицирано удостоверение:

- потребител, който е Титуляр/Създател на удостоверение;
- упълномощен представител на Удостоверяващия орган (в случая на Евротръст тази роля е запазена за администратора по сигурността)
- Създател, който като работодател прекратява трудовия договор на свой служител, прекратява и удостоверението на Титуляря, който е негов подчинен. В този случай, работодателя информира незабавно своя подчинен;
- NCA;
- когато оператор от Регистриращия орган има съмнение относно достоверността на дадената информация от потребителя.

Когато едно юридическо лице поиска прекратяване на удостоверение на упълномощено от него лице (Титуляр), Удостоверяващия орган трябва да:

- проверява дали заявителя е упълномощен да поиска прекратяването;
- подава уведомление до Титуляря;

Искане за прекратяване на действието на квалифицирано удостоверение може да се подаде при Регистриращия орган на хартия, по телефон и онлайн. Когато потребителят подава на хартия искането за прекратяване трябва да се яви при Регистриращия орган. В случаите когато се поиска онлайн прекратяване се изисква искането да се подпише с валиден за момента електронен подпис/печат. Във всеки от случаите, удостоверението се спира временно за кратък период. Впоследствие се изисква явяване пред Регистриращия орган за изясняване на случая и потвърждаване на искането за прекратяване на квалифицираното удостоверение.

Титуляр може да инициира прекратяване на удостоверение от мобилното приложение на Евротръст, с активиране на съответна функционалност, когато удостоверението е издадено отдалечено. В този случай се счита, че Титулярят е идентифициран, предвид активирането на ПИН за достъп до приложението или чрез друг биометричен идентификатор.

4.9.4 ПРОЦЕДУРА ЗА ПРЕКРАТЯВАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ

4.9.4.1 ПРОЦЕДУРА ЗА ПРЕКРАТЯВАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ НА КРАЕН ПОТРЕБИТЕЛ

Прекратяване действието на квалифицирано удостоверение на краен потребител се предхожда от подаване на искане за прекратяване пред Регистриращия орган на Евротръст. Искането за прекратяване на удостоверение може да се регистрира електронно, само когато Титуляря/Създателя има (друго) валидно и достъпно за ползване квалифицирано удостоверение за електронен подпис/печат. В противен случай се прави искане на място предоторизиран оператор при Регистриращия орган.

При искане за прекратяване Регистриращия орган регистрира искането и започва процедура по проверката му.

Пред Регистриращия орган се представят доказателства за прекратяване на

действието на квалифицирано удостоверение. След преглеждане на доказателствата, Регистриращия орган решава дали да продължи процедурата по прекратяване или да откаже на потребителя искането за прекратяване на удостоверението. Регистриращия орган изработва и изпраща автоматизирана заявка до Удостоверяващия орган за разрешаване на процедурата по прекратяване.

Всяко искане за прекратяване на удостоверение трябва да съдържа неоспорими доказателства за потвърждение на прекратяването. Всички мотиви за прекратяване трябва да са заверени (подписани по електронен път или подписани на ръка).

Процедурата за прекратяване на квалифицирано удостоверение се извършва, както следва:

- Оторизираният оператор в Регистриращия орган незабавно, без да идентифицира потребителя, спира действието на удостоверението за гратисен период.

- Регистриращият орган строго следва изискванията за идентификация и установяване на автентичност на Титуляря/Създателя или упълномощено от него лице и причините за прекратяване. Във всички случаи, Титулярят/Създателят или упълномощено от него лице трябва да посети Регистриращия орган на Евротръст за последваща проверка на идентичността, респективно самоличността на потребителя или да се идентифицира отдалечено.

- След успешна проверка за самоличността на Титулярят/Създателят или упълномощено от него лице, Регистриращия орган, чрез оторизирания оператор подава обработена заявка до оперативния Удостоверяващ орган за прекратяване на удостоверение. След потвърждение от Удостоверяващия орган се изпълнява искането за прекратяване на удостоверението.

- При неуспешна идентификация и проверка на условията за прекратяване, Регистриращият орган отхвърля искането за прекратяване на удостоверението и незабавно известява Титулярят/Създателят или упълномощено от него лице, за причините за това.

- Потребител, с отхвърлено искане за прекратяване на квалифицирано удостоверение, може да подаде ново искане за прекратяване на удостоверението, след като отстрани посочените причини за отказа.

При прекратяване на удостоверение през мобилното приложение на Евротръст,

горните процедури не се прилагат. В този случай се приема, че искането е направено с активиране на съответна функционалност за прекратяване в приложението, а Титулярят е надлежно идентифициран, предвид знанието на ПИН кодът, с който е активирано приложението. След прекратяване на удостоверението, Евротръст, чрез своя оперативен Удостоверяващ орган, незабавно публикува прекратеното удостоверение в Списъка със спрени и прекратени удостоверения (CRL), като издава нов Списък и уведомява Титуляря/Създателя на прекратеното удостоверение.

Прекратено удостоверение не подлежи на възобновяване или на подновяване.

Достъп до искането за прекратяване и документацията със системните извадки от изпълнението на прекратяване на квалифицирано удостоверение имат оторизирани лица от персонала на Евротръст.

Ако удостоверение, се съхранява на електронна криптографска карта, при прекратяване на действието на квалифицираното удостоверение, картата може да бъде физически унищожена или сигурно заличена. Тази операция трябва да се извършва от притежателя на картата.

Евротръст препоръчва притежателят на картата да я съхранява по начин, който му пречи да бъде открадната, неупълномощено използвана или физически унищожена, а частния ключ да бъде изтрит.

4.9.4.2 ПРОЦЕДУРА ЗА ПРЕКРАТЯВАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ НА УДОСТОВЕРЯВАЩ ОРГАН ИЛИ НА РЕГИСТРИРАЩ ОРГАН

Удостоверение, което принадлежи на Удостоверяващ орган или на Регистриращ орган може да бъде прекратено от органа, който го е издал. В този случай оторизирани лица на органа представят искане директно на Евротръст

Евротръст също може да представи искане за прекратяване на удостоверение на Удостоверяващ орган или на Регистриращ орган.

4.9.5 ГРАТИСЕН ПЕРИОД НА ПРЕКРАТЯВАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ

Преди да прекрати действието на валидно квалифицирано удостоверение, Евротръст спира действието му в гратисен период. В рамките на този гратисен период Евротръст

обработка искането за прекратяване на квалифицираното удостоверение, като:

- извършва всички проверки за установяване на идентичността и проверка за самоличността на потребителя, подал искането;
- установява причините предизвикващи прекратяване на удостоверението;

В случай на непотвърдени причини или след изтичане на гратисния период, Евротръст възобновява действието на удостоверението;

Евротръст допуска действието на удостоверението да бъде възобновено преди да изтече гратисния период, единствено по изрично искане на Титуляря/Създателя или упълномощено от него лице.

Спиране на удостоверение не се допуска като политика, когато удостоверението е издадено отдалечено, чрез мобилното приложение на Евротръст. В този случай удостоверението незабавно се прекратява, без гратисен период и без възможност за възобновяване.

Информацията относно прекратените удостоверения се съхранява в база данни на Евротръст. Прекратените удостоверения се публикуват в Списъка със спрени и прекратени удостоверения (CRL) в рамките на необходимото технологично време, но за не повече от 3 часа.

Операторите на прекратени удостоверения от Удостоверяващия орган или от Регистриращия орган, както и засегнатите крайни потребители биват информирани автоматично за това прекратяване.

4.9.6 СРОК ЗА ОБРАБОТКА НА ИСКАНЕТО ЗА ПРЕКРАТЯВАНЕ

Искане за прекратяване на квалифицирано удостоверение се обработва от Евротръст без неоправдано забавяне.

4.9.7 ПРОВЕРКА НА СПИСЪКА СЪС СПРЕНИ И ПРЕКРАТЕНИ УДОСТОВЕРЕНИЯ (CRL)

Всяка Доверяваща се страна, при получаване на електронен документ, подписан с квалифициран електронен подпис/печат от Титуляр/Създател, е длъжна да направи проверка на статуса на квалифицираното удостоверение в актуалния Списък със спрени и прекратени удостоверения (CRL) или чрез проверка на текущия статус на удостоверението в реално

време чрез Органа за валидация на удостоверяващия орган.

Списъка със спрени и прекратени удостоверения, на който всяка доверяваща се страна може да направи справка се намира на уеб сайта на адрес: <https://www.evrotrust.com>.

Евротръст не носи отговорност за настъпили вреди и последствия от неизпълнение на посочените изисквания.

4.9.8 ЧЕСТОТА НА ИЗДАВАНЕ НА СПИСЪКА СЪС СПРЕНИ И ПРЕКРАТЕНИ УДОСТОВЕРЕНИЯ (CRL)

Евротръст, чрез своя оперативен Удостоверяващ орган, публикува на посочения в удостоверението уеб адрес нов актуален Списък със спрени и прекратени удостоверения (CRL), всеки път когато се прекрати действието на валидно удостоверение, издадено от този орган.

Доставчикът, чрез своя оперативен Удостоверяващ орган, актуализира своя Списък със спрени и прекратени удостоверения (CRL) поне веднъж на всеки 2 седмици, ако няма спиране или прекратяване на удостоверение през този период.

Срокът на валидност от поне 2 седмици важи за всеки публикуван нов актуален Списък със спрени и прекратени удостоверения (CRL) на оперативния Удостоверяващ орган.

4.9.9 МАКСИМАЛНО ЗАБАВЯНЕ НА ПУБЛИКУВАНЕТО НА CRL

Всеки Списък със спрени и прекратени удостоверения (CRL) се публикува без неоправдано забавяне, веднага след като той е създаден (обикновено това става автоматично в рамките на няколко минути).

4.9.10 ОНЛАЙН ПРОВЕРКА НА СЪСТОЯНИЕТО НА УДОСТОВЕРЕНИЕ

Евротръст осигурява квалифицирана услуга за проверка на състоянието на издадените удостоверения в реално време. Тази услуга се извършва въз основа на Протокол за онлайн проверка на статуса на удостоверение (OCSP), описан в RFC 2560. Използването на OCSP дава възможност да се придобие информация за състоянието на удостоверенията, без да се изисква проверка в Списък със спрени и прекратени удостоверения (CRL).

Моделът на работа на OCSP е на принципа „заявка – отговор“. Извършва се онлайн достъп до Органа за валидация през Интернет. Като отговор за всяка заявка, OCSP сървър, предоставя следната информация за състоянието на едно квалифицирано удостоверение:

- добро (good) - което означава положителен отговор на заявката и трябва да се тълкува като потвърждение на валидно удостоверение;
- прекратено (revoked) - което означава, че удостоверението е прекратено;
- непознато (unknown) - което означава, че удостоверението не е издадено от Удостоверяващ орган на Евротръст.

OCSP услугата генерира отговор, основан на база данни. OCSP отговора е валиден в продължение на 7 дни. За да се поддържа правилното изпълнение на системата, отговорите на OCSP са кеширани за предварително определено време (обикновено не повече от няколко часа).

4.9.11 ИЗИСКВАНИЯ ЗА ОНЛАЙН ПРОВЕРКА НА СЪСТОЯНИЕТО НА УДОСТОВЕРЕНИЕ

Проверка на статус на удостоверение в реално време (по OCSP протокол) може да се изпълни през Интернет чрез използване на OCSP протокола, който осигурява по автоматизиран, надежден, безплатен и ефикасен начин информация относно валидността или отмяната на издадените удостоверения.

Доверяващите се страни трябва да проверяват тази информация, на които те искат да разчитат. Евротръст не носи отговорност за настъпили вреди и последствия от неизпълнение на посочените изисквания.

4.9.12 СПЕЦИАЛНИ ИЗИСКВАНИЯ ПО ОТНОШЕНИЕ НА НАРУШЕНИЕ НА СИГУРНОСТТА НА КЛЮЧА

В случай на нарушаване на сигурността на частния ключ (неговото разкриване) на Удостоверяващия орган или други субекти, опериращи в рамките Евротръст, Доставчикът незабавно информира доверяващите се страни.

4.9.13 ОСНОВАНИЯ ЗА СПИРАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ

Евротръст, чрез своя оперативен Удостоверяващ орган, спира действието на валидно удостоверение при определени условия за гратисен период.

Доставчикът предприема незабавни действия по искането за спиране на удостоверение.

За времето, през което удостоверението е спряно, то се счита за невалидно и всички електронни подписи/печати, проверявани с това удостоверение са недействителни.

Спиране и възобновяване на удостоверение, издадено отдалечено, чрез мобилното приложение на Евротръст не се допуска. Навсякъде в този раздел и неговите подраздели е изключено спирането на такива удостоверения.

4.9.14 ЛИЦА, ЛЕГИТИМИРАНИ ДА ПОИСКАТ СПИРАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ

Евротръст спира издадено от него валидно квалифицирано удостоверение ако:

- постъпи искане на Титуляря/Създателя или упълномощено от него лице, без да е длъжен да се увери в самоличността или в представителната му власт;
- постъпи искане от лице, за което според обстоятелствата е видно, че може да знае за нарушения на сигурността на частния ключ;
- постъпи искане от Комисията за регулиране на съобщенията (КРС).

4.9.15 ПРОЦЕДУРА ЗА СПИРАНЕ И ВЪЗОБНОВЯВАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ

Спиране действието на квалифицирано удостоверение се предхожда от регистриране на искане за спиране пред Регистриращия орган.

- Искането за спиране на удостоверение може да се регистрира по електронен път или се подава на хартия пред оторизиран оператор в Регистриращия орган на Евротръст.
- Искането за спиране на удостоверение, по електронен път се удостоверява с електронен подпис/печат, съответстващ на валидното удостоверение на Титуляря/Създателя.
- Оторизираният оператор в Регистриращия орган незабавно, без да идентифицира потребителя, спира действието на удостоверението. Спирането на удостоверението се извършва, чрез временното му вписване в Списъка на спрени и прекратени удостоверения (CRL).

- След успешно удостоверяване на идентичност на оторизирания оператор в Регистриращия орган пред оперативния Удостоверяващ орган, последният изпълнява потвърдената заявка за спиране на удостоверението.
- Регистриращият орган не може да отхвърля искане за спиране.
- След спиране на удостоверението, Доставчикът, чрез своя оперативен Удостоверяващ орган незабавно публикува спряното удостоверение в Списъка на спрени и прекратени удостоверения (CRL), чрез издаване на нов Списък.
- След спиране на удостоверението, Доставчикът незабавно уведомява Титуляря/Създателя на спряното квалифицирано удостоверение.

4.9.16 ГРАТИСЕН ПЕРИОД НА СПИРАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ

Евротръст спира действието на квалифицирано удостоверение за електронен подпис/печат за гратисен период до уточняване на причините за спирането.

4.9.17 ВЪЗБНОВЯВАНЕ ДЕЙСТВИЕТО НА СПРЯНО УДОСТОВЕРЕНИЕ

Евротръст възобновява действието на спряно удостоверение:

- след като отпадне основанието за спиране, преди да изтече периода на спиране;
- по искане на Титуляря, след изясняване на причините за поисканото спиране;

След възобновяване на удостоверение, последното се счита за действително.

4.9.18 ПРОЦЕДУРА ЗА ВЪЗБНОВЯВАНЕ НА ДЕЙСТВИЕТО НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ

Регистриращият орган възобновява спряно удостоверение след като получи искане за възобновяване от Титуляря/Създателя и след успешна проверка за идентификация и проверка за самоличност.

Регистриращият орган незабавно възобновява спряно удостоверение след като изтече гратисния период на спиране.

Във всички случаи, процедурата по възобновяване изважда спряното удостоверение

от текущия Списък със спрени и прекратени удостоверения (CRL) и публикува нов списък.

4.10 ПРОВЕРКА НА АКТУАЛНОТО СЪСТОЯНИЕ (СТАТУСА) НА КВАЛИФИЦИРАНИТЕ УДОСТОВЕРЕНИЯ

4.10.1 ХАРАКТЕРИСТИКИ

Информация за състоянието на удостоверенията, издадени от Евротръст може да бъде получена в Списъка със спрени и прекратени удостоверения (CRL), публикуван на сайта на Евротръст в интернет, чрез Протокола за онлайн проверка на статуса на удостоверенията (OCSP).

Удостоверителните услуги за проверка на статуса на квалифицираните удостоверения са достъпни в режим 24/7/365 (непрекъснато действащи).

Евротръст поддържа статуса на вече издадените Квалифицирани удостоверения по време на периода на тяхното действие, както и след неговото изтичане.

4.10.2 ДОПЪЛНИТЕЛНИ ФУНКЦИИ

Услугата за онлайн проверка на актуалното състояние на удостоверенията чрез Протокола за онлайн проверка на статуса на удостоверенията (OCSP) е достъпна за всички видове квалифицирани удостоверения, както и за всички доверяващи се страни.

Интернет адреса (URL) на OCSP услугата е: <http://ca.evrotrust.com/ocsp>.

Услугата OCSP е задължителна за всички оперативни удостоверяващи органи и за SSL удостоверения, издадени от Евротръст.

За онлайн проверка на състояние на удостоверенията Евротръст прилага следните изисквания:

- Информацията за състоянието на прекратяване е достъпна след периода на валидност на удостоверенията;
- Евротръст не премахва от CRL прекратените удостоверения, след като те са изтекли. В CRL е включено разширението X.509 "ExpiredCertsOnCRL", както е определено в ISO/IEC 9594-8 /Препоръка ITU-T X.509;
- В случай, че Евротръст реши да прекрати CRL, той издава и публикува последния CRL със стойност на полето NextUpdate, както е определено в т. 6.3.9 от ETSI EN 319 411-1;
- Евротръст запазва целостта и наличността на последния CRL поне за период от 10

години;

- Евротръст не издава последен CRL, докато всички удостоверения в обхвата на CRL или не изтекат или бъдат прекратени;
- При предоставяне на услугата OCSP, отговорът на OCSP използва разширението ArchiveCutOff, както е посочено в IETF RFC 6960, с дата archiveCutOff зададена в СА удостоверението "notBefore" стойност на датата. Разширението ще бъде върнато в отговорите на OCSP само за изтекли сертификати.
- Когато СА удостоверението е на път да изтече, Евротръст може да изчисли последен OCSP отговор за всяко издадено удостоверение (независимо дали е прекратено или не), като чрез "nextUpdate" полето задава стойност "99991231235959Z".
- Евротръст документира точно в настоящата практика и Общи условия, как са изпълнени следните изисквания: а) периодът, през който е предоставена информацията за състоянието на прекратяване (т. 4.9); б) как се предоставя информацията за състоянието на прекратяване в случай на компрометиране на удостоверяващ орган (т. 4.9); в) как се предоставя информация за състоянието на спиране в случай на прекратяване на дейността на Евротръст (т. 5.9).

4.11 ПРЕКРАТЯВАНЕ НА ДОГОВОР ЗА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ ОТ ПОТРЕБИТЕЛ

Договорът за квалифицирани удостоверителни услуги между Евротръст и потребител се прекратява:

- след изтичане на срока на валидност на последното издадено квалифицирано удостоверение и потребителят не е предприел действия, за да актуализира своето удостоверение;
- когато квалифицираното удостоверение е било прекратено и потребителя не е предприел действия по издаване на друго удостоверение.

4.12 ДОВЕРИТЕЛНО СЪХРАНЕНИЕ НА ЧАСТЕН КЛЮЧ (ЕСКРОУ)

Частните ключове на Удостоверяващия орган на Евротръст или на потребителите, които са включени в удостоверителната йерархия на Евротръст са персонализирани върху преносими носители и не подлежат на доверително съхранение от Евротръст (ЕСКРОУ).

Частните ключове на потребители, които са заявили издаване на удостоверения отдалечено, чрез мобилното приложение на Евротръст, се съхраняват в криптиран в надеждна криптографска система (Hardware Security Module/HSM), сертифицирана за ниво на сигурност FIPS 140-2 Level 3.

5 КОНТРОЛ НА ФИЗИЧЕСКАТА И ОРГАНИЗАЦИОННА СИГУРНОСТ

В тази част на „Практиката при предоставяне на квалифицирани удостоверителни услуги“ се описват общите изисквания по отношение на контрола на физическата и организационна сигурност, както и дейността на персонала, използвани в Евротръст. Разглеждат се изискванията и процедурите за сигурност в момента на генериране на ключове, при идентификация и проверка за самоличност на потребителите, при издаване на квалифицирани удостоверения и тяхното управление, при одитиране на Евротръст и при създаване на архив.

5.1 КОНТРОЛ НА ФИЗИЧЕСКАТА СИГУРНОСТ

Мерките, предприети по отношение на физическата защита на Евротръст са елемент от разработената и внедрена в Евротръст Система за информационна сигурност, съответстваща на изискванията на стандартите ISO/IEC 27001, ISO 9001, ISO 22301, и ISO/IEC 20000-1.

Мерките свързани с физическата защита на информационните данни, технологичните системи, помещенията и свързаните с тях поддържащи системи са насочени към предотвратяване на:

- Евротръст контролира физическия достъп до съоръженията, чиято сигурност е от решаващо значение за предоставянето на удостоверителните услуги и свежда до минимум рисковете, свързани с физическата сигурност. Сигурността на системите за издаване и управление на удостоверения е съобразена с изискванията на международни стандарти и препоръки;
- Физическият достъп до компоненти на системата на Евротръст, чиято сигурност е от решаващо значение за предоставянето на удостоверителни услуги, е ограничен до упълномощени лица. Критичността на компонентите се идентифицира чрез оценка на риска. За оборудването в защитените и изолирани помещения на Евротръст е осигурена физическа

неприкосновеност. Установен е двуфакторен контрол на достъпа и денонощна въоръжена физическа охрана. Не е позволен достъп до шкафа с оборудването на повече от 2 (две) оторизирани технически лица на Евротръст. Всеки достъп до помещенията с критична инфраструктура се документира в специални журналы;

- Контролът се прилага, за да се избегнат загуби, щети или компрометиране на активи и прекъсване на бизнес дейностите. Овластените лица от персонала на Евротръст строго спазват разработените вътрешни процедури за достъп до различните зони с ограничен физически достъп;

- Контролът се прилага, за да се избегнат компрометиране на данни или кражба на средства за обработка на информация. Физическата защита на помещенията, в които се намира Евротръст са изградени от масивна и стабилна конструкция със здрави врати и ключалки. Защитата е реализирана от невъоръжена 24-часова охрана. В помещенията на Евротръст има Система за алармена сигнализация, Система за видеонаблюдение, Сигнално-известителна система и Система за контрол на достъпа;

- Компонентите, които са критични за сигурната работа на удостоверителните услуги са разположени в защитен периметър, с физическа охрана срещу проникване, контрол на достъпа и аларми за откриване на проникване;

- Евротръст конфигурира своите системи, като премахва или деактивира всички акаунти, приложения, услуги, протоколи и портове, които не се използват в неговата дейност;

- Евротръст предоставя достъп до защитени зони и зони с висока сигурност само на доверени роли;

- Root CA системата на Евротръст е в зона с висока степен на сигурност. Базовия удостоверяващ орган на Евротръст се намира в сертифициран дейта център.

Евротръст осигурява физическа защита и контрол на достъпа на помещенията, където има инсталирани критични компоненти в неговата инфраструктура:

- Квалифициран базов удостоверяващ орган – „Evrotrust RSA Root CA“;
- Квалифициран оперативен удостоверяващ орган – „Evrotrust RSA Operational CA“;
- Квалифициран оперативен удостоверяващ орган – „Evrotrust RSA QOperational CA 2024“;

- Квалифициран оперативен удостоверяващ орган – „Evrotrust RSA REG.KE

Operational CA 2025”;

- Квалифициран оперативен удостоверяващ орган - „Evrotrust Services CA”;
- Квалифициран удостоверяващ орган за проверка на статус на удостоверения, издадени от базовия орган (OCSP service) „Evrotrust RSA Validation”
- Квалифициран удостоверяващ орган за проверка на статус на удостоверения, издадени от оперативния удостоверяващ орган (OCSP service) „Evrotrust RSA QS Validation”;
- Квалифициран удостоверяващ орган за проверка на статус на удостоверения, издадени от оперативния удостоверяващ орган (OCSP service) „Evrotrust Services Validation”;
- Квалифициран удостоверяващ орган за проверка на статус на удостоверения, издадени от оперативния удостоверяващ орган (OCSP service) „Evrotrust RSA QOperational CA 2024 OCSP”;
- Квалифициран удостоверяващ орган на време - „Evrotrust TSA”;
- Регистри и уеб сайт на доставчика;
- Регистриращи органи.

Инфраструктурата на доставчика е физически и логически обособена и не се използва при други дейности, които „Евротръст Технолъджис” АД осъществява.

5.1.1 ПОМЕЩЕНИЯ И КОНСТРУКЦИЯ НА ПОМЕЩЕНИЯТА

Евротръст разполага със специално конструирани и оборудвани помещения с най-висока степен на контрол на физически достъп, в което се помещават Удостоверяващ орган на доставчика и всичките централни компоненти на инфраструктурата.

5.1.2 ФИЗИЧЕСКИЯТ ДОСТЪП

Физическата сигурност на системите за издаване и управление на удостоверения е съобразена с изискванията на международни стандарти и препоръки.

За оборудването в защитеното и изолирано помещение на Евротръст е осигурена физическа неприкосновеност. Установен е двуфакторен контрол на достъпа и денонощна въоръжена физическа охрана. Не е позволен физически достъп до критичното оборудване за повече от 30 (тридесет) минути на посещение. Не е позволен достъп до шкафа с оборудването на повече от 2 (две) оторизирани технически лица на Евротръст. Всеки достъп до

помещенията с критична инфраструктура се документира в специални журналы.

Физическата защита на помещенията, в които се намира оборудването на Евротръст и Регистриращия орган са изградени от масивна и стабилна конструкция със здрави врати и ключалки. Защитата е реализирана от невъоръжена 24-часова охрана. В помещенията на Евротръст има Система за алармена сигнализация, Система за видеонаблюдение, Сигнално-известителна система и Система за контрол на достъпа.

Всички системи се инспектират периодично.

Овластените лица от персонала на Евротръст строго спазват разработените вътрешни процедури за достъп до различните зони с ограничен физически достъп.

Достъпът до района на операторите и администраторите е ограничен и се прилага, чрез използването на система за смарткарта и контрол на достъпа.

В офисите на Евротръст на Регистриращите органи са обособени и отделени от останалите помещения. Съоръжени са с техника, позволяваща безопасно съхранение на данни и документи. Достъпът до тези зони се следи и ограничава до оторизирани лица, свързани с дейността на органа по регистрация (оператори на регистриращия орган, системни администратори) и техните клиенти.

5.1.3 КОНТРОЛ НА ДОСТЪП

Евротръст има въведена Политика за контрол на достъп, съобразена със следните изисквания:

- достъпът до системата е ограничен до упълномощени лица. Евротръст осигурява контрол на достъпа до чувствителна информация. Правата на достъп до конкретни обекти се определят от привилегиите и ролята, притежавани от служителите;
- Евротръст администрира потребителски достъп на оператори, администратори и системни одитори, прилагайки принципа на „най-малко привилегии“ при конфигуриране на правата за достъп. Това обикновено се отнася за персонал, назначен на доверени роли;
- системният администратор управлява потребителските акаунти и навременната промяна или премахване на достъп;
- достъпът до информацията и приложенията се ограничава в съответствие с Политиката за контрол на достъпа;
- технологичната система на Евротръст осигурява достатъчен контрол на

компютърната сигурност относно администрирането и дейността на служителите в съответствие с техните роли;

- Евротръст контролира използването на софтуера, като служителите преди да използват критични приложения свързани с услугата се идентифицират;

- служителите на Евротръст носят отговорност за своята дейност, което се удостоверява с журнали на събитията;

- Евротръст гарантира, че осигурява контрол на достъпа до чувствителна информация. Чувствителните данни са защитени от разкриване от неоторизирани потребители;

- Евротръст предоставя възможност за контрол и ограничаване на достъпа на идентифицирани лица до системата и потребителските обекти, които те притежават или са отговорни за тях. Евротръст изисква всеки потребител да се идентифицира и да бъде успешно удостоверен, преди да разреши каквито и да било действия от името на този потребител или роля, поета от потребителя. Повторното удостоверяване е задължително след излизане от системата. Има внедрени механизми за привилегированите потребители, които намаляват риска по време на удостоверена потребителска сесия и ако входното устройство на потребителя е оставено без надзор, след определен период на неактивност, се прекратяване потребителската сесия. Когато броят на неуспешните опити за удостоверяване от един и същ потребител достигне максималния брой разрешени опити, Евротръст предотвратява по-нататъшни опити за удостоверяване на потребителя до административна намеса за деблокиране на потребителя (или в рамките на определен период от време).

5.1.4 ЕЛЕКТРИЧЕСКО ЗАХРАНВАНЕ И КЛИМАТИЧНИ УСЛОВИЯ

Сървърният шкаф с критично оборудване се захранва от две независимите UPS системи и е екраниран срещу външни интервенции. Климатизацията в изолираното помещение поддържа постоянна температура на въздуха за нормалната работа на технологичната система.

Поддържа се външно електрическо подаване от дизелов агрегат, което е резервирано. В случай на срыв в главния електропровод системата превключва на аварийен източник на захранване (UPS и/или електроенергия). Работната среда в областта на компютърните

системи се следи непрекъснато и независимо от другите работни области.

Вентилационната система е специално предназначена за такъв клас помещения, като не допуска компрометиране на физическата и електромагнитна защита на това помещение, както и на нормалната работа на инсталираните компютърни компоненти.

Вътрешният Регистриращия орган на Евротръст е свързан с аварийната енергийна система на сградата.

5.1.5 НАВОДНЕНИЕ

За следене на влажността в помещенията с компютърни системи, както и в цялата сграда на Евротръст са монтирани сензори за отчитане нивото на влага. Тези сензори са интегрирани в системата за сигурност на сградата на Евротръст. Охраната и служителите на Евротръст са инструктирани и задължени при настъпване на евентуални опасности да уведомяват незабавно съответните служби, администратора по сигурността и системния администратор.

5.1.6 ПРЕДОТВРЯВАНЕ НА ПОЖАР И ЗАЩИТА ОТ ПОЖАР

Евротръст спазва всички норми за пожарна безопасност, като извършва дейност в съответствие с всички нормативни и стандартизационни изисквания в тази област.

Защитното помещение с критична инфраструктура се намира в сграда, в която са инсталирани: звукова и светлинна пожароизвестителна система, активна пожароизвестителна система с газ и стоп газ бутон при усложнени обстоятелства и евакуация. При пожар е предвидено изключване на подаването на електрическото захранване към съоръженията и потушаване на пожара с газ.

5.1.7 РАБОТА С НОСИТЕЛИ

Всички носители се обработват безопасно в съответствие с изискванията на схемата за класифициране на информация. Носителите, съдържащи чувствителни данни, когато престанат да бъдат необходими се обезвреждат безопасно. Всички носители съдържащи софтуер, нъжи на данни или одитна информация се съхраняват в огнеупорна каса в специално архивно помещение с въведен контрол на достъп. В помещението с архива на Евротръст има изградена система на физическа и логическа защита. Евротръст е предприело сериозни

мерки срещу случайно или умишлено увреждане на носителите на данни. Регистриращите органи са задължени да пазят и съхраняват актуалната информация, включително документите на потребителите на хартиен носител в сейф.

5.1.8 ИЗХВЪРЛЯНЕ НА ОТПАДЪЦИТЕ

Доставчикът е създал процедура за унищожаване на информацията и изхвърляне на отпадъците.

Хартиените и електронни носители, съдържащи евентуално значима информация за сигурността на Евротръст, след изтичане на определения съгласно вътрешните правила период на съхранение, се унищожават в специални устройства за нарязване.

Носителите на информация за криптографските ключове и ПИН/ПУК номера, използвани за тяхното съхранение, се раздробяват с подходящи устройства. Това се отнася за носителите, които не позволяват окончателно заличаване на съхранени данни и тяхното повторно използване.

В определени случаи, информацията от преносими носители се унищожава, чрез изтриване или форматиране на устройството без възможност за възстановяване.

5.1.9 СРОК НА УПОТРЕБА НА ТЕХНИЧЕСКИ КОМПОНЕНТИ

Експлоатационният срок на физическите елементи в състава на всички критични компоненти на инфраструктурата на Евротръст се съблюдава съгласно предписаните експлоатационни изисквания на производителя и след предвидения период на работа, те се извеждат от употреба.

5.2 ОРГАНИЗАЦИОНЕН КОНТРОЛ

Тази част от „Практиката при предоставяне на квалифицирани удостоверителни услуги“ представя списък на доверени роли, които могат да бъдат определени от персонала на Евротръст. Също така, тази част описва отговорностите и задълженията, свързани с всяка определена роля. Всички процедури, касаещи сигурността при издаването, администрирането и използването на квалифицирани удостоверения за електронен подпис/печат, се изпълняват от доверен персонал на Евротръст. Доставчикът поддържа достатъчен брой квалифицирани служители, които във всеки момент от осъществяването на

дейността му да осигуряват съответствие с действащото законодателство и вътрешните правила и норми на дружеството.

Евротръст прилага следните изисквания:

- Евротръст гарантира, че служителите и изпълнителите спазват изискванията за надеждност на дейността;
- Евротръст наема служители и, ако е приложимо, подизпълнители, които притежават необходимите експертни знания, надеждност, опит и квалификация, и които са преминали обучение относно сигурността и правилата за защита на личните данни, подходящи за дейността, която извършват;
- Служителите на Евротръст преминават периодично (поне на всеки 12 месеца) през обучение за повишаване на своите експертни знания, опит и квалификация. Обученията включват обучения по информационна сигурност, потенциални заплахи и добри практики за сигурност;
- На служителите, които нарушават политиките на Евротръст, се прилагат подходящи дисциплинарни санкции;
- Ролите и отговорностите по информационна сигурност са документирани в длъжностни характеристики;
- Евротръст определя надеждни роли, от които зависи сигурността на дейността по предоставяне на услуга за валидиране на подписи/печати;
- Ръководството на Евротръст определя отговорностите на доверените роли;
- Доверените роли се одобряват и приемат от ръководството;
- Служителите на Евротръст (както временен, така и постоянен) имат длъжностни характеристики, определени от гледна точка на ролите, които изпълняват с разделяне на задълженията в съответствие с правилото за най-малко привилегии. Чувствителността на позицията се определя въз основа на задължения, нива на достъп, квалификация и диплома;
- В длъжностните характеристики се включват изисквания за умения и опит. В тях се разграничават общите и специфични задължения;
- Служителите упражняват административни и управленски процедури и процеси, които са част от процедурите за управление на информационната сигурност на Евротръст;
- Ръководството притежава знания по отношение на предоставените

удостоверителни услуги, познание на процедурите за сигурност, опит в областта на информационната сигурност и оценка на риска, достатъчни за изпълнение на управленски функции;

- Всички служители на Евротръст, които имат доверени роли са освободени от конфликт на интереси, който би могъл да засегне безпристрастността на дейността на Евротръст;
- Доверените роли са описани в т. 5.2.1 от настоящия документ;
- Персоналът на Евротръст се назначава на доверени роли от висшето ръководство на принципа на „най-малка привилегия“ при достъп или при конфигуриране на привилегии за достъп;
- На персонала не се дава достъп до доверени функции, докато не бъдат извършени необходимите проверки. Евротръст изисква от свидетелство за съдимост.

За управлението на дейността на Евротръст се прилагат следните изисквания:

- Евротръст, посредством регулярно извършвани, както вътрешни така и външни проверки от независими организации, гарантира сигурност и надеждност на предоставяните удостоверителни услуги;
- Евротръст гарантира, че политиката и практиката при които работи са недискриминационни;
- Удостоверителните услуги са достъпни за всички лица, чиито дейности попадат в обхвата на приложимост на услугите и които се съгласяват да спазват задълженията си, както са посочени в политиките, практиките, договора и общите условия на Евротръст;
- Във връзка с риска от отговорност за нанесени щети в съответствие с член 13 от Регламент (ЕС) № 910/2014 Евротръст сключва подходяща застраховка за отговорност в съответствие с националното право;
- Евротръст разполага с финансовата стабилност и ресурси, необходими за работа в съответствие с настоящия документ;
- Евротръст има политики и процедури за разрешаване на жалби и спорове получени от потребители или доверяващи се страни относно предоставянето на услугите или други свързани с услугите дейности;
- В случаите, когато предоставянето на удостоверителни услуги включва

подизпълнители Евротръст сключва задължително договор.

5.2.1 ДОВЕРЕНИ РОЛИ

Подробно разпределение на функциите и отговорностите на персонала е разписано във вътрешните документи на Евротръст: длъжностни характеристики, щатно разписание и съответни вътрешни оперативни процедури.

Разпределянето на функциите се осъществява по такъв начин, че да бъде сведена до възможен минимум опасността от компрометиране, изтичане на конфиденциална информация или възникване на конфликт на интереси.

Евротръст поддържа квалифицирани служители на длъжности, които осигуряват изпълнението на задълженията му във всеки момент при осъществяването на дейността по издаване, поддържане и управление на квалифицирани удостоверения, в съответствие с нормативната уредба.

Доставчикът осигурява дейността си със собствен персонал, като за определени дейности съгласно Регламент (ЕС) № 910/2014, Евротръст може да привлича и външни лица.

Евротръст е разработил длъжностни характеристики за всяка една от доверените роли на персонала, както следва:

- администратор по сигурността - цялостна отговорност по управлението и изпълнението на процедурите по сигурност на системите: разработва политика по сигурността; предприема мерки за техническа защита на данните и системите; определя операционните мерки за сигурност; осъществява пряк контрол по отношение на спазването на изискванията за сигурност на информационните системи, като следи за спазването на процедурите за сигурност при инсталирането, конфигурирането, поддръжката и промените в информационните системи или мрежата.
- системен администратор - отговаря за инсталиране, конфигуриране и поддържане на надеждни системи за управление на услугите: възстановяване на системата при необходимост; извършване на преконфигурация на устройства и системи по повод реализация на нови услуги или решения; следене за техническото и софтуерно състояние на сървърите и сигнализиране за нередности;
- системен оператор - отговаря пряко за експлоатацията на надеждните

технологични системи на Евротръст и за създаване на резервно копие (backup) на системата; създаване и управление на удостоверения за квалифициран електронен подпис/печат, включително създаване на двойка ключове - частен и публичен за квалифициран електронен подпис/печат; използване на ефикасни технологии за осигуряване на ежедневната работа на системата; провеждане на изпитвания и проверки за безотказна работа и сигурност на системата; спазване на техническите изисквания за работа с устройствата и при установяване на техническа неизправност уведомяване на съответните длъжностни лица;

➤ Системен одитор – отговаря за съхранение на данни, архивиране и управление на регистрите на събития (по-специално за проверката на тяхната цялост) при извършване на вътрешни проверки, както и за съответствието на дейността с Регламент (ЕС) № 910/2014. Системният одитор контролира дейността на всички регистриращи органи, опериращи въз основа на възлагане от Евротръст.

5.2.2 ИЗИСКВАНИЯ ЗА РАЗДЕЛЯНЕ НА ОТГОВОРНОСТИТЕ

Служителите на Евротръст (както временен, така и постоянен) имат длъжностни характеристики, определени от гледна точка на ролите, които изпълняват с разделяне на задълженията в съответствие с правилото за най-малко привилегии. Чувствителността на позицията се определя въз основа на задължения, нива на достъп, квалификация и диплома

Евротръст изпълнява следните изисквания за разделяне на задълженията и областите на отговорност:

- ролите и отговорностите, както са описани в политиката за информационна сигурност на Евротръст, са посочени в длъжностни характеристики на служителите;
- доверените роли, от които зависи сигурността на дейността на Евротръст са ясно установени;
- Персоналът на Евротръст е официално назначен на доверени роли от висшето ръководство;
- Доверени роли се приемат от назначеното лице за изпълнение на ролята;
- доверените роли се изпълняват от различни служители;
- Евротръст гарантира, че всички служители с доверени роли нямат конфликт на интереси, който може да накърни тяхната безпристрастност;
- доверените роли са служители по сигурността, системни администратори,

системни оператори и системни одитори.

За определени удостоверителни услуги могат да се изисква прилагане на допълнителни специфични роли.

5.2.3 ИДЕНТИФИКАЦИЯ И ПРОВЕРКА ЗА САМОЛИЧНОСТ ЗА ВСЯКА РОЛЯ

Персоналът на Евротръст е подложен на идентификация и проверка за самоличност в следните ситуации:

- когато са включени в списък на лица с ограничен достъп до сгради на Евротръст;
- когато са включени в списък на лица с физически достъп до технологичната система и мрежови ресурси на Евротръст;
- когато са овластени да изпълняват конкретна възложена роля;
- създаване и възлагане на акаунт и парола в информационната система на Евротръст;

Всяко упълномощаване за изпълнение на определена роля изисква:

- ролята трябва да бъде уникална и пряко свързана с конкретната личност;
- не може да бъде споделена с друго лице;
- трябва да бъде ограничена до функцията, произтичаща от ролята и да се изпълнява от точно определен човек. Ролята се изпълнява, чрез предоставяне на софтуер, технологична система и достъп до операционната система на Евротръст. Правилното изпълнение на ролята изисква пряк контрол върху длъжността.

Операции, извършвани в Евротръст, които изискват достъп до споделени мрежови ресурси са защитени с въведени механизми за силна автентификация и криптиране на предаваните данни.

5.3 КОНТРОЛ НА ПЕРСОНАЛА

Персоналът на Евротръст се състои от достатъчен брой високо квалифицирани служители. Лицата, извършващи доверени роли имат необходимата професионална подготовка и опит, което гарантира спазване на изискванията за сигурност и технически норми за оценка на сигурността. Професионалните познания в областта на информационните системи, криптографията и инфраструктурата на публичните ключове дава възможност на служителите с доверени роли да изпълняват качествено своите служебни задължения.

Служителите на Евротръст преминават периодично през курсове за последващо допълнително обучение, отговарящо на съвременните изисквания в областта на дейност на Евротръст.

5.3.1 КВАЛИФИКАЦИЯ НА ПЕРСОНАЛА

Евротръст се уверяват, че лицето, което изпълнява доверена роля на Удостоверяващия орган или в системата на Регистриращия орган отговаря най-малко на следните изисквания за заемане на длъжността:

- завършило е най-малко средно образование (доколкото не се изисква друго за съответната длъжност);
- подписало е граждански или трудов договор, описващ неговата роля в системата и съответните отговорности;
- преминало е необходимата подготовка, свързана с обхвата на задълженията и задачите за неговата позиция;
- било е обучено в областта на защита на личните данни;
- подписало е споразумение, съдържащо клауза, относно защитата на чувствителната (от гледна точка на сигурността на Евротръст) информация и на конфиденциалност на данните на потребителите;
- не изпълнява задачи, които могат да доведат до конфликт на интереси с дейността на Евротръст.

5.3.2 ПРОЦЕДУРИ ЗА ПРОВЕРКА НА ПЕРСОНАЛА

Всеки нов служител на Евротръст, който изпълнява доверена роля, се проверява от Евротръст:

- за да се потвърди предишна заетост;
- за проверка на препоръки;
- за да се потвърди образователната степен;
- за да се провери свидетелство за съдимост;
- за да се провери документ за самоличност.

В случай, когато исканата информация не е на разположение (например, поради действащ закон), Евротръст използват други позволени от закона методи, които позволяват да се събере нужната информация.

Евротръст може да отхвърли кандидатурата, свързани с изпълнението на доверената роля или да предприеме действия срещу лице, което вече е заето и изпълнява доверена роля, ако се установи, че:

- е било подведено от кандидат или служител по отношение на исканите данни, по-горе;
- получи силно неблагоприятни или не много надеждни препоръки от предишни работодатели;
- получи информация за кандидата за наличие на криминално минало или негов служител е бил осъден с влязло в сила и валидно съдебно решение.

При наличие на някое от горните хипотези, по-нататъшните стъпки се извършват в съответствие с процедурите за безопасност на Евротръст и приложимото право.

5.3.3 ИЗИСКВАНИЯ ЗА ОБУЧЕНИЕ НА ПЕРСОНАЛА НА ЕВРОТЪРЪСТ

Персоналът, който изпълнява функциите и задачите, произтичащи от неговата заетост в Евротръст или заетост в Регистриращия орган (при наличие на външен Регистриращ орган), трябва да премине през следните обучения:

- „Практика при предоставяне на квалифицирани удостоверителни услуги“ от „Евротръст Технолъджис“ АД;
- „Политика при предоставяне на квалифицирани удостоверителни услуги“ от „Евротръст Технолъджис“ АД;
- разпоредби, процедури и документация, свързана със заеманата роля;
- технологии за сигурност и процедурите свързани със сигурността, използвани от Удостоверяващия орган и Регистриращия орган;
- системен софтуер на Удостоверяващия орган и Регистриращия орган;
- отговорности, произтичащи от роли и задачи, изпълнявани в системата;
- процедури, изпълнявани при отказ на системата или прекъсване на дейностите на Удостоверяващия орган.

5.3.4 ЧЕСТОТА НА ОБУЧЕНИЯТА И ИЗИСКВАНИЯ ЗА НАДГРАЖДАНЕ НА КВАЛИФИКАЦИЯТА НА СЛУЖИТЕЛИТЕ

Обученията, описани по-горе се провеждат регулярно. Тези обучения се допълват при промяна в националното законодателство, в сектора или при промяна в документацията и дейността на Евротръст.

5.3.5 СМЯНА НА РАБОТАТА

„Практиката при предоставяне на квалифицирани удостоверителни услуги“ от „Евротръст Технолъджис“ АД не предполага никакви изисквания в тази област.

5.3.6 САНКЦИИ ЗА ИЗВЪРШВАНЕ НА НЕРАЗРЕШЕНИ ДЕЙСТВИЯ

В случай на откриване или на подозрение за неоторизиран достъп, системният администратор заедно с администраторът по сигурността (служители на Евротръст) или единствено на системния администратор (служител на Регистриращия орган, при наличие на външен Регистриращ орган) може да прекратят достъпа на извършителя до Евротръст или системата на Регистриращия орган. По-нататъшните дисциплинарни действия се консултират с ръководството на Евротръст.

5.3.7 ДОГОВОР С ПЕРСОНАЛА

Лица или консултанти (например разработчици на софтуер или консултантски услуги) могат да сключват договор за изпълняване на доверени роли в Евротръст. В такива случаи, те отговарят на същите изисквания, приложими за служителите, назначени в Евротръст.

Съгласно сключен договор лицата или консултантите са подложени на същата процедура за проверка, както служителите на Евротръст.

5.3.8 ДОКУМЕНТАЦИЯ, ПРЕДОСТАВЕНА НА ПЕРСОНАЛА

Управлението на Евротръст и управлението на Регистриращия орган (в случай на външен Регистриращ орган) трябва да предоставят на своите служители достъп до следните документи:

- удостоверителни политики;
- удостоверителни практики;

- шаблони на искания, заявления и декларации;
- извлечения от документи, съответстващи на изпълняваната роля, включително и на всички спешни процедури;
- набор от отговорности и задължения, свързани с изпълняваната роля в системата.

5.4 ЗАПИСИ НА СЪБИТИЯ И ПОДДЪРЖАНЕ НА ЖУРНАЛИ

За ефективното управление и функциониране на Евротръст, всички събития, имащи съществено значение върху сигурността и надеждността на технологичната система, контрола върху персонала и потребителите, както и въздействието върху сигурността на предоставяните квалифицирани удостоверителни услуги, се записват.

Евротръст регистрира всички събития, свързани с жизнения цикъл на удостоверенията, както и всички събития, свързани с генериране и разпространение на удостоверения.

Всяка страна, свързана по някакъв начин с предоставяне на удостоверителни услуги, записва информацията и я управлява адекватно. Информационните записи съставят регистри на събитията и се съхраняват по начин, позволяващ оторизирани лица да имат достъп до тази информация (например при разрешаване на спорове между страни или откриване на опити за нарушаване на сигурността на Евротръст). Записаните събития се копират и архивират. Резервните копия се съхраняват в сейфове.

Когато е приложимо, регистрите на събития се създават автоматично. Ако не може да бъде създаден автоматично, записът се съхранява на хартия. Записите подлежат на одит.

Одиторският екип в Евротръст извършва редовни проверки за спазване на въведените механизми, контроли и процедури съгласно „Практиката при предоставяне на квалифицирани удостоверителни услуги“, Регламент (ЕС) № 910/2014 и действащото национално законодателство. Одиторският екип оценява ефективността на съществуващите процедури за сигурност.

5.4.1 ВИДОВЕ ЗАПИСИ

Евротръст създава записи за всяка дейност в рамките на своята инфраструктура. Архивните записи могат да бъдат криптирани и съхранени на носители, с цел предпазване от промяна или фалшифициране.

Такива записи са разделени в три отделни категории:

➤ записи на технологичната система – при инсталиране на нов или допълнителен софтуер; при стартиране на системите и приложенията в тях; при успешни опити за стартиране на и достъп до хардуерни и софтуерни PKI-компоненти (Public Key Infrastructure/Инфраструктура на публичния ключ“ на системите); генериране и управление на двойките ключове и удостоверения за удостоверяващите органи и компоненти в инфраструктурата на Евротръст; управление на криптомодулите; съдържание на издадените удостоверения; генериране и управление на двойките ключове и удостоверения на Потребителите; стартиране на системите и приложенията в тях; при опити за стартиране и достъп до хардуерни и софтуерни PKI-компоненти на системите; генериране на Списък със спрени и прекратени удостоверения (CRL); публикуване на издадени валидни удостоверения в регистъра на удостоверенията; конфигуриране на профили на удостоверения; статус на удостоверение в реално време; удостоверяване на време на представено съдържание;

➤ грешки - записите съдържат информация за грешки на нивото на мрежови протоколи; при спиране на системите и приложенията в тях; при неуспешни опити за стартиране и достъп до хардуерни и софтуерни PKI-компоненти на системите; при системни софтуерни и хардуерни сризове на системите и други аномалии в платформите;

➤ одити - записите съдържат информация, свързана с квалифицираните удостоверителни услуги, например: постъпили документи за регистриране с цел установяване на идентичност и проверка за самоличност; на искания за издаване, подновяване, спиране/възобновяване и прекратяване на удостоверения; вътрешни процедури за идентификация и регистрация; издаване на Списък на спрените и прекратени удостоверения (CRL) и т.н.

Записите включват информация свързана с:

- тип на събитието;
- идентификатори на събитие;
- дата и час на събитието;
- идентификатор или други данни, позволяващи определяне на лицето, което е свързано със събитието;
- дали събитието е свързано с успешен или грешен резултат.

Съхраняват се записи, създадени от комуникационните компоненти в

инфраструктурата.

Съхраняват се записи на стари и актуални версии на „Практика при предоставяне на квалифицирани удостоверителни услуги“ и „Политика при предоставяне на квалифицирани удостоверителни услуги“; шаблони на искания, заявки, инструкции за работа и др.

Достъп до информацията на записите имат само овластени лица от персонала на Евротръст.

5.4.2 СЪБИРАНЕ НА ДОКАЗАТЕЛСТВА

При събиране на доказателства, Евротръст прилага следните изисквания:

- Евротръст записва и поддържа достъпна за подходящ период от време, включително за след преустановяване на дейността си, цялата информация относно данните, издадени и получени по време на дейността си, с цел предоставяне на доказателства в съдебни производства и с цел осигуряване на непрекъснатост на услугата;
- Евротръст е предприел подходящи технически и организационни мерки срещу неразрешено или незаконно обработване на лични данни и срещу случайна загуба, унищожаване или увреждане на лични данни;
- Евротръст е регистрирано в Република България, на територията на Европа, и като такава, спазвайки европейското и национално законодателство, гарантира че личните данни се обработват в съответствие с Регламент (ЕС) 2016/679. В това отношение, предоставяйки удостоверителни услуги от разстояние, Евротръст предоставя достъп до своите услуги като обработва само тези идентификационни данни, които са адекватни, подходящи и не прекомерно;
- Запазва поверителността и целостта на текущите и архивирани записи относно работата на услугите;
- Документи, касаещи функционирането на услугите, се архивират изцяло и поверително в съответствие с добрите бизнес практики;
- Записите, отнасящи се до експлоатацията на услугите, се предоставят, ако се изискват с цел предоставяне на доказателства за правилното функциониране на услугите за целите на съдебното производство;
- Записва се точното време на значимите за управление на дейността събития, като управление на ключовете и синхронизация на часовник;

- Времето, използвано за записване на събития, както се изисква в одитните записи (audit log), се синхронизира с UTC на поне веднъж на ден;
- Записите, отнасящи се до услугите, се съхраняват за определен период от време, който е подходящ за предоставяне необходимите правни доказателства и както е записано в Общите условия и договор;
- Събитията се регистрират по начин, който не може лесно да бъде изтрит или унищожен, освен ако са надеждно прехвърлени към дългосрочни архиви в рамките на срока, в който те трябва да бъдат съхранявани.

5.4.3 ЧЕСТОТА НА СЪЗДАВАНЕ НА ЗАПИСИ

Информацията за електронните журнали се генерира автоматично.

С цел да се идентифицират възможни незаконни дейности администраторът по сигурността, системните администратори и одиторът, анализират информацията, най-малко веднъж в рамките на един работен ден.

Администраторът по сигурността има задължението да прави преглед и оценка на точността и пълнотата на регистрираните събития и да проверява съответствието с процедурите за сигурност на Евротръст.

Записите в регистъра на събитията се разглеждат в детайли най-малко веднъж месечно. Всяко събитие подлежи на обяснение и се описва в дневник на събитията. Процесът по преглед на дневника на събитията включва и проверка за неговото фалшифициране или промяна.

5.4.4 ПЕРИОД НА СЪХРАНЕНИЕ НА ЗАПИСИ

Журнали на записи на регистрирани събития се съхраняват във файлове на системния диск за най-малко 6 (шест) месеца. През това време те са достъпни онлайн или в процес на търсене от всеки оторизиран служител на Евротръст. След този период, записите се съхраняват в архивите.

Архивирани журнали се запазват в продължение на поне 10 години.

5.4.5 ЗАЩИТА НА АРХИВА

Архивът се подписва с електронен подпис и електронен времеви печат. Информацията от записите в логовете периодично се записва на физически носители, които се съхраняват в специален сейф, намиращ се в помещение с висока степен на физическа защита и контрол на достъпа.

Протокол от логове на събитията може да бъде преразгледан единствено от администратора по сигурността, системния администратор или одитора. Достъп до регистъра на събитията е конфигуриран по такъв начин, че:

- само упълномощени лица имат право на четене на записите в регистъра;
- само администраторът по сигурността може да архивира или изтрива файлове (след тяхното архивиране), съдържащи регистрираните събития;
- е възможно да се открие всяко нарушение на целостта;
- Евротръст гарантира, че записите не съдържат пропуски или подправени записи;
- лица без право да променят съдържанието на журналите, нямат достъп до тях.

Евротръст прилага процедурите за защита на регистрираните събития по такъв начин, че дори и след като журналите бъдат архивирани, е невъзможно да бъдат изтрети записи, преди да изтече периодът на поддържане на архива.

5.4.6 ПОДДЪРЖАНЕ НА РЕЗЕРВНИ КОПИЯ НА ЗАПИСИ НА СЪБИТИЯ

Поддържат се резервни копия от записите в логовете на системите, които се съхраняват надеждно. Тези копия са създават от овластени лица на Евротръст.

Процедурите за сигурност на Евротръст изискват регистрите на събития да бъдат подложени на резервно копиране (backup) в съответствие с утвърден график, но не по-малко от 4 пъти в годината.

5.4.7 СИСТЕМА ЗА УВЕДОМЯВАНЕ СЛЕД АНАЛИЗ НА ЗАПИСИ

Евротръст е разработил процедура за анализ на записи на събития, изпълнявани в системата, която позволява преглед на текущите събития и автоматично уведомява за заплахи или пробив в сигурността. В случай на дейности, имащи влияние върху сигурността на системата, администраторът по сигурността и системния администратор биват уведомявани автоматично. В останалите случаи, уведомлението се насочва само към системния администратор.

Когато се предава критична информация на упълномощени лица, от гледна точка на сигурността на системата, са предвидени ситуации, при които трансферът се извършва чрез други, подходящо обезпечени средства за комуникация, например мобилен телефон, електронна поща.

Компетентните органи имат задължението да предприемат съответните мерки за предотвратяване на откритата заплаха.

5.4.8 УЯЗВИМОСТ И ОЦЕНКА НА РИСКА

Евротръст класифицира и поддържа регистри на всички активи в съответствие с изискванията на ISO/IEC 27001. Съгласно „Политиката по сигурност“ на Евротръст се извършва анализ за оценката на уязвимост по всички вътрешен процедури, приложения и информационни системи. Изисквания за анализ могат, също така, да бъдат определени от външна институция, упълномощена да извършва одит на Евротръст.

Анализът на риска се извършва най-малко веднъж годишно. Решението да се пристъпи към анализ се извършва от Съвета на директорите.

Администраторът по сигурността контролира опазване на записите по сигурността в журналите, коректното архивиране

на резервните копия, дейностите, изпълнени в случай на заплахи и съответствието с настоящата Практика.

Евротръст изпълнява следните изисквания:

- Евротръст извършва оценка на риска, за да идентифицира, анализира и оценява рисковете при предоставяне на удостоверителни услуги, като взема предвид бизнес и технически въпроси;
- Евротръст избира подходящите мерки за третиране на риска, като взема предвид резултатите от оценката на риска. Мерките за третиране на риска гарантират, че нивото на сигурност е съизмеримо със степента на риска;
- Евротръст определя всички изисквания за сигурност и оперативни процедури, необходими за прилагане на избраните мерки за третиране на риска, както е документирано в политиката за сигурност на информацията и практиката при предоставяне на удостоверителни услуги;
- Ръководството на Евротръст редовно преразглежда и ревизира оценката на

риска.

5.5 АРХИВИРАНЕ

Информацията за значимите събития се архивира в електронен вид периодично.

Евротръст архивира всички данни и файлове, свързани с: информацията при регистрация; със сигурността на системата; всички искания, подадени от потребителите; цялата информация за потребителите; всички ключове, използвани от Удостоверяващите органи и от Регистриращия орган; и цялата кореспонденция между Евротръст и потребителите. На архивиране са подложени всички документи и данни, използвани в процеса на проверка на самоличността.

Доставчикът съхранява архива във формат, позволяващ възпроизвеждане и възстановяване.

5.5.1 ВИДОВЕ АРХИВИ

Евротръст управлява два вида архиви: хартиени и електронни.

5.5.2 ПЕРИОД НА СЪХРАНЕНИЕ НА АРХИВА

Архивираните данни (на хартия и в електронен вид) се съхраняват за период от 10 години. След изтичане на този период на съхранение, архивираните данни могат да бъдат унищожени.

5.5.3 ЗАЩИТА НА АРХИВНА ИНФОРМАЦИЯ

Евротръст съхранява архивираните записи по начин, който изключва неоторизирани и недоверени лица да имат достъп до тях. Информацията, която е архивирана по електронен път, е защитена срещу неоторизирано разглеждане, модифициране, изтриване или фалшифициране, чрез внедряването на Система за контрол на достъпа (посредством акаунти и пароли). За целите на архивирането се използват надеждни електронни носители, които не могат да бъдат лесно унищожени или изтрети през периода на съхранение.

За целите на сигурното съхраняване на архивните файлове в електронна форма те се

подписват с електронен подпис.

Електронните комуникации между локалните компоненти на инфраструктурата са защитени на база стандарта PKIX.

Отдалечените електронни комуникации са защитени и са базирани на стандарта PKIX.

Доставчикът преценява използването на пощенски и куриерски услуги и факс с Потребителите.

5.5.4 ВЪЗСТАНОВЯВАНЕ НА АРХИВИРАНА ИНФОРМАЦИЯ

От съществено значение за правилното функциониране на Евротръст е възможността резервните копия да бъдат напълно възстановени (например след срив в системата).

Подробни процедури за архивиране, създаване на копия и възстановяване на системата след аварии, са описани в техническата документация на Евротръст със статут „Вътрешна“. Тази документация е достъпна единствено за оторизиран персонал и проверяващи органи.

5.5.5 ИЗИСКВАНИЯ ЗА ОТБЕЛЯЗВАНЕ НА ВРЕМЕТО НА АРХИВИРАНЕ

Архивните данни се обезпечават с удостоверяване на точното време на подписването им.

5.5.6 СЪХРАНЯВАНЕ НА АРХИВА

Системата за събиране на архивни данни е вътрешна система за Евротръст. Изключение от това правило са архивите, които се събират от Регистрирания орган.

Архивната информация (на хартия и на електронни носители) се съхранява надлежно в специален сейф в помещение с висока степен на физическа защита.

5.5.7 ПРОЦЕДУРИ ЗА ДОСТЪП И ПРОВЕРКА НА АРХИВИРАНАТА ИНФОРМАЦИЯ

Достъп до архива е възможен само за оторизирани служители на Евротръст след успешно удостоверяване и потвърждение на правата за достъп.

Данните се проверяват периодично и се съпоставят спрямо оригиналните данни, с цел проверка на целостта на архивираната информация. Тази дейност се извършва под надзора на администратор по сигурността, като се водят записи за всеки етап от процедурата.

Резултатите от проверката се записват в съответните регистри на събитията.

Ако се установят повреди или модификации на оригиналните данни, щетите се премахват възможно най-бързо, съгласно вътрешните процедури и правила в Евротръст.

5.6 УПРАВЛЕНИЕ НА АКТИВИ

Евротръст управлява своите активи прилагайки изискванията, както следва:

- Евротръст е осигурило подходящо ниво на защита на своите активи, включително и на информационните активи;
- Евротръст поддържа инвентаризация на всички информационни активи и определя класификация в съответствие с оценката на риска.

5.7 ПРОМЯНА НА КЛЮЧ НА ДОСТАВЧИКА

Доставчикът може да промени ключа, съответстващ на издадено удостоверение, само като издаде ново удостоверение или поднови текущото.

Частният ключ на Удостоверяващ орган може да бъде променен в случай на:

- изтичане на срока на валидност на съпътстващото му удостоверение;
- въвеждане на нови услуги от Евротръст, които налагат промени в характеристиките на частния ключ (например промени свързани със сигурността и изискване за нови приложими криптографски комбинации).

При промяна на частният ключ на Удостоверяващия орган на Евротръст се спазват следните правила:

- Удостоверяващият орган, с чийто ключ се подписват потребителските удостоверения, и чийто ключ ще бъде променен, спира издаването на удостоверения 60 (шестдесет) дни преди момента, в който оставащия период на валидност на частния ключ се изравни с периодът на валидност на последното издадено удостоверение;
- Удостоверяващият орган, с чийто частен ключ се подписва Списъка със спрени и прекратени удостоверения (CRL) и чийто частен ключ ще бъде променен, продължава да публикува списъци, подписани със стария частен ключ до момента, в който изтече срокът на валидност на последното публикувано удостоверение.

5.8 КОМПРОМЕТИРАНЕ НА КЛЮЧОВЕ И ВЪЗСТАНОВЯВАНЕ СЛЕД АВАРИИ

Тази част от „Практиката при предоставяне на квалифицирани удостоверителни услуги“ описва процедурите, извършвани от Евротръст, при аварии (включително природни бедствия) за да се възстанови обслужването на потребителите. Тези процедури се извършват в съответствие с приет „План за възстановяване при бедствия“.

За случаите на настъпила авария или заплахата от настъпване на авария са разработени процедури за справяне с тези необичайни ситуации и за възстановяване на нормалната работа на Евротръст. При евентуални заплахи за настъпване на аварии се прави анализ на наличността на критичните ресурси необходими за възстановяване на системата. Правят се текущи оценки на разходите за възстановяване. Има процедури за аварии с информационните технологии и за аварии с бизнес процесите. Така например, в областта на информационните технологии, има изисквания за съхранение на системни хардуерни ресурси, изисквания за съхранение на системни данни, както и за съхранение на специфични (нестандартни) хардуерни ресурси, разпределяне на системни (работни) станции, интернет, интранет и т.н.

Този план се тества веднъж годишно и е обект на обучение от служителите на Евротръст.

Планът на Евротръст за възстановяване след бедствие е създаден с цел да осигури пълно възстановяване на всички функции на Евротръст в рамките на една седмица след криза, засегнала главните структури. Евротръст изпробва своето оборудване в структурата си, за да поддържа функциите на Удостоверяващия орган и Регистриращия орган след значима криза, която би спряла функционирането на цялата структура. Резултатите от тези проверки служат за оценъчни и планиращи дейности. Целта е при необходимост, например след значима криза, дейността на структурата на Евротръст да се възстанови колкото се може по-скоро.

5.8.1 ДЕЙСТВИЯ ПРИ АВАРИИ

Архивните данни, съдържащи информация за исканията за издаване, управление и прекратяване на удостоверения, както и записите на всички издадени удостоверения в базата данни се съхраняват на сигурно и надеждно място и са на разположение на Евротръст при поискване от упълномощените лица в случаи на възникване на авария.

За действия при аварии Евротръст е разработил „План за извънредни ситуации“, който

се проверява веднъж годишно.

Евротръст трябва да може да открие всеки възможен инцидент. След анализ на случилото се, целта е да се предотвратят бъдещи инциденти, основани на системни грешки или сризове на услуги и технологии. За да се извърши всичко това, Евротръст наблюдава всички системи и услуги без прекъсване (24x7), а също има на разположение телефон за информация и помощ, където потребителите могат да уведомяват за инциденти или неизправни услуги.

Планът посочва приблизителното време за откриване на всякакъв вид инциденти. Евротръст гарантира, че всеки потенциален инцидент може да бъде открит. Доставчикът е в състояние да разграничава реален инцидент от фалшива тревога. За тежките инциденти се съобщава на ръководството. Планът посочва приблизително време за уведомление и потвърждаване. Определя ролите и отговорностите. Дава оценка на вида инцидент, подходящо време за реакция и последващи действия. Събитията се записват. Документират се причините за инцидента и по какъв начин той се е отразил на ефективността на работата. Записват се предприетите мерки (време за реакция и време за възстановяване на услугата или системата и т.н.). Предлагат се подобрения. Този план посочва какъв тип архивиране се извършва, на какви интервали, къде да се съхранява информацията и структурата и т.н.

5.8.2 ИНЦИДЕНТИ, СВЪРЗАНИ СЪС СРИВОВЕ В ХАРДУЕРА, СОФТУЕРА И/ИЛИ ДАННИТЕ

Цялата информация при кражба на хардуер, софтуер и/или данни се предава на администратора по сигурността, който действа, в съответствие с вътрешни процедури, разработени от Евротръст.

Тези процедури са свързани с анализ на ситуацията, разследване на инцидента, мерки за минимизиране на последиците и недопускане на подобни инциденти в бъдеще.

В случай на сризове в хардуера, софтуера или в данните, Доставчикът уведомява потребителите, възстановява компонентите на инфраструктурата и приоритетно възобновява достъпа до предлаганите удостоверителни услуги, до уеб сайта си и до Списъка със спрени и прекратени удостоверения (CRL).

За такива случаи Евротръст е разработил „План за управление на инциденти“. Доставчикът има план за управление на всички инциденти, които засягат нормалното

функциониране на инфраструктурата на публичния ключ. Този план е в съответствие с План за бизнес, План за непрекъснатост и План за възстановяване при бедствия..

5.8.3 КОМПРОМЕТИРАНЕ ИЛИ СЪМНЕНИЕ ЗА КОМПРОМЕТИРАНЕ НА ЧАСТЕН КЛЮЧ НА УДОСТОВЕРЯВАЩИЯ ОРГАН НА ЕВРОТРЪСТ

Доставчикът полага дължимата грижа, за да поддържа непрекъсваемост и цялостност на удостоверителните услуги, свързани с удостоверенията, които издава, поддържа и управлява.

Доставчикът полага максимални грижи в рамките на възможностите и ресурсите си, да минимизира риска от компрометиране на ключовете на Удостоверяващите си органи вследствие на природни бедствия или аварии.

В случай на компрометиране или съмнение за компрометиране на частен ключ на Удостоверяващ орган на Евротръст, се предприемат следните действия:

- прекратява се незабавно удостоверението на оперативния орган;
- Удостоверяващият орган генерира нова двойка ключове и ново удостоверение;
- всички потребители на удостоверения се информират за случилото се незабавно, с помощта на средствата за масово осведомяване (информация на страницата на Евротръст) и електронна поща;
- информират се всички доверяващи се страни;
- удостоверението, съответстващо на компрометирания ключ се вписва в Списъка със спрени и прекратени удостоверения (CRL), заедно с подходяща причина за прекратяване;
- всички потребителски удостоверения издадени от удостоверението съответстващо на компрометирания частен ключ се прекратяват и записват в Списъка със спрени и прекратени удостоверение, като се посочва подходяща причина за прекратяването им;
- издават се нови удостоверения на засегнатите потребители;
- новите удостоверения на потребителите се издават за сметка на Евротръст (потребителите не дължат такса);
- извършва се незабавен анализ и изготвя доклад за причината за компрометирането.

Тези операции се извършват в съответствие с плана, разработен от Евротръст, за инциденти със сигурността. Този план се разработва от екип на Евротръст под ръководството

на администратора по сигурността и се одобрява от Съвета на директорите на Евротръст.

5.8.4 НЕПРЕКЪСНАТОСТ НА БИЗНЕСА И ВЪЗСТАНОВЯВАНЕ СЛЕД АВАРИИ

Евротръст управлява непрекъснатостта на бизнеса си прилагайки следните изисквания:

- Евротръст има създаден План за непрекъснатост на работата, който периодично тества и поддържа актуален, и който следва да се приеме в случай на бедствие. Този документ урежда подготовката и процесите, за да се гарантира запазването на дейността на Евротръст. Целта е постигане на приемственост в дейността на дружеството и защита на бизнеса, когато са налични големи прекъсвания на нормалните търговски операции;
- в случай на бедствие, при отказ на критични компоненти на технологичната система, включително хардуер, софтуер или компрометиране на частен ключ на Евротръст, операциите се възстановяват в рамките на забавянето, установено в плана за непрекъснатост. Разглеждат се причините за бедствието, взимат се подходящи мерки за отстраняването му и се набеязват мерки то да не се повтори.

Политиката за сигурност, която изпълнява Евротръст, взема под внимание следните заплахи, влияещи върху непрекъснатостта на предоставяните услуги:

- срив в компютърната система на Евротръст, включително срив в мрежовите ресурси - може да настъпи по случаен път;
- срив в софтуера, неизправност или спиране на достъпа до данни - може да настъпи чрез неподходящи приложения или зловреден софтуер от потребители (например вируси, червеи, троянски коне);
- загуба на важни мрежови услуги, свързани с интересите на Евротръст - може да настъпи при срив в електропреносната мрежа;
- компрометиране на част от мрежата, използвана от Евротръст за предоставяне на своите услуги.

За да се предотвратят или ограничат загубите от горните заплахи, като адекватна политика за сигурност, Евротръст предприема следното:

- всички Титуляри/Създатели и доверяващи се страни да бъдат информирани,

възможно най-бързо и по начин, който е най-подходящ за съществуващото положение;

- регулярно се създават и архивират копия на всички компоненти от инфраструктурата на Евротръст, които се съхраняват на добре защитено и безопасно място;
- периодично се създава резервно копие на базата данни, което включва всички подадени искания, издадени, подновени и прекратени удостоверения. Резервните копия се архивират и съхраняват на добре защитено и безопасно място;
- периодично се създава резервно копие на всеки сървър;
- частните ключове на Евротръст са разделени в съответствие с процедурите за сигурност и чрез тайно споделяне. Те се държат от доверени лица на сигурно и защитено място;
- подмяната на ресурсите се осъществява по начин, който позволява възстановяване на най-новите данни.

Процедурите за възстановяване на системата след аварии са тестват върху всеки компонент на технологичната система на Евротръст най-малко веднъж годишно. Тези тестове са част от вътрешния одит.

Актуализация на софтуера е възможна само след провеждане на интензивни тестове в тестова среда и действия в строго съответствие с описаните процедури на Евротръст. Всяка промяна в системата изисква съгласие и приемане от администратора по сигурност.

При всяко възстановяване на системата след бедствие, администраторът по сигурността или системният администратор изпълняват следното:

- ако анализът на риска идентифицира информация, изискваща двоен контрол за управление, например ключове, тогава за възстановяването се прилага двоен контрол;
- променят всички използвани преди това пароли;
- премахват всички права за достъп до ресурсите на системата;
- променят всички кодове и ПИН номера, свързани с физическия достъп до съоръженията и компонентите на системата;
- ако възстановяването от аварията включва преинсталация на операционната система и помощен софтуер, всички IP адреси от системата и нейните подмрежи се променят;
- преглед на анализ на причините за бедствията.

5.9 ПРЕКРАТЯВАНЕ НА ДЕЙНОСТТА НА ЕВРОТРЪСТ

Задълженията, описани по-долу, са разработени, за да минимизират прекъсванията в дейността на потребителите и доверяващите се страни, произтичащи от решението на Евротръст да преустанови работа.

5.9.1 ПЛАН ЗА ПРЕКРАТЯВАНЕ НА ДЕЙНОСТТА

Евротръст е създадо План за прекратяване на дейността за осигуряване на непрекъснатост на обслужването и конкретни сценарии към него в съответствие с изискванията на *Наредба за отговорността и за прекратяването на дейността на доставчиците на удостоверителни услуги* и следните изисквания:

- Евротръст е предприел мерки за свеждане до минимум на потенциални прекъсвания на удостоверителните услуги, които ползват потребители и доверяващи се страни, в резултат на прекратяването на дейността на дружеството. По-специално Евротръст осигурява непрекъсната поддръжка на информацията, необходима за проверка на коректността на удостоверителните услуги;
- Евротръст има актуален План за прекратяване;
- преди да прекрати услугите си, Евротръст информира всички заинтересовани страни, потребители, доверяващи се страни, доставчици, подизпълнители или други страни, с които има споразумения и съответните надзорни органи;
- преди да прекрати услугите си, Евротръст прекратява разрешението на всички подизпълнители (при наличие на такива) да действат от негово име при изпълнение на каквито и да било функции, свързани с процеса на издаване на удостоверителни токени;
- преди да прекрати услугите си Евротръст прехвърля задълженията си на надеждна страна за поддръжане на цялата информация, необходима за предоставяне на доказателства за неговата дейност за разумен период от време, освен ако се докаже, че не притежава такава информация;
- преди да прекрати услугите си, Евротръст унищожава или изтегля от употреба по начин, по който не могат да бъдат извлечени, своите частни ключове, включително резервни копия (при наличие);
- преди да прекрати услугите си, когато е възможно, Евротръст предприема мерки за прехвърляне на предоставяните удостоверителни услуги за съществуващите си

потребители на друг доставчик на квалифицирани удостоверителни услуги;

- Евротръст има застраховка за покриване на разходите, доколкото това е възможно, в случай че фалира или по други причини не е в състояние да покрие разходите, но в рамките на ограниченията на приложимото законодателство по отношение на несъстоятелността;
- Евротръст поддържа или прехвърля на надеждна страна своите задължения да предоставя на разположение публичните или удостоверителни токени на доверяващите се страни за разумен период от време.

5.9.2 ИЗИСКВАНИЯ, СВЪРЗАНИ С ПРЕХОДА ДО ПРЕКРАТЯВАНЕ НА ДЕЙНОСТТА НА ДОСТАВЧИКА

Преди удостоверяващия орган да прекрати услугите си, той е длъжен да:

- уведомява Органа по надзор за своето намерение да прекрати услугите си, в случай на иск за обявяване на дружеството в несъстоятелност, обявяване на дружеството за недействително или за друго искане за прекратяване, или за започване на процедура по ликвидация. Уведомлението следва да бъде направено 4 (четири) месеца преди договорената дата на прекратяване;
- уведоми (най-малко 4 месеца преди това) своите потребители за решението да прекрати предоставяните от него услуги;
- промени статуса на своите удостоверения;
- прекрати всички удостоверения на потребителите в рамките на обявения период за прекратяване на дейността;
- уведоми всички свои потребители за преустановяване на услугите;
- прави търговски разумни усилия, за да сведе до минимум нарушаването на интересите на потребителите;
- извършва необходимите действия, за да може Органа по надзор да поддържа Списъка със спрени и прекратени удостоверения (CRL).

Ако Регистриращ орган като външна организация, е взела решение за прекратяване на представителството на Евротръст по повод предоставяни удостоверителни услуги, той е длъжен да:

- уведоми Евротръст за своето намерение да прекрати дейността. Уведомлението

следва да бъде направено 4 (четири) месеца преди договорената дата на прекратяване;

➤ предава на Евротръст цялостната документация, свързана с обслужването на потребителите, включително архива и данните за одит.

5.9.3 ПРЕКРАТЯВАНЕ НА ДЕЙНОСТТА НА УДОСТОВЕРЯВАЩ ОРГАН

При прекратяване на дейността на удостоверяващ орган, Евротръст извършва следното:

➤ Следва актуализиран и одобрен от ръководството план и сценарий за прекратяване на дейността на удостоверяващ орган. Информирането може да се извърши чрез имейл или чрез публикуване;

➤ уведомява потребителите, Органа по надзор и третите страни за прекратяването на дейността на своя удостоверяващ орган. Информацията се предоставя чрез имейл или чрез публикуване на сайта на Евротръст;

➤ прекратява разрешението на всички лица, които имат договорни дейности да извършват дейности, свързани конкретния удостоверяващ орган;

➤ преди прекратяване на дейността на удостоверяващия орган, в разумен срок, прехвърля задълженията си по поддържане на цялата информация, необходима за предоставяне на доказателства на надеждна страна;

➤ преди да прекрати дейността, частните ключове, включително резервните копия, биват унищожени или изтеглени от употреба по такъв начин, че личните ключове да не могат да бъдат извлечени;

➤ при възможност прехвърля дейността си на друг квалифициран доставчик;

➤ Евротръст прилага мерки за покриване на разходите в случай на банкрут или поради други причини за прекратяване на действието на удостоверяващ орган. В случай, че не е в състояние да покрие разходите сам е предвидил мерки в рамките на приложимото законодателство;

➤ променя статуса на оперативното удостоверение;

➤ прекратява издаването нови удостоверения, но продължава да управлява активните удостоверения до края на тяхното действие;

➤ прави търговски разумни усилия, за да се сведе до минимум нарушаването на интересите на потребителите.

Евротръст следи и не допуска издаване на удостоверение за срок, по-дълъг от валидността на удостоверяващия орган, който го е издал.

5.9.4 ПРЕХВЪРЛЯНЕ НА ДЕЙНОСТ КЪМ ДРУГ ДОСТАВЧИК НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ

За да се осигури непрекъснатост на издаване на квалифицирани удостоверителни услуги за потребителите, Евротръст може да подпише споразумение с друг квалифициран доставчик на удостоверителни услуги. В този случай, Евротръст:

- уведомява Органа по надзор за намерението си, не по-късно от 4 месеца преди датата на прекратяване и прехвърляне на дейността;
- полага всички усилия и грижи, за да продължи действието на издадените потребителски удостоверения;
- уведомява писмено Органа по надзор и Потребителите, че дейността му се поема от друг регистриран доставчик, както и относно наименованието му. Уведомлението се публикува в Интернет страницата на Евротръст;
- уведомява Потребителите относно условията по поддръжка на прехвърлените удостоверения към приемащия Доставчик;
- променя статуса на оперативните удостоверения и надлежно предава цялата документация, свързана с дейността си на приемащия Доставчик, заедно с всички архиви, както и всички издадени удостоверения (валидни, прекратени и спрени);
- извършва необходимите действия за прехвърляне на задълженията по поддръжка на информацията към приемащия Доставчик;
- прехвърля управлението на вече издадените удостоверения за крайни потребители към приемащия Доставчик;

Приемащият Доставчик поема правата и задълженията на Евротръст с прекратена дейност и продължава да управлява активните удостоверения до края на тяхното действие.

Архивът на Евротръст с прекратен статус трябва да бъде предаден на Доставчика, приел дейността.

5.9.5 ОТНЕМАНЕ НА КВАЛИФИЦИРАН СТАТУТ НА ЕВРОТЪРЪСТ ИЛИ НА КВАЛИФИЦИРАНИЯ СТАТУТ НА СЪОТВЕТНА УСЛУГА

При отмяна на квалифицирания статут на Евротръст или на някоя от предоставяните от него удостоверителни услуги, той извършва следното:

- уведомява потребителите си за променения си статут или този, на своите услуги;
- променя статуса на своите удостоверения;
- прекратява да издава нови квалифицирани удостоверения, но продължава да управлява активните удостоверения до края на тяхното действие;
- прави търговски разумни усилия, за да се сведе до минимум нарушаването на интересите на потребителите.

6 УПРАВЛЕНИЕ И КОНТРОЛ НА ТЕХНИЧЕСКАТА СИГУРНОСТ

Тази част от „Практиката при предоставяне на квалифицирани удостоверителни услуги“ описва процедурите за генериране и управление на криптографските ключове и свързаните с тях технически изисквания.

Евротръст използва единствено надежден и сигурен хардуер и софтуер, които са част от компютърната система на дружеството. Компютърните системи, на които работят всички критични компоненти от инфраструктурата на Евротръст, са оборудвани и конфигурирани със средства за локална защита на достъпа до софтуера и информационните данни. Евротръст използва процедури за управление на информационната сигурност на цялата инфраструктура на Евротръст в съответствие с общоприети в международната практика стандарти.

За осигуряване на надеждна експлоатация и сигурност на жизнения цикъл на компютърните системи Евротръст прилага следните изисквания:

- при разработване на нови системи Евротръст извършва анализ на изискванията за сигурност още на етап проектиране и спецификация като по този начин гарантира, че сигурността е вградена в ИТ системите;
- Евротръст прилага политика за сигурност и процедура за контрол на промени при извършване на осъвременявания, модификации на аварийен и оперативен софтуер и промени в конфигурацията;
- процедурите включват документация за промените;
- Евротръст защитава целостта на системите и информацията от вируси, злонамерен и неоторизиран софтуер;
- Евротръст създава и прилага процедури за всички доверени и административни

роли, които оказват влияние върху предоставянето на услуги;

➤ Евротръст определя и прилага процедури, с които гарантира, че:

а) при наличие на защитни и функционални актуализации на софтуера (security patches), то те се прилагат в разумен срок, след като са налични;

б) защитните и функционални актуализации не се прилагат, ако има вероятност да въведат допълнителни уязвимости или нестабилности, които да превишават ползите от прилагането им;

в) причините за неприлагане на никакви защитни и функционални актуализации се документират.

6.1 ГЕНЕРИРАНЕ И ИНСТАЛИРАНЕ НА ДВОЙКА КЛЮЧОВЕ

Криптографските двойки ключове за оперативните удостоверения на Евротръст се генерират и инсталират съгласно инструкциите и процедурите в този документ. Генерирането се осъществява от овластени лица от Евротръст, като се спазват изискванията за поне двуфакторен контрол. За създаване на подпис се използва защитен механизъм, със защитен профил, определен в съответствие със технически спецификации, определящи нива на сигурността.

Доставчикът използва своите частни ключове само за целите на дейността си, както следва:

➤ да подписва издаваните оперативни удостоверения на Удостоверяващите органи в своята инфраструктура;

➤ да подписва издаваните и публикувани Списъци със спрени и прекратени удостоверения (CRL);

➤ да подписва всички издадени и публикувани удостоверения за електронен подпис/печат на Потребителите.

Криптографската двойка ключове (частен и публичен) на издаваните удостоверения за електронен подпис/печат в инфраструктурата на Евротръст се генерира както следва:

➤ от Титуляря/Създателя, с хардуер и софтуер, който е под негов контрол, но е одобрен от Евротръст;

➤ от оператор на Регистриращия орган на Евротръст, с хардуер и софтуер, който е под контрола на инфраструктурата на Евротръст;

➤ От Евротръст, когато издаването на удостоверенията се заявява отдалечено, чрез мобилното приложение на Евротръст.

За генерирането на двойка ключове на квалифицирано удостоверение за електронен подпис/печат винаги се използва устройство за създаване на електронен подпис/печат, със защитен профил съгласно Регламент (ЕС) № 910/2014.

Само електронни подписи/печати, създадени с частен ключ на двойка ключове генерирани в устройство за създаване на квалифициран електронен подпис/печат имат характера на квалифициран електронен подпис/печат.

Титулярят/Създателят се задължава да използва лицензиран софтуер за работа с устройство за създаване на електронен подпис/печат.

6.1.1 ГЕНЕРИРАНЕ НА ДВОЙКА КЛЮЧОВЕ НА УДОСТОВЕРЯВАЩ ОРГАН

Доставчикът генерира двойки криптографски (RSA) ключове на базовия и на оперативния Удостоверяващи органи като използва хардуерна криптосистема (HSM/Hardware Security Module) с ниво на сигурност FIPS 140-2 Level 3 или по-високо, съответно CC EAL 4+ или по-високо.

Оторизирани лица от персонала на Евротръст изпълняват стъпките по генериране, инсталиране и съхраняване на двойките ключове на базовия и на оперативните Удостоверяващи органи, съответно „Evrotrust RSA Root CA“, „Evrotrust RSA Operational CA“, „Evrotrust RSA QOperational CA 2024“, „Evrotrust RSA REG.KE Operational CA 2025“ и „Evrotrust Services CA“ съгласно документирана вътрешна процедура, съгласувана и утвърдена от ръководството на Евротръст.

Процедурата се изпълнява в присъствие на член на Съвета на директорите на Евротръст.

Преди да се генерира базова двойка ключове на Евротръст се прави процедура за достъп до инсталиран криптомодул (HSM/Hardware Security Module), като се генерират самостоятелно и независимо един от друг симетрични ключове, които се съхраняват на токъни, защитени с персонален идентификационен номер (PIN) за достъп. Всеки от операторските токъни съдържа част от ключовете за достъп до криптомодула. За управление на съхраняваните в криптомодула частни ключове на Евротръст са необходими два от четири

комплекта с трите роли операторски токъни и съответните PIN за достъп.

Кодовете за достъп до частния ключ са независимо поделени между оторизирани лица от персонала на Евротръст, с оглед на невъзможност за персонална активация на достъпа до съответния частен ключ.

Създадените частни ключове на Удостоверяващите органи се съхраняват разделно върху отделни устройства за създаване на квалифициран електронен подпис, всяко от които е под контрола на повече от едно оторизирано лице от персонала на Евротръст. Разделното съхранение на частните ключове и индивидуалният контрол на достъп до съхраняваните части на частни ключове на Удостоверяващия орган в отделните устройства за създаване на квалифициран електронен/печат не позволява тези ключове да бъдат компрометирани и/или нерегламентирано репродуцирани извън Евротръст.

Ключовете и удостоверенията на Удостоверяващия орган са генерирани само по време на церемония по генериране на ключове, в която участват единствено лица, оправомощени от Евротръст. Евротръст генерира ново удостоверение на СА и прилага всички необходими действия, преди изтичане на това удостоверение, за да има непрекъснатост на услугите. Новото удостоверение се генерира и разпространява в съответствие с настоящия документ. Процедурата се извършва в подходящ интервал между датата на изтичане на удостоверението и последното подписано удостоверение, за да могат всички страни, които имат взаимоотношения с Евротръст (субекти, потребители, доверяващи се страни и др.), да са наясно с тази смяна на ключове и да приложат необходимите операции, за да избегнат неудобства и неизправности. Това не се отнася в случай, че Евротръст прекрати дейността си преди датата на изтичане на оперативното му удостоверение за подписване. Евротръст документира процедурата за провеждане на генериране на двойка ключове на удостоверяващи органи.

Процедурата по генериране включва най-малко следното:

- a) роли, участващи в церемонията (вътрешни и външни за Евротръст);
- b) функции, които трябва да се изпълнява всяка една роля и в кои фази;
- c) отговорности по време и след церемонията; и
- d) изисквания за събиране на доказателства за церемонията.

Евротръст изготвя доклад, доказващ, че церемонията е проведена в съответствие с

посочената процедура и че целостта и поверителността на двойката ключове е било осигурено. Този доклад трябва да бъде подписан:

- За root CA: от доверената роля, отговорна за сигурността на церемонията по управление на ключовите услуги (напр. Служител по сигурността) и доверен човек, независим от ръководството на Евротръст (напр. нотариус, одитор) като свидетел, че докладът правилно е записал церемонията;
- За оперативни CA: от доверената роля, отговорна за сигурността на церемонията по управление на ключовите услуги (например служител по сигурността) като свидетел, че докладът правилно записва церемонията по управлението на ключовете.

Публичните ключове на CA са достъпни за доверяващите се страни по начин, който гарантира целостта им и удостоверява техния произход.

6.1.2 ГЕНЕРИРАНЕ НА ДВОЙКА КЛЮЧОВЕ НА ТИТУЛЯР/СЪЗДАТЕЛ

Двойката ключове на Титуляр/Създател на квалифицирано удостоверение за електронен подпис/печат се генерира само в одобрено от Евротръст устройство за създаване на електронен подпис/печат (външно), проверено за ниво на сигурност и за успешна работа през интерфейсите на инфраструктурата на Евротръст.

Когато двойката ключове се генерира при Евротръст, винаги се използва устройство за създаване на електронен подпис/печат. Частният ключ на генерираната двойка ключове не може да бъде изведен от устройството.

Контролът на частния ключ е чрез код за достъп. Титулярият използва кодът за достъп до устройството, с цел да осъществи достъп до частния ключ за създаване на квалифициран електронен подпис/печат.

Когато двойката ключове се генерира при Титуляр/Създател, Доставчикът препоръчва последният да използва одобрено устройство, в инфраструктурата на Евротръст за създаване на квалифициран електронен подпис/печат или еквивалентно такова, отговарящо на изискванията на Регламент (ЕС) № 910/2014 и съвместимо с инфраструктурата на Евротръст.

В случаите, когато генерирането на двойката ключове се осъществява при Титуляря или Създателя, същият носи пълната отговорност по защитата на частния ключ, с цел предотвратяване на неговото компрометиране, разкриване, модифициране, загуба или неразрешено ползване. Титулярият/Създателят носи отговорност за пропуски или действия на

упълномощени от тях лица, които са делегирани да генерират, пазят или съхраняват техните частни ключове.

6.1.2.1 ОТДАЛЕЧЕНО ГЕНЕРИРАНЕ НА ДВОЙКА КЛЮЧОВЕ

Създателят/Титулярят използва предоставен от Евротръст специализиран софтуер, чрез който се реализира процеса по генериране и управление на криптографската двойка ключове.

Генерирането, използването и съхраняването на частния ключ е с много високо ниво на сигурност, което е гарантирано от самия носител. Той е надеждно защитен посредством персонален идентификационен номер (PIN), който е известен само на Титуляря/Създателя.

Създателят/Титулярят генерира електронна заявка за квалифицирано удостоверение в PKCS#10 формат и я изпраща на Евротръст. Съгласно препоръките на RFC 2314 - PKCS#10, ASN.1 форматът за електронна заявка съдържа DN, публичен ключ и други атрибути, като всички те са подписани с частния ключ.

Двойка ключове може да се генерира отдалечено, при заявяване на отдалечено издаване на удостоверение за квалифициран електронен подпис/печат. В този случай ключовете се генерират в хардуерен криптомодул и частният ключ се съхраняват в криптиран от потребителя вид с неговия ПИН код.

6.1.3 ДОСТАВКА НА ЧАСТЕН КЛЮЧ НА ПОТРЕБИТЕЛЯ

Когато двойката ключове се генерира при Евротръст, Титулярят/Създателят или упълномощено от него лице получава частния ключ и издаденото квалифицирано удостоверение върху устройство за създаване на електронен подпис/печат в Регистриращия орган на доставчика.

При първоначално издаване на удостоверение върху устройство за създаване на електронен подпис/печат, преди генериране на двойка ключове, устройството се инициализира и се създават следните кодове за достъп: Потребителски („User“) и Административен („SO“). Създават се също кодове за персонален достъп до частния ключ и за деблокиране на блокирано устройство.

Началният Потребителски и Административен код за достъп и за деблокиране на устройството се предоставят на Титуляря/Създателя или на упълномощеното от него лице в

запечатан, непрозрачен хартиен плик.

Титулярят/Създателят е задължен на смени своя първоначален Потребителски код за достъп до устройството посредством софтуера, който се предоставя с него. Евротръст препоръчва Титуляря/Създателя да сменя периодично своя Потребителски код.

В случай на определен брой неуспешни опити за въвеждане на коректен код за достъп до частния ключ на Титуляря/Създателя, достъпът до него се блокира. В такива случаи Титулярят/Създателят трябва да използва предоставеният му съответен код за деблокиране.

Горните процедури не се прилагат при отдалечено издаване на квалифицирано удостоверение през мобилното приложение на Евротръст. В този случай двойката ключове се генерират в хардуерен криптомодул на Евротръст, а частният ключ се криптира с ПИН кода на Титуляря/Създателя. Евротръст не съхранява информация за ПИН кода. Същият се използва от потребителя само в мобилното приложение.

6.1.4 ДОСТАВКА НА ПУБЛИЧЕН КЛЮЧ ОТ ПОТРЕБИТЕЛ НА ДОСТАВЧИК

Изпълнява се единствено от Титуляр/Създател, при който се генерира двойка ключове и който следва да достави своя публичен ключ на Евротръст за нуждите на процеса на издаване на квалифицирано удостоверение.

Титулярят/Създателят доставя, чрез Регистриращия орган на Евротръст, публичния ключ от генерираната двойка ключове, чрез заявка в електронен форма, чийто формат е PKCS # 10. Заявката съдържа публичен ключ и е подписана електронно с кореспондиращия частен ключ. Чрез проверка на достоверността на подписа Евротръст може да установи и достоверността на изпратения публичен ключ.

Титулярят/Създателят може да предостави електронната заявка на носител, лично в Регистриращия орган, заедно с другите документи съгласно Политиката на Евротръст или отдалечено.

Регистриращият орган на Евротръст задължително прави проверка на държането на частния ключ от Титуляря/Създателя и потвърждава искането за квалифицирано удостоверение.

Горните процедури не се прилагат при отдалечено издаване на квалифицирано удостоверение през мобилното приложение на Евротръст.

6.1.5 ДОСТАВКА НА ПУБЛИЧЕН КЛЮЧ НА ДОСТАВЧИКА НА ДОВЕРЯВАЩИТЕ СЕ СТРАНИ

Публичните ключове на Евротръст са публикувани в удостоверенията на Удостоверяващия орган на Евротръст във формат X.509 v.3.

Удостоверенията са публикувани в регистъра на удостоверенията.

Всяка Доверяваща се страна изгражда доверие към Евротръст, като приеме и инсталира в системите под неин контрол оперативните удостоверения на Евротръст.

6.1.6 ДЪЛЖИНА НА КЛЮЧОВЕ

Дължината на базовия ключ на Евротръст „Evrotrust RSA Root CA“ е 4096 бита, с приложима комбинация на асиметрични и хеш алгоритми: sha384-with-RSA.

Дължината на двойката ключове на оперативния Удостоверяващ орган „Evrotrust RSA Operational CA“ е 2048 бита, с приложима комбинация на асиметрични и хеш алгоритми: sha256-with-RSA .

Дължината на двойката ключове на оперативния Удостоверяващ орган „Evrotrust RSA QOperational CA 2024“ е 4096 бита, с приложима комбинация на асиметрични и хеш алгоритми: sha256-with-RSA .

Дължината на двойката ключове на оперативния Удостоверяващ орган „Evrotrust RSA REG.KE Operational CA 2025“ е 4096 бита, с приложима комбинация на асиметрични и хеш алгоритми: sha256-with-RSA .

Дължината на двойката ключове на оперативния Удостоверяващ орган „Evrotrust Services CA“ е 4096 бита, с приложима комбинация на асиметрични и хеш алгоритми: sha256-with-RSA .

Дължината на двойката ключове на оперативните органи „Evrotrust TSA“, „Evrotrust RSA Validation“, „Evrotrust Services Validation“ и „Evrotrust RSA QOperational CA 2024 OCSP“ е 2048 бита, с приложима комбинация на асиметрични и хеш алгоритми: sha256-with-RSA.

Дължината на двойка ключове за квалифициран и усъвършенстван електронен подпис/печат на Титуляр/Създател може да е 2048, 3072 или 4096 бита с приложима криптографска комбинация за подписване "sha256-with-RSA".

За съответните профили приложимите комбинации са:

Профил на квалифицираното удостоверение	Тип и дължина на двойките ключовете	Използвани асиметрични и хеш алгоритми
Evrotrust Qualified Natural Person Certificate for QES	RSA 2048 RSA 3072 RSA 4096	sha256-with-RSA
Evrotrust Qualified Natural Person Attribute Certificate for QES	RSA 2048 RSA 3072 RSA 4096	sha256-with-RSA
Evrotrust Qualified Legal Person Certificate for QESeal	RSA 2048 RSA 3072 RSA 4096	sha256-with-RSA
Evrotrust SSL Domain Validated Certificate	RSA 2048 RSA 3072 RSA 4096	sha256-with-RSA
Evrotrust SSL Organization Validated Certificate	RSA 2048 RSA 3072 RSA 4096	sha256-with-RSA
Evrotrust SSL EV Certificate	RSA 2048 RSA 3072 RSA 4096	sha256-with-RSA
Evrotrust SSL PSD2 Certificate	RSA 2048 RSA 3072 RSA 4096	sha256-with-RSA
Evrotrust Qualified Natural Person Certificate for AES	RSA 2048 RSA 3072 RSA 4096	sha256-with-RSA
Evrotrust Qualified Legal Person Certificate for AESeal	RSA 2048 RSA 3072 RSA 4096	sha256-with-RSA

Профил на квалифицираното удостоверение	Тип и дължина на двойките ключовете	Използвани асиметрични и хеш алгоритми
Evrotrust Qualified PSD2 Legal Person Certificate for ASeal	RSA 2048 RSA 3072 RSA 4096	sha256-with-RSA
Evrotrust REG.KE Qualified Natural Person Certificate for QES	RSA 2048 RSA 3072 RSA 4096	sha256-with-RSA
Evrotrust REG.KE Qualified Natural Person Certificate for AES	RSA 2048 RSA 3072 RSA 4096	sha256-with-RSA
Evrotrust REG.KE Qualified Natural Person Attribute Certificate for QES	RSA 2048 RSA 3072 RSA 4096	sha256-with-RSA

Независимо къде е генерирана двойката ключове за издаване на удостоверение за електронен подпис/печат, ключът трябва да е с дължина най-малко 1024 бита за алгоритми RSA и DSA, и 160 бита за алгоритми ECDSA.

6.1.7 КРИПТОГРАФСКИ АЛГОРИТМИ

Всички използвани алгоритми са съобразени с техническата спецификация ETSI TS 119 312. Евротръст следи регулярно за сигурността и приложимостта на използвания хеш алгоритъм. Всички използвани алгоритми се проверяват веднъж годишно или когато настъпят промени. В случай, че алгоритъмът бъде компрометиран или стане неподходящ, за целта се пристъпва към регенерирането на всички засегнати ключове.

За всеки поддържан профил Евротръст наблюдава силата на всеки криптографски алгоритъм, използван във връзка с този профил. В случай, че един от използваните алгоритми или параметри се счита за по-малко сигурен или валидността на съответното удостоверение изтича, той се актуализира или се създаде нов профил.

Ако някой от алгоритмите или свързаните с него параметри, използвани от Евротръст или потребителите, стане недостатъчен за оставащото му предназначение, Евротръст информира всички потребители и доверяващи се страни, с които има договор. Освен това Евротръст предоставя тази информация на други доверяващи се страни. В такива случаи Евротръст предприема прекратяване на всички засегнати удостоверения.

6.1.8 ПАРАМЕТРИ НА ПУБЛИЧЕН КЛЮЧ

Параметрите на публичния ключ са посочени в удостоверението, което Доставчикът издава за този публичен ключ.

Титулярят/Създателят на ключова двойка е отговорен за проверката на качеството на параметрите на генерирания частен ключ. Той е длъжен да провери способността на ключа да криптира и декриптира, включително да създава електронен подпис и да извършва проверка на такъв.

Използваната среда за генериране и съхраняване на ключовете на основните компоненти в инфраструктурата на Евротръст „Evrotrust RSA Root CA“, „Evrotrust RSA Operational CA“, „Evrotrust RSA QOperational CA 2024“, „Evrotrust RSA REG.KE Operational CA 2025“, „Evrotrust Services CA“, „Evrotrust TSA“, „Evrotrust RSA QS Validation“, „Evrotrust Services Validation“, „Evrotrust RSA QOperational CA 2024 OCSP“ и други е криптомодул (HSM) с удостоверение ниво на сигурност FIPS 140-2 Level 3 и CC EAL 4+, което удовлетворява приложимите нормативни изисквания.

Устройствата за създаване на квалифициран електронен подпис/печат и осигурената среда за генериране и съхраняване на ключовете на Титуляря/Създателя са с ниво на сигурност CC EAL 4+ и FIPS 140-2 Level 3.

Всички устройства извън инфраструктурата на Евротръст, които потребителите могат да използват, за да генерират двойка ключове и да съхраняват частния ключ за електронен подпис/печат, трябва да са сертифицирани за ниво на сигурност CC EAL 4+ и по-високо еквивалентно ниво.

6.1.9 ИЗПОЛЗВАНЕ НА КЛЮЧА

Параметрите на използване на двойката ключове, по-конкретно на частния ключ, се съдържат в удостоверението, което издава Евротръст чрез атрибутите „Key Usage“ и

„Extended Key Usage“, отговарящи на стандарта X.509 v3. Употребата на всеки атрибут от посочените области е съобразена с RFC 5280.

6.2 ЗАЩИТА НА ЧАСТЕН КЛЮЧ И КОНТРОЛ НА КРИПТОГРАФСКИЯ МОДУЛ

Всеки потребител, оператор на Удостоверяващ орган и оператор на Регистриращ орган създава и съхранява частен ключ, като използва надеждна система за неговата сигурност. Удостоверяващият орган генерира двойка ключове при поискване от потребителя и му ги предава в защитен вид, като го уведомява за правилата на съхранение и защита на неговия частен ключ. Когато удостоверението е заявено отдалечено, чрез мобилното приложение на Евротръст, предаването на частния ключ на Титуляря/Създателя не се прави.

Когато криптографското устройство, върху което е генериран и се съхранява частния ключ, не се предава лично на потребителя, а се използва посредник за доставката (напр. куриерска фирма), издаденото удостоверение се спира до потвърждаване на получаването от страна на потребителя. Кодовете за достъп на полученото криптографското устройство се изпращат на потребителя по независим сигурен канал (напр. през мобилното приложение на Евротръст).

Частните ключове на Удостоверяващия орган на Евротръст, както и ключовете на потребителите, които са заявили отдалечено издаване на квалифицирани удостоверения, се съхраняват в сигурни криптографски модули, удовлетворяващи нормативните изисквания на Регламент (ЕС) № 910/2014.

Инсталираните криптографски модули са най-висока степен на сигурност, съгласно изискванията на международните стандарти.

Защитеното криптографско устройство работи единствено в неговата конфигурация, както е описано в съответната документация за сертифициране. Частният ключ за подписване на СА се съхранява и използва в защитено криптографско устройство, отговарящо на изискванията на Регламент (ЕС) № 910/2014 г. Когато е извън защитеното криптографско устройство, частният ключ на СА е защитен по начин, който осигурява същото ниво на защита, както е осигурено от защитеното криптографско устройство. Частният ключ за подписване на СА се архивира, съхранява и възстановява само от персонал в доверени роли, като се използва поне двоен контрол във физически обезпечена среда. Броят на персонала, упълномощен да извърши резервно копие, съхранение и възстановяване на частния ключ за

подписване на СА, е сведен до минимум и е в съответствие с практиката на Евротръст. Копията на частните ключове се подлагат на същото или по-високо ниво на контрол на сигурността като използваните в момента ключове. Когато частните ключове и всички копия се съхраняват в специално защитено криптографско устройство, Евротръст осигурява контрол на достъпа, за да гарантира, че ключовете не са достъпни извън това устройство. Защитеното криптографско устройство не е манипулирано по време на изпращането. Евротръст осигурява защита на криптографското устройство от манипулации докато то се съхранява. Евротръст гарантира, че защитеното криптографско устройство функционира правилно. Частните ключове за подписване, съхранявани в защитено криптографско устройство се унищожават при излизане от употреба на устройството. Това унищожаване не засяга непременно всички копия на частния ключ. Унищожаване се само физическият екземпляр на ключа, съхранен в защитеното криптографско устройство.

6.2.1 СТАНДАРТИ ЗА КРИПТОГРАФСКИ МОДУЛИ

Основните компоненти в инфраструктурата на Евротръст „Evrotrust RSA Root CA“, „Evrotrust RSA Operational CA“, „Evrotrust RSA QOperational CA 2024“, „Evrotrust RSA REG.KE Operational CA 2025“ и „Evrotrust Services CA“ използват надеждна криптографска система (Hardware Security Module/HSM), сертифицирана за ниво на сигурност FIPS 140-2 Level 3, което удовлетворява нормативните изисквания.

Устройството за създаване на квалифициран електронен подпис, в което се генерира и съхранява частния ключ на Титуляря/Създателя е с ниво на сигурност CC EAL 4+/FIPS 140-1 Level 2 или по-високо.

Всички устройства за създаване на квалифицирани електронни подписи извън инфраструктурата на Евротръст, които Потребителят може да ползва за да генерира двойка ключове и да съхранява частния ключ, трябва да са сертифицирани за ниво на сигурност CC EAL 4 и по-високо еквивалентно ниво, отговарящо на изискванията на Регламент (ЕС) № 910/2014.

6.2.2 КОНТРОЛ НА ИЗПОЛЗВАНЕ И СЪХРАНЕНИЕ НА ЧАСТЕН КЛЮЧ

Частните ключове на Удостоверяващите органи на Евротръст се съхраняват и използват само в криптосистемата (HSM/Hardware Security Module) и са достъпни

посредством кодове за достъп, разделени на няколко части - известни на оторизирани лица от персонала на Евротръст. Базовият удостоверяващ орган на Евротръст е в режим „Offline“.

Едновременно с генериране на двойка ключове на Удостоверяващия орган се изпълнява и процедурата по съхраняване на частния ключ (или двойката ключове) в съответствие с утвърдена вътрешна процедура. За управление на съхраняваните в криптомодула частни ключове на Евротръст са необходими два от четири комплекта с трите роли операторски токъни и съответните персонални идентификационни номера (PIN) за достъп.

Архив на ключовете се прави първоначално – след създаването на всички ключове, както и в последствие след регенериране на някои от тях. Архивирането на частните ключове, намиращи се в криptosистемата (HSM) с ниво на сигурност FIPS 140-2 Level 3 се извършва върху устройство със същото ниво на сигурност. За да бъде направен архив на ключовете са нужни двама от четиримата, разполагащи с токъни за достъп до криptosистемата (HSM). Архивирането се извършва в защитена среда. След създаването на архива (Backup), той се слага в сейф на отдалечено местоположение с необходимите мерки за сигурност.

Частният ключ на Титуляря/Създателя се използва само в устройство за създаване на електронен подпис/печат или в устройство с еквивалентно ниво на сигурност (съгласно изискванията на Регламент (ЕС) № 910/2014) и е достъпен посредством личен код за достъп. Едновременно с генериране на двойка ключове на Титуляр/Създател се изпълнява съхраняване на частен ключ в устройство за създаване на електронен подпис/печат.

Доставчикът по никакъв начин не съхранява и не архивира частен ключ на Титуляр/Създател за създаване на електронен подпис/печат, освен ако удостоверението за квалифициран електронен подпис се заявява отдалечено, чрез мобилното приложение на Евротръст.

6.2.3 ДОВЕРИТЕЛНО СЪХРАНЯВАНЕ НА ЧАСТЕН КЛЮЧ (ЕСКРОУ)

Прилагат се правилата, описани по-горе.

6.2.4 СЪХРАНЯВАНЕ НА ЧАСТЕН КЛЮЧ

Частните ключове на Удостоверяващия орган се съхраняват на части разделно върху отделни токъни със защитен профил CC EAL 4+ или по-висок, като достъпът до всяко устройство се контролира чрез код за достъп от съответното оторизирано лице от персонала на Евротръст.

Разделното съхранение на частните ключове на Удостоверяващия орган върху няколко токъна и личния контрол на достъп до тези устройства не позволява ключовете да бъдат компрометирани или нерегламентирано репродуцирани извън Евротръст.

Репродуцирането на частни ключове на Евротръст върху резервен криптомодул след дефектиране на оперативната такава, се изпълнява само в присъствие на поне 2 оторизирани лица, всяко от които контролира достъпа до неговото устройство.

Евротръст не съхранява копия на частните ключове на операторите на Регистрацията орган.

Доставчикът не създава копия на частните ключове на потребителите, освен в случаите на отдалечено издаване на квалифицирани удостоверения чрез мобилното приложение на Евротръст. Частният ключ на Титуляря/Създателя се съхранява само на устройство за създаване на квалифициран електронен подпис/печат и не може да се възпроизведе на друго устройство. При дефектиране на потребителско устройство за създаване на квалифициран електронен подпис/печат, Потребителят трябва да го подмени и да поиска издаване на ново квалифицирано удостоверение.

6.2.5 АРХИВИРАНЕ НА ЧАСТНИЯ КЛЮЧ

Частният ключ на Удостоверяващия орган, използван за създаване на квалифицирани електронни подписи/печати се архивира, за най-малко 10 години след изтичане на срока му на валидност или след неговото прекратяване. Същото изискване важи и за удостоверението на публичния ключ, съответстващо на частния ключ, след изтичане на срока му на валидност или след прекратяването му.

Удостоверенията на Евротръст с изтекъл срок на валидност или прекратени трябва да са достъпни по електронен път за срок от най-малко 10 години.

Евротръст не създава архивни копия от частните ключове на Регистрацията орган и на частните ключове на потребителите, освен при отдалечено заявяване на квалифицирано удостоверение през мобилното приложение на Евротръст.

6.2.6 ТРАНСФЕР НА ЧАСТЕН КЛЮЧ В КРИПТОГРАФСКИ МОДУЛ

Трансфер на частен ключ в криптографски модул се извършва в следните случаи:

- за защита, в случай на създаване на резервни копия на частни ключове, съхранявани в криптографски модул (например в случай на компрометиране или неизправност в криптографския модул);
- когато се налага да се прехвърли частния ключ от оперативния криптомодул на друг криптомодул (в случай на отказ на оперативния криптомодул или при необходимост от унищожаване).

Трансферът на частен ключ в криптомодул е критична операция. Такава операция изисква подходящи мерки и процедури, предотвратяващи разкриването на частния ключ или неговата промяна и фалшифициране по време на изпълнение на операцията.

Трансферът на частен ключ в криптографски модул изисква възстановяване на ключа от картите на двама от четирима оторизирани служители в присъствието на член на Съвета на Директорите.

6.2.7 СЪХРАНЯВАНЕ НА ЧАСТЕН КЛЮЧ В КРИПТОГРАФСКИ МОДУЛ

В зависимост от използвания криптографски модул, частните ключове на Удостоверяващия орган на Евротръст се съхраняват винаги в криптиран вид. Независимо от формата на съхранение на частния ключ, той не е достъпен за неоторизирани лица извън криптографския модул.

6.2.8 МЕТОД ЗА АКТИВИРАНЕ НА ЧАСТЕН КЛЮЧ

Частният ключ на доставчика се активира посредством поделен системен код за достъп, отделните части на който са известни на повече от едно овластени лица от Евротръст. Само в присъствие на тези лица, след въвеждане на всички части на кода за достъп, се разрешава достъпът до слота в криптографския модул (HSM) и се активира частния ключ.

Частният ключ на Титуляр/Създател се активира, чрез въвеждане на потребителския код за достъп до мястото, където защитено се съхранява ключа или се използва друг способ на идентификация със същото или по-високо ниво на сигурност.

6.2.9 МЕТОД ЗА ДЕАКТИВИРАНЕ НА ЧАСТЕН КЛЮЧ

Частен ключ на Удостоверяващ орган на Евротръст намиращ се в криптографски модул (HSM) се деактивира посредством преустановяване на логическия достъп до този ключ. Деактивирането изисква нулиране на паметта на криптографския модул. По този начин се прекратява възможността за достъп и използване на частния ключ. Всяко деактивиране на частен ключ се записва в дневник.

Частен ключ на Титуляр/Създател се деактивира посредством преустановяване на логическия достъп до устройството за създаване на квалифициран електронен подпис/печат или чрез физическо му унищожаване, когато е външно. По този начин окончателно се прекратява възможността за достъп и използване на частния ключ.

6.2.10 МЕТОД ЗА УНИЩОЖАВАНЕ НА ЧАСТЕН КЛЮЧ

Частен ключ на Удостоверяващ орган в криптографски модул (HSM) се унищожава посредством изтриване на ключа или съответния слот. При необходимост се изтриват и съхраняваните в архива носители за възстановяване. Всяко достъп до частен ключ се записва в дневник.

Частният ключ на квалифицирано удостоверение на Титуляр/Създател се унищожава посредством изтриването му от устройството за създаване на квалифициран електронен подпис/печат или чрез физическото унищожаване на устройството, когато е външно.

6.2.11 ОЦЕНКА НА КРИПТОГРАФСКИЯ МОДУЛ

Евротръст използват надеждна криптографска система (Hardware Security Module/HSM), сертифицирана за ниво на сигурност по FIPS 140-2 Level 3. Тя е сертифицирана и като Qualified Electronic Signature Creation Device (QSigCD) и Qualified Electronic Seal Creation Device (QSealCD) в съответствие с Регламент (ЕС) № 910/2014. Сертификацията е базирана на Common Criteria (CC) EAL4+ AVA_VAN.5.

6.3 ДРУГИ АСПЕКТИ НА УПРАВЛЕНИЕТО НА ДВОЙКАТА КЛЮЧОВЕ

Изискванията описани в тази част на „Практика при предоставяне на квалифицирани удостоверителни услуги“ се прилагат в процедурите за архивиране на публични ключове и процедурите описващи сроковете на валидност на потребителските ключове и на ключовете

на удостоверяващия орган.

Евротръст гарантира, че използва подходящо частните ключове за подписване.

Евротръст не използва частните ключове след края на техния жизнен цикъл и за цели различни от тяхното предназначение. Ключовете се използват само във физически обезопасени помещения. Използването на частните ключове е съвместимо с алгоритъма на хеширане, алгоритъма за подпис и дължината на ключа, използвани за генериране на удостоверения, в съответствие с настоящия документ. Всички копия на частните ключове за подписване се унищожават в края на техния жизнен цикъл.

6.3.1 АРХИВИРАНЕ НА ПУБЛИЧЕН КЛЮЧ

Публичните ключове на Удостоверяващите органи се съдържат в издадените оперативни удостоверения на Евротръст и се съхраняват във вътрешен регистър. Публичните ключове са достъпни за доверяващите се страни и потребителите, чрез публикуване на удостоверенията на уеб сайта на Евротръст.

Публичните ключове на Удостоверяващите органи се архивират и съхраняват за период от най-малко 10 години след изтичане на периода на валидност или прекратяването на съответните удостоверения. Целта на архивиране на публичния ключ е да се създаде възможност за проверка на електронния подпис/печат след отстраняване на удостоверението от регистъра на удостоверенията. Това е изключително важно в случай на проверка на статуса на удостоверението.

Публичните ключове на Титуляри/Създатели се съдържат в издадените за тях удостоверения, които са публикувани в регистъра на удостоверенията на Евротръст.

Публичните ключове на Титуляри/Създатели се съхраняват в регистъра на удостоверенията и периодично се архивират.

Всеки архив на публичен ключ или всяко логическо и физическо унищожение на публичен ключ се записва в дневник.

6.3.2 ПЕРИОД НА ВАЛИДНОСТ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ И УПОТРЕБА НА КЛЮЧОВЕ

Периода на употреба на публични ключове се определя от стойността на полето в удостоверението му, описващо валидността на публичния ключ. Валидността на

удостоверенията и съответните им частни ключове могат да бъдат съкратени, в случай на прекратяване на удостоверенията.

Максимални периоди на използване на квалифицирани удостоверения:

Evrotrust RSA Root CA	20 (двадесет) години
Evrotrust RSA Validation	5 (пет) години
Evrotrust RSA Operational CA	10 (десет) години
Evrotrust RSA QOperational CA 2024	10 (десет) години
Evrotrust RSA REG.KE Operational CA 2025	10 (десет) години
Evrotrust Services CA	10 (десет) години
Evrotrust TSA	5 (пет) години
Evrotrust RSA QS Validation	5 (пет) години
Evrotrust Services Validation	5 (пет) години
Evrotrust RSA QOperational CA 2024 OCSP	5 (пет) години
Evrotrust Qualified Validation Service SU 2024	5 (пет) години
Удостоверения за крайни потребители	не повече от 3 (три) години

Когато се използва ключ за подписване, след изтекъл период на валидност на удостоверението, подписът е невалиден.

Шест месеца преди изтичането на периода на валидност на квалифицирано удостоверение на Удостоверяващ орган, Доставчикът издава ново квалифицирано удостоверение и генерира нова двойка ключове. Удостоверението се прави публично достояние съгласно процедурите описани в настоящия документ.

6.4 ДАННИ ЗА АКТИВИРАНЕ

Когато потребителят лично присъства пред Регистриращия орган, данните за активиране на частен ключ се използват основно от оператор на Регистриращия орган. Потребителите използват автентификация и контрол на достъпа до своя частен ключ.

Инсталирането и възстановяването на двойките ключове на СА в сигурно криптографско устройство изисква едновременно контрол на най-малко двама доверени служители. Активирането и деактивирането на защитеното криптографско устройство се извършва по сигурен начин. Когато потребителите използват персонализирано защитено

криптографско устройство, за активиране на се използват свързани данни (напр. ПИН код). Данните за активиране са сигурно подготвени и се разпространяват отделно от защитеното криптографско устройство.

ЗАБЕЛЕЖКА: Разделянето може да се постигне чрез осигуряване на разпространение на данни за активиране и доставка на защитено потребителско устройство по различно време или чрез различен канал.

В случаите, в които Титулярят/Създателят генерират двойка ключове за квалифицирано удостоверение, те сами създават и управляват данните за активиране.

Когато Титулярят/Създателят заявява отдалечено издаването на квалифицирано удостоверение през мобилното приложение на Евротръст, той създава ПИН код, с който се криптира генерирания частния ключ в хардуерния криптомодул на Евротръст. Последният не съхранява данни за ПИН кода. Същият се използва от потребителя за декриптиране и активиране на частния ключ при подписване отдалечено, от мобилното приложение на Евротръст.

6.4.1 ГЕНЕРИРАНЕ И ИНСТАЛИРАНЕ НА ДАННИ ЗА АКТИВИРАНЕ

Данни за активиране се използват при първоначално издаване на удостоверение, върху устройство за създаване на подпис/печат, преди генериране на двойка ключове. В този случай устройството се инициализира и се създават кодове за достъп: Потребителски („User“) и Административен („SO“). Тези кодове позволяват персонален достъп до частния ключ в устройството и при необходимост за деблокиране на същото.

Кодовете за достъп и за деблокиране на устройството за създаване на квалифициран електронен подпис/печат се предоставят на Титуляря/Създателя или на упълномощеното от него лице в запечатен, непрозрачен хартиен плик.

Титулярят е задължен да смени първоначалния Потребителски код за достъп посредством софтуера, който се предоставя заедно с устройството.

Доставчикът препоръчва Титулярят/Създателят да сменя периодично своя Потребителски код за достъп до устройството за създаване на квалифициран електронен подпис/печат.

Титулярят/Създателят следва да използва предоставения Административен код за достъп да деблокира блокирано устройство.

Когато се използва мобилно приложение на Евротръст, кодът за достъп се генерира от Титуляря/Създателя. Кодът не се съхранява от Евротръст и е достъпен за работа от потребителя само докато е активирано мобилното приложение. За възстановяване на персоналния код, Титулярят/Създателят въвежда тайна дума. Тайната дума не се пази от Евротръст.

6.4.2 ЗАЩИТА НА ДАННИ ЗА АКТИВИРАНЕ

Титулярят/Създателят е задължен да съхранява и пази от компрометиране кодовете за достъп до устройството за създаване на квалифициран електронен подпис/печат.

Потребителите трябва да знаят, че при няколко неуспешни опити за достъп до устройството, то се блокира (заклучва се). В тези случаи потребителят трябва да използва предоставения му Административен код за достъп за да деблокира устройството.

Доставчикът препоръчва данните за активиране на устройството никога да не се съхраняват заедно със самото устройство.

6.4.3 ДРУГИ АСПЕКТИ НА ДАННИТЕ ЗА АКТИВИРАНЕ

Данните за активиране трябва да се съхраняват винаги в един единствен екземпляр.

Персоналният идентификационен номер (PIN) за достъп трябва периодично да бъде променян.

Данните за активиране могат да бъдат архивирани.

6.5 СИГУРНОСТ НА КОМПЮТЪРНИТЕ СИСТЕМИ

Евротръст използва единствено надежден и сигурен хардуер.

Компютърните системи, на които работят всички критични компоненти от инфраструктурата на Евротръст, са оборудвани и конфигурирани със средства за локална защита на достъпа до софтуера и информационните данни.

Евротръст използва процедури за управление на информационната сигурност на цялата инфраструктура на Евротръст в съответствие с общоприети в международната практика стандарти.

За по-голяма надеждност и сигурност на използваните системи, техническата и криптографска сигурност на осъществяваните чрез тях процеси, Евротръст извършва редица

тестове и проверки на техническото оборудване и използваните технологии. Тестове и проверки на компютърните системи се правят съгласно методика за оценка на сигурността (относно: статус на процесорите - консумиране, натоварване, употреба; статус на съхранение; състояние на паметта-основна, padding in-out; статус на съхранение; брой на протичащите процеси; балансиране на натоварването). Те се извършват както периодично, така и при всяка промяна, която засяга сигурността на инфраструктурата. Тестовите включват vulnerability и penetration тестове. Vulnerability тестовите се извършват през период не по-голям от 3 месеца.

За управление на сигурността на компютърните системи в Евротръст се взимат в предвид изискванията на ISO/IEC 27001.

В Евротръст има Съвет за информационна сигурност, който е контролен орган по отношение на информационната сигурност. Съветът участва в анализа на информационните рискове и се свиква за обсъждане на възникнали въпроси или инциденти, свързани с информационната сигурност.

Компонентите на локалната мрежа (напр. рутери) се съхраняват във физически и логически защитена среда. Конфигурациите на локални мрежови компоненти (напр. рутери) периодично се проверяват за съответствие с изискванията, определени от Евротръст. Евротръст прилага многофакторно удостоверяване за акаунти, участващи в издаване на удостоверения. Приложението за разпространение на удостоверения (OCSP) налага контрол на достъпа при опити за добавяне или изтриване на удостоверения и промяна на друга свързана информация. Приложението за статус на прекратени удостоверения (CRL) налага контрол на достъпа при опити за промяна на информация за състоянието на прекратяване. Евротръст осигурява непрекъснат мониторинг на системите и сигнализация при откриване, регистриране на нарушения, както и своевременно реагиране при всякакви неоторизирани опити за достъп до неговите ресурси.

6.5.1 СТЕПЕН НА КОМПЮТЪРНА СИГУРНОСТ

Степента на сигурност на използваните системи в инфраструктурата на Евротръст отговаря на нормативните изисквания за изпълнение на дейността на Евротръст и се определя, чрез документа Политика за сигурност на Евротръст.

6.5.2 УПРАВЛЕНИЕ НА ИНЦИДЕНТИ И МОНИТОРИНГ

Евротръст извършва мониторинг и управлява инцидентите прилагайки следните изисквания:

- Евротръст има създадени и внедрени строги процедури, свързани с наблюдаване на работата на технологичната система, достъпа до информационната система, както и до заявките за удостоверителни услуги;
- Дейностите по мониторинг анализират и отчитат чувствителността на всяка събрана информация;
- В случаите на неналична услуга или ненормални системни дейности, които показват потенциално нарушение на сигурността, включително проникване в мрежата на Евротръст, се откриват и сигнализират;
- Оторизирани служители на Евротръст следят следните събития:
 - ✓ Стартиране и спиране на дейностите по регистриране;
 - ✓ Наличността и използването на необходимите услуги с мрежата на Евротръст;
- В случаи на нарушения на сигурността Евротръст има процедури за своевременна, бърза и координирана реакция, за ограничаване на нарушенията на сигурността;
- Сигналите за инциденти със сигурността се проследяват и докладват от служители с доверени роли в съответствие с процедурите на дружеството;
- Евротръст е установил процедура за уведомяване на съответните надзорни органи, в съответствие с приложимите регулаторни правила, за всяко нарушение на сигурността на информацията или загуба на нейната цялост, което оказва значително влияние върху предоставяната удостоверителна услуга, в рамките на 24 часа след установяване на нарушението;
- Когато нарушаването на сигурността на информацията или загубата на целостта ѝ вероятно ще се отрази неблагоприятно на физическо или юридическо лице, на което е предоставена удостоверителна услуга, Евротръст уведомява физическото или юридическото лице без ненужно забавяне;
- Евротръст извършва наблюдение на технологичната си система и редовно

преразглежда одиторските дневници, за да идентифицира доказателства за злонамерени дейности. Дружеството има разработени автоматични механизми за обработка на одитните дневници и за сигнализиране на персонала за възможни критични събития, свързани със сигурността;

- Системата генерира своевременно предупреждения, известяващи необичайни събития, които могат да окажат влияние върху способността на системата за сървърно подписване в съответствие с изискванията за сигурност (напр. действия на потребител извън стандартното работно време; действия, предизвикани от нечовешка намеса; потребителски действия, извън стандартните регламентирани дейности);

- За всяка новооткрита критична уязвимост се създава план за решаването ѝ в рамките на период от 48 часа след откриването ѝ;

- За всяка опасност, предвид потенциалното ѝ въздействие, Евротръст:

- ✓ създава план за намаляване на щетите;

- ✓ документира фактите и докладва на ръководството.

- Процедурите за докладване на инциденти пред ръководството и реакцията от взетите решения се използват по такъв начин, че предприетите мерки да сведат щетите до минимум, както и да се предприемат мерки в бъдеще да не се допускат подобни инциденти.

6.5.3 ПОЛИТИКАТА ЗА ИНФОРМАЦИОННА СИГУРНОСТ

При предоставяне на квалифицирано удостоверение за квалифициран електронен подпис/печат Евротръст отговаря на изискванията, предвидени в Регламент (ЕС) № 910/2014 и в член 21 от Директива (ЕС) 2022/2555. Целта на дружеството е да защити мрежовите и информационните системи, и физическата среда на тези системи от инциденти, като мерките включват поне следното:

- а) политики за анализ на риска и сигурност на информационните системи;

- б) действия при инцидент;

- в) непрекъснатост на стопанската дейност, например управление на съхраняването на резервни копия на данните и възстановяване след бедствия, и управление на кризи;

- г) сигурност на веригата за доставка, включително свързани със сигурността аспекти относно взаимовръзките между всеки субект и неговите преки снабдители или доставчици на услуги;

д) сигурност при придобиването на мрежови и информационни системи, разработване и поддръжка, включително предприемане на действия при уязвимости и оповестяването им;

е) политики и процедури за оценяване на ефективността на мерките за управление на риска в областта на киберсигурността;

ж) основни киберхигиенни практики и обучение в областта на киберсигурността;

з) политики и процедури относно използването на криптография и, когато е целесъобразно, криптиране;

и) сигурност на човешките ресурси, политики за контрол на достъпа и управление на активи;

й) използването на многофакторни решения за удостоверяване на автентичността или непрекъснато удостоверяване на автентичността, защитени гласови, видео и текстови съобщения и защитени системи за спешна комуникация в рамките на субекта, когато е целесъобразно.

Политиката за информационна сигурност е насочена към изискванията, свързани със стратегията на дейността, нормативните актове, законодателството и договорите, както и с текущата и възможната среда на заплахата за сигурността на информацията. Политиката за сигурност съдържа декларации, цели и принципи, които да ръководят всички дейности при възлагане на общи и конкретни отговорности за управление на сигурността на определени роли и процеси за справяне с отклонения, пробиви и извънредни ситуации. По-конкретно Политиката за информационна сигурност включва процедури, които описват механизмите за контрол на сигурността на информацията: контрол на достъпа, класифициране на информацията, физическа сигурност и сигурност на заобикалящата среда, активи, обмен на информация, работа от разстояние, използван софтуер, криптографски механизми за контрол, сигурност на комуникациите, защита на личните данни и взаимоотношение с доставчици.

Евротръст има разработена и одобрена от ръководството Политика за информационна сигурност, съобразена със следните изисквания:

➤ Политиката за информационна сигурност определя подхода на Евротръст за

управление на дейността;

- Промените в политиката за информационна сигурност се съобщават на трети страни (потребители, доверяващи се страни, надзорни и други регулаторни органи, органи за оценяване на съответствието), когато е приложимо;

- Политиката за информационна сигурност на Евротръст е документирана, внедрена и поддържана в актуално състояние;

- Всички служители на Евротръст са запознати с Политиката за информационна сигурност;

- Евротръст носи отговорност за спазването на процедурите в Политиката за информационна сигурност в случаи, когато е възложил на подизпълнители част от своите дейности. При наличие на подизпълнители, Евротръст определя тяхната отговорност и гарантира, че те прилагат стриктно всички контроли по информационна сигурност, изисквани от Евротръст;

- Политиката за информационна сигурност на Евротръст и инвентаризацията на активите за информационна сигурност се преразглеждат в планирани интервали от време или ако настъпят значителни промени, за да се гарантира тяхната пригодност, адекватност и ефективност;

- Всички промени, които могат да окажат влияние върху нивото на предоставената информационна сигурност, се одобряват от орган за управление на информационната сигурност;

Конфигурацията на системите на Евротръст се проверяват редовно за промени, които могат да нарушат правилата за информационна сигурност. Максималният интервал между две проверки е съгласно вътрешните процедури на Евротръст;

- Политиката за сигурност документира контролите за сигурност и неприкосновеността на личните данни. Личните данни, предоставени на Евротръст се съхраняват и обработват в съответствие със Закона за защита на личните данни и РЕГЛАМЕНТ (ЕС) 2016/679 General Data Protection Regulation (GDPR). Евротръст събира количество информация пропорционално на нейното предназначение и употреба. Всеки потребител дава съгласие за обработването на личните му данни. Това съгласие се заявява с подписването на Договор за удостоверителни услуги. Личните данни се използват само във връзка с

предоставянето на конкретната удостоверяваща услуга. Личните данни са защитени в съответствие с правилата за поверителност, съдържащи се в политиката за сигурност на Евротръст.

6.6 СИГУРНОСТ НА ЖИЗНЕНИЯ ЦИКЪЛ НА ТЕХНОЛОГИЧНАТА СИСТЕМА

6.6.1 КОНТРОЛИ ЗА РАЗВИТИЕ НА ТЕХНОЛОГИЧНАТА СИСТЕМА

Софтуерните приложения, използвани в технологичната система на Евротръст са разработени и внедрени от високо квалифицирани специалисти. Преди въвеждане на нови приложения те преминават през тестов период. Тестванията се правят на отделни системи, независими от тези в редовната експлоатация.

Всички хардуерни промени са наблюдават и регистрират. При закупуване на ново техническо оборудване, то се доставя с необходимите процедури за експлоатация и инструкции за ползване.

Евротръст наблюдава изискванията за капацитет и прави прогнози за бъдещи изисквания за капацитет, за да се осигури адекватна мощност за обработка и съхранение.

Технологичната сигурност на системата се гарантира както следва:

- технологично оборудване се доставя по начин, позволяващ неговото проследяване. Прави се оценка на трасето от първоначалната точка до мястото на неговото инсталиране;
- доставка и подмяна на технологично оборудване се извършва единствено с оригинален хардуер. Смяната се извършва от доверен и обучен персонал.

6.6.2 КОНТРОЛИ ЗА УПРАВЛЕНИЕ НА СИГУРНОСТТА НА ТЕХНОЛОГИЧНАТА СИСТЕМА

Целта на контрола за управление на сигурността е да се осъществява надзор на функционалността на технологичната система и да се гарантира, че тя функционира правилно и в съответствие с доставената производствена конфигурация.

Текущата конфигурация на технологичната система на Евротръст, както и всички изменения и актуализации на системата, се записват и извършват контролирано. Контролите позволяват непрекъсната проверка на целостта на технологичната система и своевременна актуализация, и отстраняване на неизправности.

6.6.3 КРИПТОГРАФСКИ КОНТРОЛИ

Евротръст е въвело подходящи контроли за сигурност на управление на криптографските ключове и всички криптографски устройства през целия им жизнен цикъл. За генериране на криптографската двойка ключове (частен и публичен) се използват хеш алгоритми и асиметрични алгоритми, които отговарят на изискванията на посочени в ETSI TS 119 312. Приложимите комбинации на асиметрични и хеш алгоритми спрямо сигурността на квалифицирания електронен подпис по времетраене е както е посочено в ETSI TS 119 312. Използва се дължина на ключа, която отговаря на изискванията на ETSI TS 119 312: Дължината на двойка ключове за квалифициран и усъвършенстван електронен подпис/ печат на Титуляр/Създател може да бъде 2048, 3072 или 4096 бита с приложима криптографска комбинация за подписване sha256-with-RSA. Ключът трябва да е с дължина най-малко 1024 бита за алгоритми RSA и DSA и 160 бита за алгоритми ECDSA.

Евротръст генерира двойки криптографски (RSA) ключове на базовия и на оперативния удостоверяващи органи като използва хардуерна криптосистема (HSM/Hardware Security Module) с ниво на сигурност FIPS 140-2 Level 3 или по-високо, съответно CC EAL 4+ или по-високо. Евротръст използва своите частни ключове само за целите на дейността си, както следва:

- да подписва издаваните оперативни удостоверения на удостоверяващите органи в своята инфраструктура;
- да подписва издаваните и публикувани Списъци със спрени и прекратени удостоверения (CRL);
- да подписва всички издадени и публикувани квалифицирани удостоверения за електронен подпис/печат на потребителите.

Когато се извършва отдалечено генериране на двойката ключове на потребител при заявено издаване на удостоверение от мобилното приложение на Евротръст, частният ключ се генерира и съхранява в криптиран вид в хардуерния криптомодул на Евротръст, отговарящ на изискванията на Регламент (ЕС) № 910/2014 г. за устройство за сигурно създаване на подпис (QSCD). Криптирането на ключа е чрез създаден от потребителя ПИН код, което обезпечава възможността единствено той да има достъп за активиране на ключа. Устройствата за създаване на квалифициран електронен подпис/печат гарантират, чрез

подходящи технически и процедурни средства, най-малко че:

- поверителността на данните за създаване на електронен подпис/печат, използвани за създаването на електронния подпис/печат, е разумно гарантирана;
- данните за създаване на електронен подпис/печат на практика се срещат само веднъж;
- данните за създаване на електронен подпис/печат са обезпечени в достатъчна степен и не могат да бъдат извлечени, а електронният подпис/печат е надеждно защитен срещу подправяне, чрез използване на наличната към момента технология;
- данните за създаване на електронен подпис могат да бъдат надеждно защитени от законния Титуляр/Създател на електронния подпис/печат срещу използване от други лица.

6.6.4 ОЦЕНКА НА ЖИЗНЕНИЯ ЦИКЪЛ НА СИГУРНОСТТА НА ТЕХНОЛОГИЧНАТА СИСТЕМА

„Практиката при предоставяне на квалифицирани удостоверителни услуги“ не предполага никакви изисквания в тази област.

6.7 МРЕЖОВА СИГУРНОСТ

В инфраструктурата на Евротръст се използват съвременни технически средства за обмен и защита на информация, за да се гарантира мрежовата сигурност на системите срещу външни интервенции и заплахи. Евротръст защитава мрежата и системите си от атаки прилагайки следните изисквания:

- Евротръст разделя своите системи в мрежи или зони на функционална, логическа и физическа (включително по местоположение) въз основа на оценката на риска и връзката между надеждните системи и услугите. Подробно описание на мрежовата конфигурация и средствата за защита са представени в техническа документация на инфраструктурата. Тази документация има „вътрешен“ статут и е достъпна само за оторизирани лица;
- Евротръст прилага едни и същи контроли за сигурност за всички системи, разположени в една и съща зона;
- Евротръст ограничава достъпа и комуникациите между зоните до необходимите за извършване на дейност. Опитите за неправомерен достъп до системата се документират чрез Intrusion Prevention System (IPS);

- Евротръст изрично забранява или деактивира ненужните връзки и услуги;
- Евротръст редовно преразглежда установения набор от правила;
- Евротръст поддържа всички системи, критични за работата му, в две защитени зони. Сървърите и критичната технологична система на Евротръст са свързани с вътрешна LAN мрежа. Отдалечения достъп до мрежата на инфраструктурата (PKI) на Евротръст се извършва чрез специално инсталиран и конфигуриран VPN сървър, който приема автентификация, чрез специално име и парола, издадени само за тази цел на оторизирани лица, участващи в издаването на електронен подпис/печат и администрирането на инфраструктурата (Public Key Infrastructure/ PKI);
- Евротръст има отделени специална мрежа за администриране на ИТ системите и оперативна мрежа;
- Евротръст не използва системи, използвани за администриране на прилагането на политиката за сигурност за други цели;
- Евротръст отделя системите за обслужване на удостоверителните услуги от системите, използвани за разработка и тестване;
- Евротръст установява комуникация между отделни надеждни системи само чрез доверени канали, които са изолирани чрез логическо, криптографско или физическо разделяне от други комуникационни канали и осигуряват гарантирана идентификация на своите крайни точки и защита на данните от канала от модификация или разкриване. Сървърите и критичната технологична система на Евротръст са свързани с вътрешна LAN мрежа. Отдалечения достъп до мрежата на инфраструктурата (PKI) на Евротръст се извършва чрез специално инсталиран и конфигуриран VPN сървър, който приема автентификация, чрез специално име и парола, издадени само за тази цел на оторизирани лица, участващи в издаването на електронен подпис/печат и администрирането на инфраструктурата (Public Key Infrastructure/ PKI).
- При необходимост от високо външно ниво на достъпност до удостоверителна услуга Евротръст осигурява високо ниво на сигурност на външния достъп до удостоверителна услуга посредством многоканална външна мрежова връзка, за да гарантира наличността на услугите в случай на един отказ;
- Евротръст извършва редовно сканиране на уязвимостта на идентифицираните публични и частни IP адреси и записва доказателства от този процес. За осигуряване на

надеждни доклади всяко сканиране на уязвимостта се извършено от упълномощено лице с необходимите умения, квалификации, инструменти, спазвайки етичния кодекс и липса на конфликт на интереси. Сканирането на уязвимости се извършва веднъж на тримесечие.

➤ След всяко актуализирани, модификация или надстройка на критични приложения Евротръст извършва тестове за проникване в системите;

➤ Евротръст записва доказателства, че всеки тест за проникване е извършен от оторизирано лице, притежаващо необходимите умения, инструменти, спазва етичния кодекс и няма конфликт на интереси с цел осигуряване на надежден доклад. Тестът за проникване се извършва поне веднъж годишно.

Подробно описание на мрежовата конфигурация на Евротръст и средствата за защита на Евротръст са представени в техническа документация на инфраструктурата. Тази документация има „вътрешен“ статут и е достъпна само за оторизирани лица.

7 ПРОФИЛИ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ, CRL И НА OCSP

Евротръст издава удостоверения с профили, които отговарят на изискванията, посочени в ITU-T X.509 или IETF RFC 5280.

Евротръст издава удостоверения със съответни профили, както следва:

а) за издаване на удостоверения на физически лица (с изключение на удостоверения за уеб сайт) (с приложими политики: NCP и NCP +) в съответствие с изискванията на ETSI EN 319 412-2;

б) за издаване на удостоверения на юридически лица (с изключение на удостоверения за уебсайтове) (с приложими политики: NCP и NCP +): в съответствие с изискванията на ETSI EN 319 412-3;

в) за издаване на удостоверения за уеб сайтове или устройства (с приложима политика: PTC): в съответствие с изискванията на ETSI EN 319 412-4.

7.1 ПРОФИЛ НА БАЗОВ УДОСТОВЕРЯВАЩ ОРГАН „EVROTRUST RSA ROOT“

Version	V3
Serial number	6C 6E C9 BF 48 51 72 A5 4B D4 0F 27 78 62 52 45
Signature Algorithm	SHA384RSA

Issuer	CN=	Evrotrust RSA Root CA
	OU=	Evrotrust Qualified Root
	O=	Evrotrust Technologies JSC
	organizationIdentifier	NTRBG-203397356
	C=	BG
Valid from	20 май 2016 г. 15:39:19 UTC	
Valid to	20 май 2036 г. 15:49:19 UTC	
Subject	CN=	Evrotrust RSA Root CA
	OU=	Evrotrust Qualified Root Authority
	O=	Evrotrust Technologies JSC
	organizationIdentifier (2.5.4.97)=	NTRBG-203397356
	C=	BG
Public Key Type/Length	RSA (4096 Bits)	
Subject Key Identifier	74 5c a1 40 73 2e 1f e6 f9 3b bc ab a0 a4 a7 54 44 74 4f 70	
Key Usage (critical)	Certificate Signing, Off-line CRL Signing, CRL Signing (06)	
Basic Constrains (critical)	Subject Type=CA Path Length Constraint=None	

7.2 ПРОФИЛ НА УДОСТОВЕРЯВАЩИ ОРГАНИ ЗА ПРОВЕРКА НА СТАТУС

Евротръст издава удостоверение за отговор с разумна продължителност.

Когато услугата се предлага като приложение на трети страни (SVA), които разчитат на услугите за информация за състоянието на удостоверенията издадени от Евротръст и не са в състояние да се справят с некритичното разширение и следователно да се окажат с оперативни проблеми, Евротръст допълнително осигурява проверка чрез CRL.

Когато са предоставени както OCSP, така и CRL, Евротръст конфигурира отговорите на OCSP за неиздадени удостоверения по начин, който изключва възможността неиздадени удостоверения да се появяват в CRL, като в тези случаи, ако отговорът е „отменен“ причината се идентифицирана. Евротръст наблюдава искания относно неиздадени удостоверения като част от процедурите за сигурност, за да провери дали това е индикация за атака.

а) Профил на отговор за онлайн проверка на статуса на удостоверение (OCSP/Online certificate status protocol)

Удостоверяващите органи за валидация „Evrotrust RSA Validation“ на базовия удостоверяващ орган „Evrotrust RSA Root CA“, „Evrotrust RSA QS Validation“ на оперативния удостоверяващ орган „Evrotrust RSA Operational CA“, „Evrotrust Services Validation“ и „Evrotrust RSA QOperational CA 2024 OCSP“ на оперативния удостоверяващ орган „Evrotrust Services CA“ на Евротръст работят и предоставят квалифицираната услуга „онлайн проверка на статус на удостоверение в реално време“ в съответствие с международно утвърдената препоръка IETF RFC 6960.

OCSP-потребителят изпраща искане за проверка на статус на подпис/печат до OCSP-сървър и получава отговор – удостоверение за статус, подписан от Органа за валидация. Отговорът съдържа информация за статуса на проверяваното удостоверение за електронен подпис/печат, периода на валидност на получения отговор и има доказателствен характер. OCSP сървърът, който издава потвърждения за състоянието на квалифицираните удостоверения притежава специално генерирана двойка ключове, издадени единствено за тази цел.

Евротръст, чрез своите Удостоверяващи органи за валидация, издава удостоверения за статус на издадените квалифицирани удостоверения във формат, определен в международната препоръка RFC 6960. Версията се вписва в издадените удостоверения за статус.

в) формат

Евротръст издава удостоверения за статус, чийто формат е в съответствие с изискванията в международната препоръка RFC 6960.

г) Основни атрибути на удостоверенията за статус

- Version - версия на удостоверението за статус;
- Response Type - тип на отговора за статус;
- OCSP Response Status - статус на отговора;
- Responder Id - Идентификатор на услугата по валидация
- Produced At - дата и час на издаване на удостоверението за статус;
- Responses - информация, уникално идентифицираща квалифицираното удостоверение, за което е отправено запитване и за което органа за валидация издава

настоящото удостоверение за статус;

- Cert Status - статус на квалифицираното удостоверение, за което е отправено запитване;
- This Update - времето на издаден CRL, на базата на който е издадено удостоверението за статус;
- Next Update - времето на валидност на CRL, на базата на който е издадено удостоверението за статус;
- Response Extensions - допълнителни разширения, включени в отговора;
- OCSP Nonce - съдържа същата информация, която е подадена при заявката в полето за Nonce;
- Signature Algorithm - използван алгоритъм за електронно подписване на удостоверението за статус;
- Certificate - Съдържа квалифицираното удостоверение на органа за валидация на Евротръст.

Съдържанието на удостоверението за статус на Евротръст е:

OCSP Response Status	• successful (0) - Валиден отговор на запитването; • malformedRequest (1) - Запитването не отговаря на изискванията за OCSP синтакс; • internalError (2) - Вътрешна грешка. Моля опитайте по-късно; • tryLater (3) - Услугата временно е недостъпна. Моля опитайте по-късно; • sigRequired (5) - Запитването трябва да е подписано; • unauthorized (6) - Клиента не е оторизиран да извърши запитването.
	Response Type
Version	1 (0x0)
Responder Id	[Уникален идентификатор на отговора на услугата]
Produced At	[дата и час по UTC на генериране на отговора]
Responses:	Certificate ID:

	Hash Algorithm - Използван хеш алгоритъм Issuer Name Hash- Хеш сума на името на издателя на удостоверението Issuer Key Hash - Хеш сума на публичния ключ на издателя на удостоверението Serial Number - Сериен номер на удостоверението
Cert Status	• good - удостоверението не присъства в CRL • unknown - не може да бъде открито такова удостоверение • revoked - удостоверението е спряно или прекратено;
This Update	[начална дата и час по UTC на валидност на издадения CRL, въз основа на който е генериран отговора]
Next Update	[дата и час по UTC на планирана актуализация на CRL]
OCSP Nonce:	[информация, която е подадена при заявката в полето за Nonce]
Signature Algorithm:	sha256WithRSAEncryption
Certificate:	[Квалифицираното удостоверение на органа за валидация]

7.2.1 ПРОФИЛ НА УДОСТОВЕРЯВАЩ ОРГАН „EVROTRUST RSA VALIDATION“

Съдържанието на удостоверението за статус „Evrotrust RSA Validation“ на базовия удостоверяващ орган „Evrotrust RSA Root CA“ е:

Version	V3	
Serial number	38:00:00:00:09:93:96:2D:78:FF:6E:BA:79:00:00:00:00:00:09	
Signature Algorithm	SHA256RSA	
Valid from	20210317095231Z	
Validit to	20260317100231Z	
Issuer	CN=	Evrotrust RSA Root CA
	OU=	Evrotrust Qualified Root Authority
	O=	Evrotrust Technologies JSC
	OrganizationIdentifier(2.5.4.97)=	NTRBG-203397356
	C=	BG
Subject	CN=	Evrotrust RSA Root CA OCSP
	OU=	OCSP Signing

	O=	Evrotrust Technologies JSC
	OrganizationIdentifier(2.5.4.97)=	NTRBG-203397356
	C=	BG
Public Key	RSA(2048 Bits)	
Subject Key Identifier	9C:F5:52:24:C8:91:5B:3B:AC:B0:1A:82:C5:8B:F8:06:25:5C:3B:46	
Key Usage (critical)	Digital Signature, Non Repudiation (c0)	
Extended Key Usage	OCSP Signing (1.3.6.1.5.5.7.3.9)	
Authority Key Identifier	74:5C:A1:40:73:2E:1F:E6:F9:3B:BC:AB:A0:A4:A7:54:44:74:4F:70	
OCSP No Revocation Checking	NULL	
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://ca.evrotrust.com/crl/EvrotrustRSARootCA.crl	

Thumbprint SHA1: 0BFA92A3EA5B058792618A270A0B196A18CDF07B

Thumbprint

SHA256:

77D7A7B05EC6BEA6AD3C80EFDAB2C0CA769F239821659EE7A86BEBE631217F12

7.2.2 ПРОФИЛ НА УДОСТОВЕРЯВАЩ ОРГАН „EVROTRUST RSA QS VALIDATION“

Съдържанието на удостоверение за статус „Evrotrust RSA QS Validation“ на оперативния удостоверяващ орган „Evrotrust RSA Operational CA“ е:

Version	V3
Serial number	5E:42:D8:F7:21:03:C4:BC:3F:C1:11:06:A8:D8:9E:DB:9D:3A:4C:3E
Signature Algorithm	SHA256RSA

Valid from	20210317111914Z	
Valid to	20260316111914Z	
Issuer	CN=	Evrotrust RSA Operational CA
	OU=	Qualified Operational CA
	O=	Evrotrust Technologies JSC
	organizationIdentifier (2.5.4.97)	NTRBG-203397356
	C=	BG
Subject	CN=	Evrotrust RSA Operational CA OCSP
	OU=	OCSP Signing
	O=	Evrotrust Technologies JSC
	OrganizationIdentifier(2.5.4.97)=	NTRBG-203397356
	C=	BG
Public Key	RSA(2048 Bits)	
Subject Key Identifier	E2:F3:4D:3A:F3:20:8A:71:55:D5:8D:97:FA:BB:73:5C:F5:77:24:E6	
Key Usage (critical)	Digital Signature, Non Repudiation (c0)	
Extended Key Usage	OCSP Signing (1.3.6.1.5.5.7.3.9)	
Authority Key Identifier	7F3E6459852BDD2329C201E7CBC369C087932B08	
OCSP No Revocation Checking	NULL	
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://ca.evrotrust.com/crl/EvrotrustRSAOperationalCA.crl	

Thumbprint SHA1: 3AAFAC82D429A697AEDFCCB9CB8C81FF805308CC

Thumbprint SHA256:

10DDCB60DCB2E600FA2ACE15DC79BEF9A3F2E6E375E2722CDBCE6319DD14968E

7.2.3 ПРОФИЛ НА УДОСТОВЕРЯВАЩ ОРГАН „EVROTRUST SERVICES VALIDATION“

Съдържанието на удостоверение за статус „Evrotrust Services Validation“ на оперативния удостоверяващ орган „Evrotrust Services CA“ е:

Version	V3
---------	----

Serial number	03ad545fd8129a1115c6f3e1cbdb23306731cc88	
Signature Algorithm	SHA256RSA	
Valid from	Feb 6 13:32:26 2024 GMT	
Validit to	Feb 4 13:32:25 2029 GMT	
Issuer	CN=	Evrotrust Services CA
	O=	Evrotrust Technologies JSC
	organizationIdentifier (2.5.4.97)	NTRBG-203397356
	C=	BG
Subject	CN=	Evrotrust Services OCSP 2024
	O=	Evrotrust Technologies JSC
	OrganizationIdentifier(2.5.4.97)=	NTRBG-203397356
	C=	BG
Public Key	RSA(2048 Bits)	
Subject Key Identifier	71d54d65955a8d93762399b91e398b3dabbe8208	
Key Usage (critical)	Digital Signature, Non Repudiation (c0)	
Extended Key Usage	OCSP Signing (1.3.6.1.5.5.7.3.9)	
Authority Key Identifier	KeyID=1b3a9e6d3191a15b461984fe9c98602c09d3332e	
OCSP No Revocation Checking	NULL	
Certificate Policies	[1]Certificate Policy: Policy Identifier= 1.3.6.1.4.1.47272.2.14.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.evrotrust.com/cps	
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://services.evrotrust.com/EvrotrustServicesCA.crl	
Basic Constraints (critical)	Subject Type=End Entity Path Length Constraint=None	

Thumbprint SHA256:

26650d3f5880e76d1e124a85a0b745ef141477d14073583879d606960eb64c8e

Thumbprint SHA1: 3d13ffe712c69a0c8ed1205f6328c058e30a7767

7.2.4 ПРОФИЛ НА УДОСТОВЕРЯВАЩ ОРГАН „EVROTRUST RSA QOPERATIONAL CA 2024 OCSP“

Съдържанието на удостоверението за статус „Evrotrust RSA QOperational CA 2024 OCSP“ на оперативния удостоверяващ орган „Evrotrust RSA QOperational CA 2024“ е:

Version	V3	
Serial number	73e6df8d5a69e0adcc6b8ee2a5ef3c1cfce27bfd	
Signature Algorithm	SHA256RSA	
Valid from	21 март 2025 г. 16:14:40 GMT	
Validit to	20 март 2030 г. 16:14:39 GMT	
Issuer	CN=	Evrotrust RSA QOperational CA 2024
	O=	Evrotrust Technologies JSC
	OU=	Qualified Operational CA
	organizationIdentifier (2.5.4.97)	NTRBG-203397356
	C=	BG
Subject	CN=	Evrotrust RSA QOperational CA 2024 OCSP
	O=	Evrotrust Technologies JSC
	OU=	OCSP Signing
	OrganizationIdentifier(2.5.4.97)=	NTRBG-203397356
	C=	BG
Public Key	RSA(2048 Bits)	
Subject Key Identifier	bf5e75ecdd4c592f617e792b2d0e8868f1a0cbae	
Key Usage (critical)	Digital Signature, Non Repudiation (c0)	
Extended Key Usage	OCSP Signing (1.3.6.1.5.5.7.3.9)	
Authority Key Identifier	KeyID=892b1433df16a3593cdefde203c89400dab9faa8	
OCSP No Revocation Checking	NULL	
Certificate Policies	[1]Certificate Policy:	

	Policy Identifier=1.3.6.1.4.1.47272.2.19.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.evrotrust.com/cps
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://ca.evrotrust.com/crl/EvrotrustRSAQOperationalCA2024.crl
Basic Constraints (critical)	Subject Type=End Entity Path Length Constraint=None

Thumbprint SHA256:

0190a31070aaa04b124dc25102aca1aa32730d0b450d23283842955d094b6126

Thumbprint SHA1: 43d8f688dd691a53fd6fbd1c70b3a2a975a84386

7.3 ПРОФИЛ НА ОПЕРАТИВЕН УДОСТОВЕРЯВАЩ ОРГАН „EVROTRUST RSA OPERATIONAL CA“

Version	V3	
Serial number	38 00 00 00 03 4e 8e cb 48 09 25 01 bc 00 00 00 00 00 03	
Signature Algorithm	SHA256RSA	
Issuer	CN=	Evrotrust RSA Root CA
	OU=	Evrotrust Qualified Root
	O=	Evrotrust Technologies JSC
	organizationIdentifier	NTRBG-203397356
	C=	BG
Valid from	21 май 2016 г. 00:34:35 UTC	
Valid to	21 май 2026 г. 03:44:35 UTC	
Subject	CN=	Evrotrust RSA Operational CA
	OU=	Qualified Operational CA
	O=	Evrotrust Technologies JSC
	organizationIdentifier	NTRBG-203397356

	(2.5.4.97)=(2.5.4.97)	
	C=	BG
Public Key Type/Length	RSA (2048 Bits)	
Subject Key Identifier	7f 3e 64 59 85 2b dd 23 29 c2 01 e7 cb c3 69 c0 87 93 2b 08	
Certificate Policies	[1]Certificate Policy: Policy Identifier=All issuance policies [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.evrotrust.com/cps	
Enhanced Key Usage	Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2) Code Signing (1.3.6.1.5.5.7.3.3) Secure Email (1.3.6.1.5.5.7.3.4) Time Stamping (1.3.6.1.5.5.7.3.8) OCSP Signing (1.3.6.1.5.5.7.3.9)	
Subject Alternative Name	URL= http://www.evrotrust.com RFC822 Name=ca@evrotrust.com	
Authority Key Identifier	KeyID=74 5c a1 40 73 2e 1f e6 f9 3b bc ab a0 a4 a7 54 44 74 4f 70	
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://ca.evrotrust.com/crl/EvrotrustRSARootCA.crl	
Authority Information Access	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name:	

	URL=http://ca.evrotrust.com/aia/EvrotrustRSARootCA.crt [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ca.evrotrust.com/ocsp
Key Usage (critical)	Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86)
Basic Constrains (critical)	Subject Type=CA Path Length Constraint=0

7.4 ПРОФИЛ НА ОПЕРАТИВЕН УДОСТОВЕРЯВАЩ ОРГАН „EVROTRUST SERVICES

CA”

Version	V3	
Serial number	38 00 00 00 07 58 F6 72 2B 87 3D 45 0D 00 00 00 00 00 07	
Signature Algorithm	SHA256RSA	
Issuer	CN=	Evrotrust RSA Root CA
	OU=	Evrotrust Qualified Root Authority
	O=	Evrotrust Technologies JSC
	organizationIdentifier	NTRBG-203397356
	C=	BG
Valid from	10 юли 2019 г. 12:50:59 UTC	
Validit to	10 юли 2029 г. 13:00:59 UTC	
Subject	CN=	Evrotrust Services CA
	OU=	Qualified Operational CA
	O=	Evrotrust Technologies JSC
	organizationIdentifier (2.5.4.97)= (2.5.4.97)	NTRBG-203397356
	C=	BG
Public Key Type/Length	RSA (2048 Bits)	

Subject Key Identifier	1B 3A 9E 6D 31 91 A1 5B 46 19 84 FE 9C 98 60 2C 09 D3 33 2E
Certificate Policies	[1]Certificate Policy: Policy Identifier=All issuance policies [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.evrotrust.com/cps
Subject Alternative Name	URL=http://www.evrotrust.com RFC822 Name= servicesca@evrotrust.com
Authority Key Identifier	KeyID=74 5c a1 40 73 2e 1f e6 f9 3b bc ab a0 a4 a7 54 44 74 4f 70
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://ca.evrotrust.com/crl/EvrotrustRSARootCA.crl
Authority Information Access	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://ca.evrotrust.com/aia/EvrotrustRSARootCA.crt [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ca.evrotrust.com/ocsp
Key Usage (critical)	Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86)
Basic Constraints (critical)	Subject Type=CA Path Length Constraint=0

Thumbprint SHA1: 7448B95DC14FF7127AF731C580E0D6CA74F3FE10

Thumbprint SHA256:

5C7AC0F5ADA82E251B4CB8D701A43A4A5BAF369289D4F29E27AB2690A88162EC

7.5 ПРОФИЛИ НА CRL-И

Профилът на CRL-те е както е определено в ISO/IEC 9594-8/Препоръка ITU-T X.509 или IETF RFC 5280:

а) Основни атрибути на Списъка със спрени и прекратени удостоверения (CRL)

- Version - версия на Списъка;
- Issuer Name - наименование на издателя на Списъка (Удостоверяващ орган);
- Effective Date/This update - дата и час на издаване на Списъка (CRL);
- Next Update - времето на валидност на CRL. След посоченото време,

Удостоверяващия орган издава незабавно нов Списък. През периода на валидност, в случай на прекратяване/спиране на удостоверение, Удостоверяващия орган издава автоматично нов CRL;

- Signature algorithm - идентификатор на алгоритъма за създаване на електронен подпис на CRL;

- Signature hash algorithm - алгоритъм за създаване на електронен подпис;

- ExpiredCertsOnCRL - идентификатор, указващ, че всички удостоверения, включително и тези с изтекъл срок на действие, са включени в този CRL.

б) Допълнителни атрибути в списъка със спрени и прекратени удостоверения (CRL)

„Authority Key Identifier“- идентификатора на Удостоверяващия орган, който издава и подписва Списъка със спрени и прекратени удостоверения (CRL), съдържа значението на „subjectKeyIdentifier“ от удостоверението на Удостоверяващия орган.

в) Формат на елемент в списъка със спрени и прекратени удостоверения (CRL)

Списъкът със спрени и прекратени удостоверения (CRL) на Удостоверяващия орган съдържа елементи за всички спрени удостоверения. Тези елементи са постоянни в Списъка.

Списъкът със спрени и прекратени удостоверения (CRL) на Удостоверяващия орган съдържа елемент за всяко спряно удостоверение от Удостоверяващия орган. Такъв елемент е временен в списъка до момента на възобновяване на удостоверението.

г) Атрибути на елемент в Списъкът със спрени и прекратени удостоверения (CRL)

- Serial number - сериен номер на спряно удостоверение;
- Revocation date - време на прекратяване/спиране на удостоверение;

- CRL Reason Code - код идентифициращ причината за прекратяване/спиране.

A) означения на причината за прекратяване/спиране на удостоверение

- keyCompromise - компрометиран частен ключ на Титуляр/Създател;
- ACompromise - компрометиран частен ключ на оперативен Удостоверяващ орган

на Евротръст;

➤ affiliationChange - променен статут на Титуляр спрямо друго лице - промяна в представителната власт, отнемане на представителната власт, прекратяване на трудово правоотношение и т.н;

- superseded - удостоверението е заместено с друго;
- certificateHold - действието на удостоверението временно е спряно.

7.5.1 CRL ПРОФИЛ НА БАЗОВИЯ УДОСТОВЕРЯВАЩ ОРГАН „EVROTRUST RSA ROOT CA“

Version	V2	
Issuer	CN=	Evrotrust RSA Root CA
	OU=	Evrotrust Qualified Root
	O=	Evrotrust Technologies
	organizationIdentifier	NTRBG-203397356
	C=	BG
Effective date	[начална дата и час по UTC на валидност на издадения CRL]	
Next update	[дата и час по UTC на планирана актуализация на CRL]	
Signature Algorithm	SHA256RSA	
Signature hash algorithm	SHA256	
Authority Key Identifier	KeyID=74 5c a1 40 73 2e 1f e6 f9 3b bc ab a0 a4 a7 54 44 74 4f 70	
CA Version	V0.0	
CRL Number	[пореден номер на CRL]	
ExpiredCertsOnCRL	[начална дата за включени удостоверения]	
Next CRL Publish	[дата и час по UTC на планирано публикуване на следващ CRL]	

7.5.2 CRL ПРОФИЛ НА ОПЕРАТИВНИЯ УДОСТОВЕРЯВАЩ ОРГАН „EVROTRUST RSA OPERATIONAL CA“

Version	V2	
Issuer	CN=	Evrotrust RSA Operational CA
	OU=	Qualified Operational CA
	O=	Evrotrust Technologies JSC
	organizationIdentifier	NTRBG-203397356
	C=	BG
Effective date	[начална дата и час по UTC на валидност на издадения CRL]	
Next update	[дата и час по UTC на планирана актуализация на CRL]	
Signature Algorithm	SHA256RSA	
Signature hash algorithm	SHA256	
Authority Key Identifier	KeyID=7f 3e 64 59 85 2b dd 23 29 c2 01 e7 cb c3 69 c0 87 93 2b 08	
CA Version	V0.0	
CRL Number	[пореден номер на CRL]	
expiredCertsOnCRL (OID=2.5.29.60)	[UTC дата, на която CRL започва да запазва информация за прекратените сертификати]	

7.5.3 CRL ПРОФИЛ НА ОПЕРАТИВНИЯ УДОСТОВЕРЯВАЩ ОРГАН „EVROTRUST SERVICES CA“

Version	V2	
Issuer	CN=	Evrotrust Services CA
	O=	Evrotrust Technologies JSC
	organizationIdentifier	NTRBG-203397356
	C=	BG
Effective date	[начална дата и час по UTC на валидност на издадения CRL]	
Next update	[дата и час по UTC на планирана актуализация на CRL]	
Signature Algorithm	SHA256RSA	
Signature hash algorithm	SHA256	
Authority Key Identifier	KeyID=1b 3a 9e 6d 31 91 a1 5b 46 19 84 fe 9c 98 60 2c 09	

	d3 33 2e
CRL Number	[пореден номер на CRL]
expiredCertsOnCRL (OID=2.5.29.60)	[UTC дата, на която CRL започва да запазва информация за прекратените сертификати]

7.5.4 CRL ПРОФИЛ НА ОПЕРАТИВНИЯ УДОСТОВЕРЯВАЩ ОРГАН „EVROTRUST RSA QOPERATIONAL CA 2024“

Version	V2	
Issuer	CN=	Evrotrust RSA QOperational CA 2024
	OU=	Qualified Operational CA
	O=	Evrotrust Technologies JSC
	organizationIdentifier	NTRBG-203397356
	C=	BG
Effective date	[начална дата и час по UTC на валидност на издадения CRL]	
Next update	[дата и час по UTC на планирана актуализация на CRL]	
Signature Algorithm	SHA256RSA	
Signature hash algorithm	SHA256	
Authority Key Identifier	KeyID=89 2b 14 33 df 16 a3 59 3c de fd e2 03 c8 94 00 da b9 fa a8	
CRL Number	[пореден номер на CRL]	
expiredCertsOnCRL (OID=2.5.29.60)	[UTC дата, на която CRL започва да запазва информация за прекратените сертификати]	

7.5.5 CRL ПРОФИЛ НА ОПЕРАТИВНИЯ УДОСТОВЕРЯВАЩ ОРГАН „EVROTRUST RSA REG.KE OPERATIONAL CA 2025“

Version	V2	
Issuer	CN=	Evrotrust RSA REG.KE Operational CA 2025
	O=	Evrotrust Technologies JSC
	organizationIdentifier	NTRBG-203397356

	C=	BG
Effective date	[начална дата и час по UTC на валидност на издадения CRL]	
Next update	[дата и час по UTC на планирана актуализация на CRL]	
Signature Algorithm	SHA256RSA	
Signature hash algorithm	SHA256	
Authority Key Identifier	KeyID=1e3c1d32408421b9f18da1eb5f4344175c33e6	
CRL Number	[пореден номер на CRL]	
expiredCertsOnCRL (OID=2.5.29.60)	[UTC дата, на която CRL започва да запазва информация за прекратените сертификати]	

7.6 ПРОФИЛИ НА ПОТРЕБИТЕЛСКИ УДОСТОВЕРЕНИЯ

а) съдържание на профил на квалифицирани удостоверения

В съответствие със стандарта X.509 v.3, електронното удостоверение е последователност от следните полета:

- Version: версия на удостоверението (X.509 v.3);
- SerialNumber: уникален идентификационен код на удостоверението;
- SignatureAlgorithm: идентификатор на алгоритъм за създаването на електронния подпис;
- Issuer: наименование на издателят на удостоверението (DN);
- Validity: срок на валидност, описан от дата и час на издаване на удостоверението (notBefore) до дата и час на изтичане на срока (notAfter) на удостоверението (универсално координирано време, представено във формат Zulu);
- Subject: уникалното име (DN) на Титуляря/Създателя, подлежащ на вписване в удостоверението;
- SubjectPublicKeyInfo: идентификатор на ключа;
- Signature: идентификатор на алгоритъм за създаването на електронния подпис/печат, в съответствие с RFC 5280.

б) Версия

Всички удостоверения, които издава Евротръст, са в съответствие с версия 3 (X.509 v.3).

в) Допустими разширения във формата на квалифицирано удостоверение

Стойностите на разширенията са създадени в съответствие с препоръката RFC 5280. Функцията на всяко разширение се определя от стандартната стойност на съответния идентификатор на обект (IDENTIFIER):

- Subject Key Identifier - формира се от публичния ключ, удостоверен в удостоверението като хеш-стойност на публичния ключ;
- Authority Key Identifier - формира се като хеш-стойност на публичния ключ на оперативния Удостоверяващ орган на Евротръст;
- Issuer Alternative Name - съдържа URL-стринг като алтернативно име на Евротръст;
- Basic Constrains - опционален и определя типа на удостоверението;
- Certificate Policy - определя идентификатора на Политиката за квалифицирано удостоверение за квалифициран електронен подпис/печат;
- Key Usage - атрибут, който определя ограниченията в употреба на удостоверението;
- Extended Key Usage - допълва значението на атрибут "Key Usage" и указва допълнителните и специфични приложения на удостоверението;
- CRL Distribution Point - съдържа връзка към актуалния CRL на оперативния Удостоверяващ орган на Евротръст;
- Authority Information Access - съдържа URL-адреса на OCSP сървър на удостоверението;
- Qualified Statements - атрибутът съдържа указание, че удостоверението е квалифицирано и показва дали частния ключ е генериран и се съхранява върху устройства за създаване на електронен подпис (QSCD).

г) Идентификатори на алгоритмите на електронен подпис/печат

Атрибутът „Signature algorithm“ идентифицира алгоритмите (криптографските механизми), които се използват.

В Евротръст се използва приложима комбинация на асиметрични и хеш алгоритми: sha256-with-RSA и sha384-with-RSA.

а) Форми на именуване

Формите на именуване са описани в частта „Видове имена“ на този документ.

е) Ограничения на имената

Видовете ограничения на имената са описани в частта „Видове имена“ на този документ.

ж) Идентификатор на Политика

Квалифицирано удостоверение се издават съгласно Политика на Евротръст, която се вписва в атрибута „Certificate Policy“ на удостоверението.

з) Идентификатор за продължение

Този идентификатор („Extensions“) дава специфична, свързана с услугата информация. За употребата му на този етап Практиката не поставя никакви ограничения.

и) Означение на квалифицираното удостоверение

Евротръст използва в квалифицирано удостоверение с профил по стандарта X.509 v.3 атрибута „Qualified Statements“ с идентификатор: „esi4-qcStatement-1“ (OID=0.4.0.1862.1.1).

Евротръст използва в квалифицирано удостоверение за квалифициран електронен подпис с профил по стандарта X.509 v.3 атрибута „Qualified Statements“ с идентификатори: „esi4-qcStatement-1“ (OID=0.4.0.1862.1.1) и „esi4-qcStatement-4“ (OID=0.4.0.1862.1.4).

Евротръст използва в квалифицирано удостоверение с профил по стандарта X.509 v.3 атрибута „Certificate Policy“, на който се присвоява идентификатора (OID) със значение, както следва:

Квалифицирано Удостоверение	Наименование	Идентификатор (OID) вписан в атрибута „Certificate Policy“
Квалифицирано удостоверение за квалифициран електронен подпис на физическо лице	Evrotrust Qualified Natural Person Certificate for QES	OID=1.3.6.1.4.1.47272.2.2
Квалифицирано атрибутивно удостоверение за квалифициран електронен подпис на физическо лице	Evrotrust Qualified Natural Person Attribute Certificate for QES	OID=1.3.6.1.4.1.47272.2.2.1
Квалифицирано удостоверение за квалифициран електронен	Evrotrust Qualified Legal Person Certificate for QESeal	OID=1.3.6.1.4.1.47272.2.3

Квалифицирано Удостоверение	Наименование	Идентификатор (OID) вписан в атрибута „Certificate Policy“
печат на юридическо лице/организация		
Квалифицирано удостоверение за усъвършенстван електронен подпис на физическо лице	Evrotrust Qualified Natural Person Certificate for AES	OID=1.3.6.1.4.1.47272.2.7
Квалифицирано удостоверение за усъвършенстван електронен печат на юридическо лице/организация	Evrotrust Qualified Legal Person Certificate for AESeal	OID=1.3.6.1.4.1.47272.2.8
Квалифицирано удостоверение за PSD2 усъвършенстван електронен печат на юридическо лице/организация	Evrotrust Qualified PSD2 Legal Person Certificate for AESeal	OID=1.3.6.1.4.1.47272.2.8.1
Квалифицирано удостоверение за автентичност на уебсайт за домейн	Evrotrust SSL Domain Validated Certificate	OID=1.3.6.1.4.1.47272.2.4.1
Квалифицирано удостоверение за автентичност на уебсайт за организация	Evrotrust SSL Organization Validated Certificate	OID=1.3.6.1.4.1.47272.2.4.2
Квалифицирано удостоверение за автентичност на уебсайт с	Evrotrust SSL EV Certificate	OID=1.3.6.1.4.1.47272.2.5

Квалифицирано Удостоверение	Наименование	Идентификатор (OID) вписан в атрибута „Certificate Policy“
разширено валидиране		
Квалифицирано удостоверение за автентичност на PSD2 уебсайт	Evrotrust SSL PSD2 Certificate	OID=1.3.6.1.4.1.47272.2.5.1
Квалифицирано удостоверение за квалифициран електронен подпис на физическо лице за регион KE	Evrotrust REG.KE Qualified Natural Person Certificate for QES	OID=1.3.6.1.4.1.47272.2.24
Квалифицирано удостоверение за усъвършенстван електронен подпис на физическо лице за регион KE	Evrotrust REG.KE Qualified Natural Person Certificate for AES	OID=1.3.6.1.4.1.47272.2.25
Квалифицирано атрибутивно удостоверение за квалифициран електронен подпис на физическо лице за регион KE	Evrotrust REG.KE Qualified Natural Person Attribute Certificate for QES	OID=1.3.6.1.4.1.47272.2.26
Други идентификатори (OID), вписани в атрибута "Certificate Policy" в квалифицираните удостоверения		
QCP-n: Удостоверителна политика на Европейския съюз (ЕС) за Квалифицирани удостоверения, издавани на физически лица	qcp-natural	OID=0.4.0.194112.1.0

Квалифицирано Удостоверение	Наименование	Идентификатор (OID) вписан в атрибута „Certificate Policy“
QCP-I: Удостоверителна политика на Европейския съюз (ЕС) за Квалифицирани удостоверения, издавани на юридически лица/организации	qcp-legal	OID=0.4.0.194112.1.1
QCP-n-qscd: Удостоверителна политика на Европейския съюз (ЕС) за Квалифицирани удостоверения, издавани на физически лица с частен ключ, свързан с удостоверения публичен ключ, разположен в QSCD	qcp-natural-qscd	OID=0.4.0.194112.1.2
QCP-l-qscd: Удостоверителна политика на Европейския съюз (ЕС) за Квалифицирани удостоверения, издавани на юридически лица/организации с частен ключ, свързан с удостоверения публичен ключ, разположен в QSCD	qcp-legal-qscd	OID=0.4.0.194112.1.3
QCP-w: Удостоверителна политика на Европейския	qcp-web	OID=0.4.0.194112.1.4

Квалифицирано Удостоверение	Наименование	Идентификатор (OID) вписан в атрибута „Certificate Policy“
съюз (ЕС) за удостоверения за автентичност на уебсайт		
OVCP (Organizational Validation Certificate Policy) според ETSI TS 102 042	ovcp	OID=0.4.0.2042.1.7

й) Използване на идентификатор за разширение на ключа „критично“

В Практиката няма изисквания за използване на „CRITICAL CERTIFICATE EXTENSIONS“.

**7.6.1 ПРОФИЛ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ ЗА КВАЛИФИЦИРАН
ЕЛЕКТРОНЕН ПОДПИС НА ФИЗИЧЕСКО ЛИЦЕ „EVROTRUST QUALIFIED NATURAL
PERSON CERTIFICATE FOR QES“**

КУКЕП издадено от Оперативен удостоверяващ орган "Evrotrust RSA Operational CA":

Version	V3	
Serial number	[сериен номер]	
Signature Algorithm	SHA256RSA	
Issuer	CN=	Evrotrust RSA Operational CA
	OU=	Qualified Operational CA
	O=	Evrotrust Technologies JSC
	organizationIdentifier	NTRBG-203397356
	C=	BG
Valid from	[начална дата и час по UTC на валидност на удостоверението]	
Validit to	[крайна дата и час по UTC на валидност на удостоверението]	
Subject	C=	Държава: Двубуквен код на държавата според ISO 3166. Указва общият контекст, в който трябва да се разбират други атрибути
	(countryName)	

		на полето Subject.
	CN= (commonName)	Обичайно име: Избрано от физическото лице име, с което то обичайно се представя. Когато не е избрано, се вписва пълното име на физическото лице.
	G= (givenName)	Собствено име: Име на физическото лице с документ за самоличност
	S= (surname)	Фамилно име: Фамилия на физическото лице с документ за самоличност
	или	
	2.5.4.65= (pseudonym)	Псевдоним: Псевдоним, избран от физическото
	SERIALNUMBER= (serialNumber)	Идентификатор на физическото лице (ETSI EN 319 412-1 т.5.1.3), например: - PNOBG-8310257645 за ЕГН; - PASSBG-12345678 за номер на паспорт; - IDCBG-195416023 за номер на лична карта; - TINBG-123434341 за ДДС номер. Ако лицето не желае да се вписва националният му идентификатор, се вписва клиентски номер, генерират от доставчика, с цел идентифициране на физическото лице при необходимост.
	Oi= (organizationName)	Наименование на юридическо лице: Пълно наименованието по регистрацията или акт на вписване на юридическото лице, с което физическото лице е асоциирано.

	2.5.4.97 ⁱ = (organizationIdentifier)	Идентификатор на юридическо лице (ETSI EN 319 412-1 т.5.1.4), например: - VARBG-123456789 - ДДС; - NTRBG-123456789 - ЕИК (БУЛСТАТ). Вписва се националния идентификатор според местното законодателство на
	E ⁱⁱ = (e-mailAddress)	Имейл адрес на Титуляря
Public Key Type/Length	RSA (2048/ 3072/ 4096 Bits)	
Subject Key Identifier	[Изчислена стойност за издаденото удостоверение]	
Authority Key Identifier	Key ID=7F3E6459852BDD2329C201E7CBC369C087932B08	
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://ca.evrotrust.com/crl/EvrotrustRSAOperationalCA.crl	
Authority Information Access	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://ca.evrotrust.com/aia/EvrotrustRSAOperationalCA.crt [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ca.evrotrust.com/ocsp	
Subject Alternative Name	RFC822 Name=[Имейл адрес на Титуляря]	

Enhanced Key Usage	Secure Email (1.3.6.1.5.5.7.3.4)												
Certificate Policies	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.47272.2.2 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.eurotrust.com/cps [2]Certificate Policy: Policy Identifier=0.4.0.194121.1.2												
Key Usage (critical)	Non-repudiation (Bit 1) ^{iv}												
QCStatements	<table border="1"> <tr> <td>id-qcs-pkixQCSyntax-v2ⁱ (oid=1.3.6.1.5.5.7.11.2)</td><td>id-etsi-qcs-semanticId-Natural (oid=0.4.0.194121.1.1) id-etsi-qcs-SemanticId-Legal (oid=0.4.0.194121.1.2)</td></tr> <tr> <td colspan="2">id-etsi-qcs-QcCompliance (oid=0.4.0.1862.1.1)</td></tr> <tr> <td>id-etsi-qcs-QcLimitValueⁱⁱⁱ (0.4.0.1862.1.2)</td><td>[Сума в EUR]</td></tr> <tr> <td colspan="2">id-etsi-qcs-QcSSCD (oid=0.4.0.1862.1.4)</td></tr> <tr> <td>id-etsi-qcs-QcType (oid=0.4.0.1862.1.6)</td><td>id-etsi-qct-esign (oid=0.4.0.1862.1.6.1)</td></tr> <tr> <td>id-etsi-qcs-QcPDS (oid=0.4.0.1862.1.5)</td><td>PdsLocations PdsLocation=https://www.eurotrust.com/pds/pds_en.pdf</td></tr> </table>	id-qcs-pkixQCSyntax-v2 ⁱ (oid=1.3.6.1.5.5.7.11.2)	id-etsi-qcs-semanticId- Natural (oid=0.4.0.194121.1.1) id-etsi-qcs-SemanticId- Legal (oid=0.4.0.194121.1.2)	id-etsi-qcs- QcCompliance (oid=0.4.0.1862.1.1)		id-etsi-qcs- QcLimitValue ⁱⁱⁱ (0.4.0.1862.1.2)	[Сума в EUR]	id-etsi-qcs- QcSSCD (oid=0.4.0.1862.1.4)		id-etsi-qcs- QcType (oid=0.4.0.1862.1.6)	id-etsi-qct- esign (oid=0.4.0.1862.1.6.1)	id-etsi-qcs- QcPDS (oid=0.4.0.1862.1.5)	PdsLocations PdsLocation= https://www.eurotrust.com/pds/pds_en.pdf
id-qcs-pkixQCSyntax-v2 ⁱ (oid=1.3.6.1.5.5.7.11.2)	id-etsi-qcs-semanticId- Natural (oid=0.4.0.194121.1.1) id-etsi-qcs-SemanticId- Legal (oid=0.4.0.194121.1.2)												
id-etsi-qcs- QcCompliance (oid=0.4.0.1862.1.1)													
id-etsi-qcs- QcLimitValue ⁱⁱⁱ (0.4.0.1862.1.2)	[Сума в EUR]												
id-etsi-qcs- QcSSCD (oid=0.4.0.1862.1.4)													
id-etsi-qcs- QcType (oid=0.4.0.1862.1.6)	id-etsi-qct- esign (oid=0.4.0.1862.1.6.1)												
id-etsi-qcs- QcPDS (oid=0.4.0.1862.1.5)	PdsLocations PdsLocation= https://www.eurotrust.com/pds/pds_en.pdf												

		language=en
--	--	-------------

КУКЕП издадено от Оперативен удостоверяващ орган "Evrotrust RSA QOperational CA 2024":

Version	V3	
Serial number	[сериен номер]	
Signature Algorithm	SHA256RSA	
Issuer	CN=	Evrotrust RSA QOperational CA 2024
	OU=	Qualified Operational CA
	O=	Evrotrust Technologies JSC
	organizationIdentifier	NTRBG-203397356
	C=	BG
Valid from	[начална дата и час по UTC на валидност на удостоверението]	
Validit to	[крайна дата и час по UTC на валидност на удостоверението]	
Subject	C= (countryName)	Държава: Двубуквен код на държавата според ISO 3166. Указва общият контекст, в който трябва да се разбират други атрибути на полето Subject.
	CN= (commonName)	Обичайно име: Избрано от физическото лице име, с което то обичайно се представя. Когато не е избрано, се вписва пълното име на физическото лице.

	G= (givenName)	Собствено име: Име на физическото лице документ за самоличност
	S= (surname)	Фамилно име: Фамилия на физическото лице документ за самоличност
	или	
	2.5.4.65= (pseudonym)	Псевдоним: Псевдоним, избран от физическо
	SERIALNUMBER= (serialNumber)	Идентификатор на физическото лице (ETSI EN 319 412-1 т.5.1.3), например: - PNOBG-8310257645 за ЕГН; - PASSBG-12345678 за номер на паспорт; - IDCBG-195416023 за номер на лична карта; - TINBG-123434341 за ДДС номер. Ако лицето не желае да се вписва националният му идентификатор, се вписва клиентски номер, генерират от доставчика, с цел идентифициране на физическото лице при необходимост.
	O ⁱ = (organizationName)	Наименование на юридическо лице: Пълно наименованието по регистрация или акт на вписване на юридическото лице, с което физическото лице е
	2.5.4.97 ⁱ = (organizationIdentifier)	Идентификатор на юридическо лице (ETSI EN 319 412-1 т.5.1.4), например: - VARBG-123456789 - ДДС; - NTRBG-123456789 - ЕИК (БУЛСТАТ). Вписва се националният идентификатор според местното законодателство на

	E ⁱⁱ = (e-mailAddress)	Имейл адрес на Титуляря
Public Key Type/Length	RSA (2048/ 3072/ 4096 Bits)	
Subject Key Identifier	[Изчислена стойност за издаденото удостоверение]	
Authority Key Identifier	Key ID=892b1433df16a3593cdefde203c89400dab9faa8	
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://ca.evrotrust.com/crl/EvrotrustRSAQOperationalCA2024.crl	
Authority Information Access	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://ca.evrotrust.com/aia/EvrotrustRSAQOperationalCA2024.crt [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL= http://ca.evrotrust.com/ocsp	
Subject Alternative Name	RFC822 Name=[Имейл адрес на Титуляря]	
Enhanced Key Usage	Secure Email (1.3.6.1.5.5.7.3.4)	
Certificate Policies	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.47272.2.2	

	[1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.evrotrust.com/cps [2]Certificate Policy: Policy Identifier=0.4.0.194112.1.2	
Key Usage (critical)	Non-repudiation (Bit 1) ^{iv}	
QCStatements	id-qcs- pkixQCSyntax-v2 ⁱ (oid=1.3.6.1.5.5.7.1 1.2)	id-etsi-qcs-semanticId- Natural (oid=0.4.0.194121.1.1) id-etsi-qcs-SemanticsId- Legal (oid=0.4.0.194121.1.2)
	id-etsi-qcs- QcCompliance (oid=0.4.0.1862.1.1)	
	id-etsi-qcs- QcLimitValue ⁱⁱⁱ (0.4.0.1862.1.2)	[Сума в EUR]
	id-etsi-qcs- QcSSCD (oid=0.4.0.1862.1.4)	
	id-etsi-qcs- QcType (oid=0.4.0.1862.1.6)	id-etsi-qct- esign (oid=0.4.0.1862.1.6.1)
	id-etsi-qcs- QcPDS (oid=0.4.0.1862.1.5)	PdsLocations PdsLocation=https://www.evrotrust.com/pds/pds_en.pdf language=en

7.6.2 ПРОФИЛ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ ЗА УСЪВЪРШЕНСТВАН ЕЛЕКТРОНЕН ПОДПИС НА ФИЗИЧЕСКО ЛИЦЕ „EVROTRUST QUALIFIED NATURAL PERSON CERTIFICATE FOR AES”

КУУЕП издадено от Оперативен удостоверяващ орган "Evrotrust RSA Operational CA":

Version	V3	
Serial number	[сериен номер]	
Signature Algorithm	SHA256RSA	
Issuer	CN=	Evrotrust RSA Operational CA
	OU=	Qualified Operational CA
	O=	Evrotrust Technologies JSC
	organizationIdentifier	NTRBG-203397356
	C=	BG
Valid from	[начална дата и час по UTC на валидност на удостоверението]	
Valid to	[крайна дата и час по UTC на валидност на удостоверението]	
Subject	C= (countryName)	Държава: Двубуквен код на държавата според ISO 3166. Указва общият контекст, в който трябва да се разбират други атрибути на полето Subject.
	CN= (commonName)	Обичайно име: Избрано от физическото лице име, с което то обичайно се представя. Когато не е избрано, се вписва пълното име на физическото лице.
	G= (givenName)	Собствено име: Име на физическото лице от документ за самоличност
	S= (surname)	Фамилно име: Фамилия на физическото лице от документ за самоличност
	Или	
	2.5.4.65= (pseudonym)	Псевдоним: Псевдоним, избран от физическото лице

	SERIALNUMBER= (serialNumber)	Идентификатор на физическото лице (ETSI EN 319 412-1 т.5.1.3), например: - PNOBG-8310257645 за ЕГН; - PASSBG-12345678 за номер на паспорт; - IDCBG-195416023 за номер на лична карта; - TINBG-123434341 за ДДС номер. Ако лицето не желае да се вписва националният му идентификатор, се вписва клиентски номер, генериран от доставчика, с цел идентифициране на физическото лице при необходимост.
	O ⁱ = (organizationName)	Наименование на юридическо лице: Пълно наименованието по регистрация или акт на вписване на юридическото лице, с което физическото лице е
	2.5.4.97 ⁱ = (organizationIdentifier)	Идентификатор на юридическо лице (ETSI EN 319 412-1 т.5.1.4), например: - VARBG-123456789 - ДДС; - NTRBG-123456789 - ЕИК (БУЛСТАТ). Вписва се националният идентификатор според местното законодателство на юридическото лице, с което физическото лице е асоциирано.
	E ⁱⁱ = (e-mailAddress)	Имейл адрес на Титуляря
Public Key Type/Length	RSA (2048/ 3072/ 4096 Bits)	
Subject Key	[Изчислена стойност за издаденото удостоверение]	

Identifier	
Authority Key Identifier	Key ID=7F3E6459852BDD2329C201E7CBC369C087932B08
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://ca.evrotrust.com/crl/EvrotrustRSAOperationalCA.crl
Authority Information Access	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://ca.evrotrust.com/aia/EvrotrustRSAOperationalCA.crt [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ca.evrotrust.com/ocsp
Subject Alternative Name	RFC822 Name=[Имейл адрес на Титуляря]
Enhanced Key Usage	Secure Email (1.3.6.1.5.5.7.3.4)
Certificate Policies	[1]Certificate Policy: Policy Identifier=0.4.0.194112.1.0 [2]Certificate Policy: Policy Identifier=1.3.6.1.4.1.47272.2.7 [2,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.evrotrust.com/cps
Key Usage (critical)	Non-repudiation (Bit 1) ^{iv}

QCStatements	id-qcs- pkixQCSyntax-v2 ⁱ (oid=1.3.6.1.5.5.7.11 .2)	id-etsi-qcs-semanticId- Natural (oid=0.4.0.194121.1.1) id-etsi-qcs-SemanticId- Legal (oid=0.4.0.194121.1.2)
	id-etsi-qcs- QcCompliance (oid=0.4.0.1862.1.1)	
	id-etsi-qcs- QcLimitValue ⁱⁱⁱ (0.4.0.1862.1.2)	[Сума в EUR]
	id-etsi-qcs- QcType (oid=0.4.0.1862.1.6)	id-etsi-qct- esign (oid=0.4.0.1862.1.6.1)
	id-etsi-qcs- QcPDS (oid=0.4.0.1862.1.5)	PdsLocations PdsLocation=https://www.eurotrust.com/pds/pds_en.pdf language=en

КУУЕП издадено от Оперативен удостоверяващ орган "Eurotrust RSA QOperational CA 2024":

Version	V3	
Serial number	[сериен номер]	
Signature Algorithm	SHA256RSA	
Issuer	CN=	Eurotrust RSA QOperational CA 2024
	OU=	Qualified Operational CA
	O=	Eurotrust Technologies JSC
	organizationIdentifier	NTRBG-203397356
	C=	BG
Valid from	[начална дата и час по UTC на валидност на удостоверението]	
Valid to	[крайна дата и час по UTC на валидност на удостоверението]	
Subject	C=	Държава: Двубуквен код на държавата според ISO 3166. Указва общият контекст,
	(countryName)	

		в който трябва да се разбират други атрибути на полето Subject.
	CN= (commonName)	Обичайно име: Избрано от физическото лице име, с което то обичайно се представя. Когато не е избрано, се вписва пълното име на физическото лице.
	G= (givenName)	Собствено име: Име на физическото лице в документ за самоличност
	S= (surname)	Фамилно име: Фамилия на физическото лице в документ за самоличност
	Или	
	2.5.4.65= (pseudonym)	Псевдоним: Псевдоним, избран от физическото лице
	SERIALNUMBER= (serialNumber)	Идентификатор на физическото лице (ETSI EN 319 412-1 т.5.1.3), например: - PNOBG-8310257645 за ЕГН; - PASSBG-12345678 за номер на паспорт; - IDCBG-195416023 за номер на лична карта; - TINBG-123434341 за ДДС номер. Ако лицето не желае да се вписва националният му идентификатор, се вписва клиентски номер, генерират от доставчика, с цел идентифициране на физическото лице при необходимост.
	Oi= (organizationName)	Наименование на юридическо лице: Пълно наименованието по регистрация или акт на вписване на юридическото лице, с което физическото лице е

	2.5.4.97 ⁱ = (organizationIdentifier)	Идентификатор на юридическо лице (ETSI EN 319 412-1 т.5.1.4), например: - VARBG-123456789 - ДДС; - NTRBG-123456789 - ЕИК (БУЛСТАТ). Вписва се националния идентификатор според местното законодателство на юридическото лице, с което физическото
	E ⁱⁱ = (e-mailAddress)	Имейл адрес на Титуляря
Public Key Type/Length	RSA (2048/ 3072/ 4096 Bits)	
Subject Key Identifier	[Изчислена стойност за издаденото удостоверение]	
Authority Key Identifier	Key ID=892b1433df16a3593cdefde203c89400dab9faa8	
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://ca.evrotrust.com/crl/EvrotrustRSAQOperationalCA2024.crl	
Authority Information Access	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://ca.evrotrust.com/aia/EvrotrustRSAQOperationalCA2024.crt [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL= http://ca.evrotrust.com/ocsp	

Subject Alternative Name	RFC822 Name=[Имейл адрес на Титуляря]	
Enhanced Key Usage	Secure Email (1.3.6.1.5.5.7.3.4)	
Certificate Policies	[1]Certificate Policy: Policy Identifier=0.4.0.194112.1.0 [2]Certificate Policy: Policy Identifier=1.3.6.1.4.1.47272.2.7 [2,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.evrotrust.com/cps	
Key Usage (critical)	Non-repudiation (Bit 1) ^{iv}	
QCStatements	id-qcs-pkixQCSyntax-v2 ⁱ (oid=1.3.6.1.5.5.7.11.2)	id-etsi-qcs-semanticId- Natural (oid=0.4.0.194121.1.1) id-etsi-qcs-SemanticId- Legal (oid=0.4.0.194121.1.2)
	id-etsi-qcs- QcCompliance (oid=0.4.0.1862.1.1)	
	id-etsi-qcs- QcLimitValue ⁱⁱⁱ (0.4.0.1862.1.2)	[Сума в EUR]
	id-etsi-qcs- QcType (oid=0.4.0.1862.1.6)	id-etsi-qct- esign (oid=0.4.0.1862.1.6.1)
	id-etsi-qcs- QcPDS (oid=0.4.0.1862.1.5)	PdsLocations PdsLocation= https://www.evrotrust.com/pds/pds_en.pdf language=en

7.6.3 ПРОФИЛ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ ЗА КВАЛИФИЦИРАН ЕЛЕКТРОНЕН ПЕЧАТ НА ЮРИДИЧЕСКО ЛИЦЕ „EVROTRUST QUALIFIED LEGAL PERSON CERTIFICATE FOR QESEAL“

КУКЕПечат издадено от Оперативен удостоверяващ орган "Evrotrust RSA Operational CA":

Version	V3	
Serial number	[сериен номер]	
Signature Algorithm	SHA256RSA	
Issuer	CN=	Evrotrust RSA Operational CA
	OU=	Qualified Operational CA
	O=	Evrotrust Technologies JSC
	organizationIdentifier	NTRBG-203397356
	C=	BG
Valid from	[начална дата и час по UTC на валидност на удостоверението]	
Validit to	[крайна дата и час по UTC на валидност на удостоверението]	
Subject	C= (countryName)	Държава: Двубуквен код на държавата според ISO 3166. Указва общият контекст, в който трябва да се разбират други атрибути на полето Subject.
	CN= (commonName)	Наименование на юридическото лице/организацията
	O= (organizationName)	Наименование на юридическото лице/организацията: Пълно наименованието по регистрация или акт на вписване на юридическото лице.

	2.5.4.97= (organizationIdentifier)	Идентификатор на юридическо лице (ETSI EN 319 412-1 т.5.1.4), например: - VARBG-123456789 - ДДС; - NTRBG-123456789 - ЕИК (БУЛСТАТ). Вписва се националния идентификатор според местното законодателство на юридическото лице, с което физическото лице е асоциирано.
		E ⁱⁱ = (e-mailAddress) Имейл адрес на Създателя на печата
Public Key Type/Length	RSA (2048/ 3072/ 4096 Bits)	
Subject Key Identifier	[Изчислена стойност за издаденото удостоверение]	
Authority Key Identifier	Key ID=7F3E6459852BDD2329C201E7CBC369C087932B08	
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://ca.evrotrust.com/crl/EvrotrustRSAOperationalCA.crl	
Authority Information Access	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://ca.evrotrust.com/aia/EvrotrustRSAOperationalCA.crt [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name:	

	URL=http://ca.evrotrust.com/ocsp	
Subject Alternative Name	RFC822 Name=[Имейл адрес на Създателя на печата]	
Enhanced Key Usage	Secure Email (1.3.6.1.5.5.7.3.4)	
Certificate Policies	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.47272.2.3 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.evrotrust.com/cps [2]Certificate Policy: Policy Identifier=0.4.0.194112.1.3	
Key Usage (critical)	Non-repudiation (Bit) ^{iv}	
QCStatements	id-qcs-pkixQCSyntax-v2 (oid=1.3.6.1.5.5.7.1.1.2)	id-etsi-qcs-SemanticsId- Legal (oid=0.4.0.194121.1.2)
	id-etsi-qcs- QcCompliance (oid=0.4.0.1862.1.1)	
	id-etsi-qcs- QcLimitValue ⁱⁱⁱ (0.4.0.1862.1.2)	[Сума в EUR]
	id-etsi-qcs- QcSSCD (oid=0.4.0.1862.1.4)	
	id-etsi-qcs- QcType (oid=0.4.0.1862.1.6)	id-etsi-qct- eseal (oid=0.4.0.1862.1.6.2)
	id-etsi-qcs- QcPDS (oid=0.4.0.1862.1.5)	PdsLocations PdsLocation=https://www.evrotrust.com/p

		ds/pds_en.pdf
		language=en

КУКЕПечат издадено от Оперативен удостоверяващ орган "Evrotrust RSA QOperational CA 2024":

Version	V3	
Serial number	[сериен номер]	
Signature Algorithm	SHA256RSA	
Issuer	CN=	Evrotrust RSA QOperational CA 2024
	OU=	Qualified Operational CA
	O=	Evrotrust Technologies JSC
	organizationIdentifier	NTRBG-203397356
	C=	BG
Valid from	[начална дата и час по UTC на валидност на удостоверението]	
Validit to	[крайна дата и час по UTC на валидност на удостоверението]	
Subject	C= (countryName)	Държава: Двубуквен код на държавата според ISO 3166. Указва общият контекст, в който трябва да се разбират други атрибути на полето Subject.
	CN= (commonName)	Наименование на юридическото лице/организацията
	O= (organizationName)	Наименование на юридическото лице/организацията: Пълно наименованието по регистрация или акт на вписване на юридическото лице.

	2.5.4.97= (organizationIdentifier)	Идентификатор на юридическо лице (ETSI EN 319 412-1 т.5.1.4), например: - VARBG-123456789 - ДДС; - NTRBG-123456789 - ЕИК (БУЛСТАТ). Вписва се националния идентификатор според местното законодателство на юридическото лице, с което физическото лице е асоциирано.
	E ⁱⁱ = (e-mailAddress)	Имейл адрес на Създателя на печата
Public Key Type/Length	RSA (2048/ 3072/ 4096 Bits)	
Subject Key Identifier	[Изчислена стойност за издаденото удостоверение]	
Authority Key Identifier	Key ID=892b1433df16a3593cdefde203c89400dab9faa8	
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://ca.evrotrust.com/crl/EvrotrustRSAQOperationalCA2024.crl	
Authority Information Access	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://ca.evrotrust.com/aia/EvrotrustRSAQOperationalCA2024.crt [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL= http://ca.evrotrust.com/ocsp	

Subject Alternative Name	RFC822 Name=[Имейл адрес на Създателя на печата]	
Enhanced Key Usage	Secure Email (1.3.6.1.5.5.7.3.4)	
Certificate Policies	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.47272.2.3 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.evrotrust.com/cps [2]Certificate Policy: Policy Identifier=0.4.0.194112.1.3	
Key Usage (critical)	Non-repudiation (Bit 1) ^{iv}	
QCStatements	id-qcs-pkixQCSyntax-v2 (oid=1.3.6.1.5.5.7.11.2)	id-etsi-qcs-SemanticsId- Legal (oid=0.4.0.194121.1.2)
	id-etsi-qcs- QcCompliance (oid=0.4.0.1862.1.1)	
	id-etsi-qcs- QcLimitValue ⁱⁱⁱ (0.4.0.1862.1.2)	[Сума в EUR]
	id-etsi-qcs- QcSSCD (oid=0.4.0.1862.1.4)	
	id-etsi-qcs- QcType (oid=0.4.0.1862.1.6)	id-etsi-qcs- eseal (oid=0.4.0.1862.1.6.2)
	id-etsi-qcs- QcPDS (oid=0.4.0.1862.1.5)	PdsLocations PdsLocation= https://www.evrotrust.com/pds/pds_en.pdf

		language=en
--	--	-------------

7.6.4 ПРОФИЛ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ ЗА УСЪВЪРШЕНСТВАН ЕЛЕКТРОНЕН ПЕЧАТ НА ЮРИДИЧЕСКО ЛИЦЕ „EVROTRUST QUALIFIED LEGAL PERSON CERTIFICATE FOR AESEAL“

КУУЕПечат издадено от Оперативен удостоверяващ орган "Evrotrust RSA Operational CA":

Version	V3	
Serial number	[сериен номер]	
Signature Algorithm	SHA256RSA	
Issuer	CN=	Evrotrust RSA Operational CA
	OU=	Qualified Operational CA
	O=	Evrotrust Technologies JSC
	organizationIdentifier	NTRBG-203397356
	C=	BG
Valid from	[начална дата и час по UTC на валидност на удостоверението]	
Validit to	[крайна дата и час по UTC на валидност на удостоверението]	
Subject	C= (countryName)	Държава: Двубуквен код на държавата според ISO 3166. Указва общият контекст, в който трябва да се разбират други атрибути на полето Subject.
	CN= (commonName)	Наименование на юридическото лице/организацията
	O= (organizationName)	Наименование на юридическото лице/организацията: Пълно наименованието по регистрация или акт на вписване на юридическото лице.

	2.5.4.97= (organizationIdentifier)	Идентификатор на юридическо лице (ETSI EN 319 412-1 т.5.1.4), например: - VARBG-123456789 (ДДС); - NTRBG-123456789 (ЕИК (БУЛСТАТ)). Вписва се националния идентификатор според местното законодателство на юридическото лице.
	E ⁱⁱ = (e-mailAddress)	Имейл адрес на Създателя на печата
Public Key Type/Length	RSA (2048/ 3072/ 4096 Bits)	
Subject Key Identifier	[Изчислена стойност за издаденото удостоверение]	
Authority Key Identifier	Key ID=7F3E6459852BDD2329C201E7CBC369C087932B08	
CRL Distribution Points	1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://ca.evrotrust.com/crl/EvrotrustRSAOperationalCA.crl	
Authority Information Access	1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://ca.evrotrust.com/aia/EvrotrustRSAOperationalCA.crt [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ca.evrotrust.com/ocsp	
Subject Alternative	RFC822 Name=[Имейл адрес на Създателя на печата]	

Name												
Enhanced Key Usage	Secure Email (1.3.6.1.5.5.7.3.4)											
Certificate Policies	[1]Certificate Policy: Policy Identifier=0.4.0.194112.1.1 [2]Certificate Policy: Policy Identifier=1.3.6.1.4.1.47272.2.8 [2,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.evrotrust.com/cps											
Key Usage (critical)	Non-repudiation (Bit 1) ^{iv}											
QCStatements*	<table><tr><td>id-qcs-pkixQCSyntax-v2 (oid=1.3.6.1.5.5.7.11.2)</td><td>id-etsi-qcs-SemanticsId-Legal (oid=0.4.0.194121.1.2)</td></tr><tr><td colspan="2">id-etsi-qcs-QcCompliance (oid=0.4.0.1862.1.1)</td></tr><tr><td>id-etsi-qcs-QcLimitValueⁱⁱⁱ (0.4.0.1862.1.2)</td><td>[Сума в EUR]</td></tr><tr><td>id-etsi-qcs-QcType (oid=0.4.0.1862.1.6)</td><td>id-etsi-qct-eseal (oid=0.4.0.1862.1.6.2)</td></tr><tr><td>id-etsi-qcs-QcPDS (oid=0.4.0.1862.1.5)</td><td>PdsLocations PdsLocation=https://www.evrotrust.com/pds/pds_en.pdf language=en</td></tr></table>		id-qcs-pkixQCSyntax-v2 (oid=1.3.6.1.5.5.7.11.2)	id-etsi-qcs-SemanticsId- Legal (oid=0.4.0.194121.1.2)	id-etsi-qcs- QcCompliance (oid=0.4.0.1862.1.1)		id-etsi-qcs- QcLimitValue ⁱⁱⁱ (0.4.0.1862.1.2)	[Сума в EUR]	id-etsi-qcs- QcType (oid=0.4.0.1862.1.6)	id-etsi-qct- eseal (oid=0.4.0.1862.1.6.2)	id-etsi-qcs- QcPDS (oid=0.4.0.1862.1.5)	PdsLocations PdsLocation=https://www.evrotrust.com/pds/pds_en.pdf language=en
id-qcs-pkixQCSyntax-v2 (oid=1.3.6.1.5.5.7.11.2)	id-etsi-qcs-SemanticsId- Legal (oid=0.4.0.194121.1.2)											
id-etsi-qcs- QcCompliance (oid=0.4.0.1862.1.1)												
id-etsi-qcs- QcLimitValue ⁱⁱⁱ (0.4.0.1862.1.2)	[Сума в EUR]											
id-etsi-qcs- QcType (oid=0.4.0.1862.1.6)	id-etsi-qct- eseal (oid=0.4.0.1862.1.6.2)											
id-etsi-qcs- QcPDS (oid=0.4.0.1862.1.5)	PdsLocations PdsLocation=https://www.evrotrust.com/pds/pds_en.pdf language=en											

2024":

Version	V3	
Serial number	[сериен номер]	
Signature Algorithm	SHA256RSA	
Issuer	CN=	Evrotrust RSA QOperational CA 2024
	OU=	Qualified Operational CA
	O=	Evrotrust Technologies JSC
	organizationIdentifier	NTRBG-203397356
	C=	BG
Valid from	[начална дата и час по UTC на валидност на удостоверението]	
Valid to	[крайна дата и час по UTC на валидност на удостоверението]	
Subject	C= (countryName)	Държава: Двубуквен код на държавата според ISO 3166. Указва общият контекст, в който трябва да се разбират други атрибути на полето Subject.
	CN= (commonName)	Наименование на юридическото лице/организацията
	O= (organizationName)	Наименование на юридическото лице/организацията: Пълно наименованието по регистрация или акт на вписване на юридическото лице.
	2.5.4.97= (organizationIdentifier)	Идентификатор на юридическо лице (ETSI EN 319 412-1 т.5.1.4), например: - VARBG-123456789 (ДДС); - NTRBG-123456789 (ЕИК (БУЛСТАТ)). Вписва се националният идентификатор според местното законодателство на юридическото лице.
	E= (e-mailAddress)	Имейл адрес на Създателя на печата
Public Key	RSA (2048/ 3072/ 4096 Bits)	

Type/Length	
Subject Identifier	Key [Изчислена стойност за издаденото удостоверение]
Authority Identifier	Key Key ID=892b1433df16a3593cdefde203c89400dab9faa8
CRL Points	Distribution [1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://ca.evrotrust.com/crl/EvrotrustRSAQOperationalCA2024.crl
Authority Information Access	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://ca.evrotrust.com/aia/EvrotrustRSAQOperationalCA2024.crt [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL= http://ca.evrotrust.com/ocsp
Subject Alternative Name	RFC822 Name=[Имейл адрес на Създателя на печата]
Enhanced Usage	Key Secure Email (1.3.6.1.5.5.7.3.4)
Certificate Policies	[1]Certificate Policy: Policy Identifier=0.4.0.194112.1.1 [2]Certificate Policy: Policy Identifier=1.3.6.1.4.1.47272.2.8 [2,1]Policy Qualifier Info: Policy Qualifier Id=CPS

	Qualifier: http://www.evrotrust.com/cps	
Key Usage (critical)	Non-repudiation (Bit 1) ^{iv}	
QCStatements*	id-qcs-pkixQCSyntax-v2 (oid=1.3.6.1.5.5.7.11.2)	id-etsi-qcs-SemanticsId- Legal (oid=0.4.0.194121.1.2)
	id-etsi-qcs- QcCompliance (oid=0.4.0.1862.1.1)	
	id-etsi-qcs- QcLimitValue ⁱⁱⁱ (0.4.0.1862.1.2)	[Сума в EUR]
	id-etsi-qcs- QcType (oid=0.4.0.1862.1.6)	id-etsi-qct- eseal (oid=0.4.0.1862.1.6.2)
	id-etsi-qcs- QcPDS (oid=0.4.0.1862.1.5)	PdsLocations PdsLocation= https://www.evrotrust.com/pds/pds_en.pdf language=en

7.6.5 ПРОФИЛ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ ПО PSD2 ЗА УСЪВЪРШЕНСТВАН ЕЛЕКТРОНЕН ПЕЧАТ НА ЮРИДИЧЕСКО ЛИЦЕ „EVROTRUST QUALIFIED PSD2 LEGAL PERSON CERTIFICATE FOR AESEAL“

Удостоверението се издава за целите на удостоверяването на юридическо лице/организация, свързана с Доставчик на платежни услуги (PSP) според PSD2. Има характера на квалифицирано удостоверение за усъвършенстван електронен печат по смисъла на Регламент (ЕС) № 910/2014 и се използва за електронно подписване на документи/данни за изпълнение на изискванията по PSD2.

PSD2 КУУЕПечат издадено от Оперативен удостоверяващ орган "Evrotrust RSA Operational CA":

Version	V3	
Serial number	[сериен номер]	
Signature Algorithm	SHA256RSA	
Issuer	CN=	Evrotrust RSA Operational CA
	OU=	Qualified Operational CA
	O=	Evrotrust Technologies JSC
	organizationIdentifier	NTRBG-203397356
	C=	BG
Valid from	[начална дата и час по UTC на валидност на удостоверението]	
Valid to	[крайна дата и час по UTC на валидност на удостоверението]	
Subject	C= (countryName)	Държава: Двубуквен код на държавата според ISO 3166. Указва общият контекст, в който трябва да се разбират други атрибути на полето Subject.
	CN= (commonName)	Наименование на юридическото лице/организацията
	O= (organizationName)	Наименование на юридическото лице/организацията: Пълно наименованието по регистрация или акт на вписване на юридическото лице.
	2.5.4.97= (organizationIdentifier)	Идентификатор на юридическо лице (ETSI TS 119 495 т.5.2.1), например: - PSDES-BDE-3DFD21 (PSD 2). Вписва се националния идентификатор според местното законодателство на юридическото лице.
Public Key	RSA (2048/3072/4096 Bits)	

Type/Length	
Subject Key Identifier	[Изчислена стойност за издаденото удостоверение]
Authority Key Identifier	Key ID=7F3E6459852BDD2329C201E7CBC369C087932B08
CRL Distribution Points	1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://ca.evrotrust.com/crl/EvrotrustRSAOperationalCA.crl
Authority Information Access	1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://ca.evrotrust.com/aia/EvrotrustRSAOperationalCA.crt [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ca.evrotrust.com/ocsp
Enhanced Usage	Secure Email (1.3.6.1.5.5.7.3.4)
Certificate Policies	[1]Certificate Policy: Policy Identifier=0.4.0.194112.1.1 [2]Certificate Policy: Policy Identifier=1.3.6.1.4.1.47272.2.8.1 [2,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier:

	http://www.evrotrust.com/cps	
Key Usage (critical)	Non-repudiation (Bit 1) ^{iv}	
QCStatements	id-qcs-pkixQCSyntax-v2 (oid=1.3.6.1.5.5.7.1.1.2)	id-etsi-qcs-SemanticsId- Legal (oid=0.4.0.194121.1.2)
	id-etsi-qcs- QcCompliance (oid=0.4.0.1862.1.1)	
	id-etsi-qcs- QcType (oid=0.4.0.1862.1.6)	id-etsi-qct- eseal (oid=0.4.0.1862.1.6.2)
	id-etsi-qcs- QcPDS (oid=0.4.0.1862.1.5)	PdsLocations PdsLocation=https://www.evrotrust.com/pds/pds_en.pdf language=en
	id-etsi- psd2 -qcStatement (oid=0.4.0.19495.2)	rolesOfPSP roleOfPspOid = 0.4.0.19495.1.1/2/3/4 roleOfPspName = PSP_AS/PSP_PI/PSP_AI/PSP_IC nCAName= Full name of the NCA nCAId= NCA abbreviated unique identifier

PSD2 КУУЕП издадено от Оперативен удостоверяващ орган "Evrotrust RSA QOperational CA 2024":

Version	V3
Serial number	[сериен номер]

Signature Algorithm	SHA256RSA	
Issuer	CN=	Evrotrust RSA QOperational CA 2024
	OU=	Qualified Operational CA
	O=	Evrotrust Technologies JSC
	organizationIdentifier	NTRBG-203397356
	C=	BG
Valid from	[начална дата и час по UTC на валидност на удостоверението]	
Valid to	[крайна дата и час по UTC на валидност на удостоверението]	
Subject	C= (countryName)	Държава: Двубуквен код на държавата според ISO 3166. Указва общият контекст, в който трябва да се разбират други атрибути на полето Subject.
	CN= (commonName)	Наименование на юридическото лице/организацията
	O= (organizationName)	Наименование на юридическото лице/организацията: Пълно наименованието по регистрация или акт на вписване на юридическото лице.
	2.5.4.97= (organizationIdentifier)	Идентификатор на юридическо лице (ETSI TS 119 495 т.5.2.1), например: - PSDES-BDE-3DFD21 (PSD 2). Вписва се националният идентификатор според местното законодателство на юридическото лице.
Public Key Type/Length	RSA (2048/3072/4096 Bits)	
Subject Key Identifier	[Изчислена стойност за издаденото удостоверение]	

Authority Identifier	Key ID=892b1433df16a3593cdefde203c89400dab9faa8
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://ca.evrotrust.com/crl/EvrotrustRSAQOperationalCA2024.crl
Authority Information Access	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://ca.evrotrust.com/aia/EvrotrustRSAQOperationalCA2024.crt [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ca.evrotrust.com/ocsp
Enhanced Usage	Secure Email (1.3.6.1.5.5.7.3.4)
Certificate Policies	[1]Certificate Policy: Policy Identifier=0.4.0.194112.1.1 [2]Certificate Policy: Policy Identifier=1.3.6.1.4.1.47272.2.8.1 [2,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.evrotrust.com/cps
Key Usage (critical)	Non-repudiation (Bit 1) ^{iv}
QCStatements	

	id-qcs- pkixQCSyntax-v2 (oid=1.3.6.1.5.5.7.1 1.2)	id-etsi-qcs-SemanticsId- Legal (oid=0.4.0.194121.1.2)
	id-etsi-qcs- QcCompliance (oid=0.4.0.1862.1.1)	
	id-etsi-qcs- QcType (oid=0.4.0.1862.1. 6)	id-etsi-qct- eseal (oid=0.4.0.1862.1.6.2)
	id-etsi-qcs- QcPDS (oid=0.4.0.1862.1. 5)	PdsLocations PdsLocation=https://www.evrotrust.com/ pds/pds_en.pdf language=en
	id-etsi- psd2 - qcStatement (oid=0.4.0.19495.2)	rolesOfPSP roleOfPspOid = 0.4.0.19495.1.1/2/3/4 roleOfPspName = PSP_AS/PSP_PI/PSP_AI/PSP_IC nCAName= Full name of the NCA nCAId= NCA abbreviated unique identifier

7.6.6 ПРОФИЛ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ ЗА АВТЕНТИЧНОСТ НА УЕБСАЙТ ЗА ОРГАНИЗАЦИЯ „EVROTRUST SSL ORGANIZATION VALIDATED CERTIFICATE”

SSL издадено от Оперативен удостоверяващ орган "Evrotrust RSA Operational CA":

Version	V3	
Serial number	[сериен номер]	
Signature Algorithm	SHA256RSA	
Issuer	CN=	Evrotrust RSA Operational CA
	OU=	Qualified Operational CA

	O=	Evrotrust Technologies JSC
	organizationIdentifier	NTRBG-203397356
	C=	BG
Valid from	[начална дата и час по UTC на валидност на удостоверението]	
Valid to	[крайна дата и час по UTC на валидност на удостоверението]	
Subject	C= (countryName)	Държава: Двубуквен код на държавата според ISO 3166. Указва общият контекст, в който трябва да се разбират други атрибути на полето Subject.
	CN= (commonName)	Домейн име, IP или Име на ресурс
	O ⁱ = (organizationName)	Наименование на лицето: Пълно наименованието по регистрацията или акт на вписване на юридическото лице.
	OU ⁱ = (organizationalUnitName)	Наименование на организационна единица/Отдел
	2.5.4.97 ⁱ = (organizationIdentifier)	Идентификатор на юридическо лице (ETSI EN 319 412-1 т.5.1.4), например: - VARBG-123456789 (АДС); - NTRBG-123456789 (ЕИК (БУЛСТАТ)). Вписва се националният идентификатор според местното законодателство на юридическото лице.
	ST ⁱ = (stateOrProvinceName)	Регион/област/щат на юридическото лице.
	L ⁱ =	Град/населено място на

	(localityName)	юридическото лице.
Public Key Type/Length	RSA (2048/3072/4096 Bits)	
Subject Key Identifier	[Изчислена стойност за издаденото удостоверение]	
Authority Key Identifier	Key ID=7F3E6459852BDD2329C201E7CBC369C087932B08	
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://ca.evrotrust.com/crl/EvrotrustRSAOperationalCA.crl	
Authority Information Access	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://ca.evrotrust.com/aia/EvrotrustRSAOperationalCA.crt [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ca.evrotrust.com/ocsp	
Enhanced Key Usage	Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2)	
Subject Alternative Name	DNS Name=[Домейн име или IP]	
Certificate Policies	[1]Certificate Policy: Policy Identifier=0.4.0.2042.1.7 [2]Certificate Policy:	

	Policy Identifier=1.3.6.1.4.1.47272.2.4.2 [2,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.evrotrust.com/cps
Key Usage (critical)	Digital Signature (Bit 0), Key Encipherment (Bit 2)

SSL издадено от Оперативен удостоверяващ орган "Evrotrust RSA QOperational CA 2024":

Version	V3	
Serial number	[сериен номер]	
Signature Algorithm	SHA256RSA	
Issuer	CN=	Evrotrust RSA QOperational CA 2024
	OU=	Qualified Operational CA
	O=	Evrotrust Technologies JSC
	organizationIdentifier	NTRBG-203397356
	C=	BG
Valid from	[начална дата и час по UTC на валидност на удостоверението]	
Validit to	[крайна дата и час по UTC на валидност на удостоверението]	
Subject	C= (countryName)	Държава: Двубуквен код на държавата според ISO 3166. Указва общият контекст, в който трябва да се разбират други атрибути на полето Subject.
	CN= (commonName)	Домейн име, IP или Име на ресурс
	O ⁱ = (organizationName)	Наименование на лицето: Пълно наименованието по регистрация или акт на вписване на юридическото лице.
	OU ⁱ =	Наименование на организационна

	(organizationalUnitName)	единица/Отдел
	2.5.4.97 ⁱ = (organizationIdentifier)	Идентификатор на юридическо лице (ETSI EN 319 412-1 т.5.1.4), например: - VARBG-123456789 (ДДС); - NTRBG-123456789 (ЕИК (БУЛСТАТ)). Вписва се националния идентификатор според местното законодателство на юридическото лице.
	ST ⁱ = (stateOrProvinceName)	Регион/област/щат на юридическото лице.
	L ⁱ = (localityName)	Град/населено място на юридическото лице.
Public Key Type/Length	RSA (2048/3072/4096 Bits)	
Subject Key Identifier	[Изчислена стойност за издаденото удостоверение]	
Authority Key Identifier	Key ID=892b1433df16a3593cdefde203c89400dab9faa8	
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://ca.evrotrust.com/crl/EvrotrustRSAQOperationalCA2024.crl	
Authority Information Access	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name:	

	URL= http://ca.evrotrust.com/aia/EvrotrustRSAQOperationalCA2024.crt [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL= http://ca.evrotrust.com/ocsp
Enhanced Key Usage	Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2)
Subject Alternative Name	DNS Name=[Домейн име или IP]
Certificate Policies	[1]Certificate Policy: Policy Identifier=0.4.0.2042.1.7 [2]Certificate Policy: Policy Identifier=1.3.6.1.4.1.47272.2.4.2 [2,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.evrotrust.com/cps
Key Usage (critical)	Digital Signature (Bit 0), Key Encipherment (Bit 2)

7.6.7 ПРОФИЛ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ ЗА АВТЕНТИЧНОСТ НА УЕБСАЙТ С РАЗШИРЕНО ВАЛИДИРАНЕ „EVROTRUST SSL EV CERTIFICATE“

Удостоверението се издава за целите на удостоверяването на уебсайт, свързан с конкретно физическото или юридическото лице. Има характера на квалифицирано удостоверение за уебсайт по смисъла на Регламента и се използва за създаване на увереност у посетител, че уебсайта е на реален и легитимен субект. Чрез технологията се обезпечават надеждна свързаност по сигурен протокол за обмен на информацията.

SSL издадено от Оперативен удостоверяващ орган "Evrotrust RSA Operational CA":

Version	V3
---------	----

Serial number	[сериен номер]	
Signature Algorithm	SHA256RSA	
Issuer	CN=	Evrotrust RSA Operational CA
	OU=	Qualified Operational CA
	O=	Evrotrust Technologies JSC
	organizationIdentifier (2.5.4.97)=(2.5.4.97)	NTRBG-203397356
	C=	BG
Valid from	[начална дата и час по UTC на валидност на удостоверението]	
Valid to	[крайна дата и час по UTC на валидност на удостоверението]	
Subject	C= (countryName)	Държава: Двубуквен код на държавата според ISO 3166. Указва общият контекст, в който трябва да се разбират други атрибути на полето Subject.
	CN= (commonName)	Домейн име, IP или Име на ресурс
	O ⁱ = (organizationName)	Наименование на юридическо лице: Пълно наименованието по регистрацията или акт на вписване на юридическото лице.
	2.5.4.97 ⁱ = (organizationIdentifier)	Идентификатор на юридическо лице (ETSI EN 319 412-1 т.5.1.4), например: - VARBG-123456789 (ДДС); - NTRBG-123456789 (ЕИК (БУЛСТАТ)). Вписва се националният идентификатор според местното законодателство на юридическото лице.
Public Key Type/Length	RSA (2048/3072/4096 Bits)	

Subject Identifier	Key	[Изчислена стойност за издаденото удостоверение]
Authority Identifier	Key	Key ID=7F3E6459852BDD2329C201E7CBC369C087932B08
CRL Distribution Points		[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://ca.evrotrust.com/crl/EvrotrustRSAOperationalCA.crl
Authority Information Access		[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://ca.evrotrust.com/aia/EvrotrustRSAOperationalCA.crt [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ca.evrotrust.com/ocsp
Enhanced Usage	Key	Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2)
Subject Alternative Name		DNS Name=[Домейн име или IP]
Certificate Policies		[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.47272.2.5 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.evrotrust.com/cps

	[2]Certificate Policy: Policy Identifier=0.4.0.194112.1.4	
Key Usage (critical)	Digital Signature (Bit 0), Key Encipherment (Bit 2)	
QCStatements	id-qcs- pkixQCSyntax-v2 ⁱ (oid=1.3.6.1.5.5.7.11.2)	id-etsi-qcs-SemanticsId- Legal (oid=0.4.0.194121.1.2)
	id-etsi-qcs- QcCompliance (oid=0.4.0.1862.1.1)	
	id-etsi-qcs- QcLimitValue ⁱⁱⁱ (0.4.0.1862.1.2)	[Сума в EUR]
	id-etsi-qcs- QcType (oid=0.4.0.1862.1.6)	id-etsi-qct- web (oid=0.4.0.1862.1.6.3)
	id-etsi-qcs- QcPDS (oid=0.4.0.1862.1.5)	PdsLocations PdsLocation=https://www.evrotrust.com/pds/pds_en.pdf language=en

SSL издадено от Оперативен удостоверяващ орган "Evrotrust RSA QOperational CA 2024":

Version	V3	
Serial number	[сериен номер]	
Signature Algorithm	SHA256RSA	
Issuer	CN=	Evrotrust RSA QOperational CA 2024
	OU=	Qualified Operational CA
	O=	Evrotrust Technologies JSC

	organizationIdentifier (2.5.4.97)= (2.5.4.97)	NTRBG-203397356
	C=	BG
Valid from	[начална дата и час по UTC на валидност на удостоверението]	
Validit to	[крайна дата и час по UTC на валидност на удостоверението]	
Subject	C= (countryName)	Държава: Двубуквен код на държавата според ISO 3166. Указва общият контекст, в който трябва да се разбират други атрибути на полето Subject.
	CN= (commonName)	Домейн име, IP или Име на ресурс
	O ⁱ = (organizationName)	Наименование на юридическо лице: Пълно наименованието по регистрацията или акт на вписване на юридическото лице.
	2.5.4.97 ⁱ = (organizationIdentifier)	Идентификатор на юридическо лице (ETSI EN 319 412-1 т.5.1.4), например: - VARBG-123456789 (ДДС); - NTRBG-123456789 (ЕИК (БУЛСТАТ)). Вписва се националният идентификатор според местното законодателство на юридическото лице.
Public Key Type/Length	RSA (2048/3072/4096 Bits)	
Subject Key Identifier	[Изчислена стойност за издаденото удостоверение]	
Authority Key Identifier	Key ID=892b1433df16a3593cdefde203c89400dab9faa8	
CRL Distribution	[1]CRL Distribution Point	

Points	Distribution Point Name: Full Name: URL= http://ca.evrotrust.com/crl/EvrotrustRSAQOperationalCA2024.crl			
Authority Information Access	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://ca.evrotrust.com/aia/EvrotrustRSAQOperationalCA2024.crt [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ca.evrotrust.com/ocsp			
Enhanced Key Usage	Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2)			
Subject Alternative Name	DNS Name=[Домейн име или IP]			
Certificate Policies	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.47272.2.5 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.evrotrust.com/cps [2]Certificate Policy: Policy Identifier=0.4.0.194112.1.4			
Key Usage (critical)	Digital Signature (Bit 0), Key Encipherment (Bit 2)			
QCStatements	<table><tr><td>id-qcs-</td><td>id-etsi-qcs-SemanticsId-Legal</td></tr></table>		id-qcs-	id-etsi-qcs-SemanticsId- Legal
id-qcs-	id-etsi-qcs-SemanticsId- Legal			

	pkixQCSyntax-v2 ⁱ (oid=1.3.6.1.5.5.7.11.2)	(oid=0.4.0.194121.1.2)
	id-etsi-qcs- QcCompliance (oid=0.4.0.1862.1.1)	
	id-etsi-qcs- QcLimitValue ⁱⁱⁱ (0.4.0.1862.1.2)	[Сума в EUR]
	id-etsi-qcs- QcType (oid=0.4.0.1862.1.6)	id-etsi-qct- web (oid=0.4.0.1862.1.6.3)
	id-etsi-qcs- QcPDS (oid=0.4.0.1862.1.5)	PdsLocations PdsLocation=https://www.evrotrust.com/pds/pds_en.pdf language=en

7.6.8 ПРОФИЛ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ ЗА АВТЕНТИЧНОСТ НА PSD2 УЕБСАЙТ „EVROTRUST SSL PSD2 CERTIFICATE“

Удостоверението се издава целите на удостоверяването на уебсайт, свързан с Доставчик на платежни услуги (PSP) според PSD2. Използва се за изпълнение на изискванията на PSD2. Има характера на квалифицирано удостоверение за уебсайт по смисъла на Регламента и се използва за създаване на увереност у посетител, че уебсайта е на реален и легитимен субект. Чрез технологията се обезпечават надеждна свързаност по сигурен протокол за обмен на информацията.

PSD2 SSL издадено от Оперативен удостоверяващ орган "Evrotrust RSA Operational CA":

Version	V3
Serial number	[сериен номер]

Signature Algorithm	SHA256RSA	
Issuer	CN=	Evrotrust RSA Operational CA
	OU=	Qualified Operational CA
	O=	Evrotrust Technologies JSC
	organizationIdentifier	NTRBG-203397356
	C=	BG
Valid from	[начална дата и час по UTC на валидност на удостоверението]	
Valid to	[крайна дата и час по UTC на валидност на удостоверението]	
Subject	C= (countryName)	Държава: Двубуквен код на държавата според ISO 3166. Указва общият контекст, в който трябва да се разбират други атрибути на полето Subject.
	CN= (commonName)	Домейн име, IP или Име на ресурс
	O ⁱ = (organizationName)	Наименование на юридическо лице: Пълно наименованието по регистрация или акт на вписване на юридическото лице.
	2.5.4.97 ⁱ = (organizationIdentifier)	Идентификатор на юридическо лице (ETSI TS 119 495 т.5.2.1), например: - PSDES-BDE-3DFD21 (PSD 2). Вписва се националния идентификатор според местното законодателство на юридическото лице.
Public Key Type/Length	RSA (2048/3072/4096 Bits)	
Subject Key Identifier	[Изчислена стойност за издаденото удостоверение]	

Authority Key Identifier	Key ID=7F3E6459852BDD2329C201E7CBC369C087932B08
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://ca.evrotrust.com/crl/EvrotrustRSAOperationalCA.crl
Authority Information Access	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://ca.evrotrust.com/aia/EvrotrustRSAOperationalCA.crt [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ca.evrotrust.com/ocsp
Enhanced Key Usage	Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2)
Subject Alternative Name	DNS Name=[Домейн име или IP]
Certificate Policies	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.47272.2.5.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.evrotrust.com/cps [2]Certificate Policy: Policy Identifier=0.4.0.194112.1.4
Key Usage (critical)	Digital Signature (Bit 0), Key Encipherment (Bit 2)

QCStatements	id-qcs- pkixQCSyntax-v2 ⁱ (oid=1.3.6.1.5.5.7.1 1.2)	id-etsi-qcs-SemanticsId- Legal (oid=0.4.0.194121.1.2)
	id-etsi-qcs- QcCompliance (oid=0.4.0.1862.1.1)	
	id-etsi-qcs- QcLimitValue ⁱⁱⁱ (0.4.0.1862.1.2)	[Сума в EUR]
	id-etsi-qcs- QcType (oid=0.4.0.1862.1.6)	id-etsi-qct- web (oid=0.4.0.1862.1.6.3)
	id-etsi-qcs- QcPDS (oid=0.4.0.1862.1.5)	PdsLocations PdsLocation=https://www.evrotrust.com /pds/pds_en.pdf language=en
	id-etsi- psd2 - qcStatement (oid=0.4.0.19495.2)	rolesOfPSP roleOfPspOid = 0.4.0.19495.1.1/2/3/4 roleOfPspName = PSP_AS/PSP_PI/PSP_AI/PSP_IC nCAName= Full name of the NCA nCAId= NCA abbreviated unique identifier

PSD2 SSL издадено от Оперативен удостоверяващ орган "Evrotrust RSA QOperational CA 2024":

Version	V3

Serial number	[сериен номер]	
Signature Algorithm	SHA256RSA	
Issuer	CN=	Evrotrust RSA QOperational CA 2024
	OU=	Qualified Operational CA
	O=	Evrotrust Technologies JSC
	organizationIdentifier	NTRBG-203397356
	C=	BG
Valid from	[начална дата и час по UTC на валидност на удостоверението]	
Valid to	[крайна дата и час по UTC на валидност на удостоверението]	
Subject	C= (countryName)	Държава: Двубуквен код на държавата според ISO 3166. Указва общият контекст, в който трябва да се разбират други атрибути на полето Subject.
	CN= (commonName)	Домейн име, IP или Име на ресурс
	O ⁱ = (organizationName)	Наименование на юридическо лице: Пълно наименованието по регистрацията или акт на вписване на юридическото лице.
	2.5.4.97 ⁱ = (organizationIdentifier)	Идентификатор на юридическо лице (ETSI TS 119 495 т.5.2.1), например: - PSDES-BDE-3DFD21 (PSD 2). Вписва се националният идентификатор според местното законодателство на юридическото лице.
Public Key Type/Length	RSA (2048/3072/4096 Bits)	
Subject Key	[Изчислена стойност за издаденото удостоверение]	

Identifier	
Authority Key Identifier	Key ID=892b1433df16a3593cdefde203c89400dab9faa8
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://ca.evrotrust.com/crl/EvrotrustRSAQOperationalCA2024.crl
Authority Information Access	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://ca.evrotrust.com/aia/EvrotrustRSAQOperationalCA2024.crt [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL= http://ca.evrotrust.com/ocsp
Enhanced Key Usage	Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2)
Subject Alternative Name	DNS Name=[Домейн име или IP]
Certificate Policies	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.47272.2.5.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.evrotrust.com/cps [2]Certificate Policy: Policy Identifier=0.4.0.194112.1.4

Key Usage (critical)	Digital Signature (Bit 0), Key Encipherment (Bit 2)	
QCStatements	id-qcs-pkixQCSyntax-v2 ⁱ (oid=1.3.6.1.5.5.7.1.1.2)	id-etsi-qcs-SemanticsId- Legal (oid=0.4.0.194121.1.2)
	id-etsi-qcs- QcCompliance (oid=0.4.0.1862.1.1)	
	id-etsi-qcs- QcLimitValue ⁱⁱⁱ (0.4.0.1862.1.2)	[Сума в EUR]
	id-etsi-qcs- QcType (oid=0.4.0.1862.1.6)	id-etsi-qct- web (oid=0.4.0.1862.1.6.3)
	id-etsi-qcs- QcPDS (oid=0.4.0.1862.1.5)	PdsLocations PdsLocation=https://www.evrotrust.com/pds/pds_en.pdf language=en
	id-etsi- psd2 -qcStatement (oid=0.4.0.19495.2)	rolesOfPSP roleOfPspOid = 0.4.0.19495.1.1/2/3/4 roleOfPspName = PSP_AS/PSP_PI/PSP_AI/PSP_IC nCAName= Full name of the NCA nCAId= NCA abbreviated unique identifier

7.6.9 ПРОФИЛ НА КВАЛИФИЦИРАНО АТРИБУТИВНО УДОСТОВЕРЕНИЕ ЗА КВАЛИФИЦИРАН ЕЛЕКТРОНЕН ПОДПИС НА ФИЗИЧЕСКО ЛИЦЕ „EVROTRUST QUALIFIED NATURAL PERSON ATTRIBUTE CERTIFICATE FOR QES”

Квалифицираното атрибутивно удостоверение за квалифициран електронен подпис на

физическо лице се издава при същите условия, както квалифицираното удостоверение за квалифициран електронен подпис на физическо лице, но се различава по вида и обема на удостоверенията в него данни. Използва се за идентификация на лицето пред Доверяваща се страна.

КУКЕП издадено от Оперативен удостоверяващ орган "Evrotrust RSA Operational CA":

Version	V3	
Serial number	[сериен номер]	
Signature Algorithm	SHA256RSA	
Issuer	CN=	Evrotrust RSA Operational CA
	OU=	Qualified Operational CA
	O=	Evrotrust Technologies JSC
	organizationIdentifier	NTRBG-203397356
	C=	BG
Valid from	[начална дата и час по UTC на валидност на удостоверението]	
Valid to	[крайна дата и час по UTC на валидност на удостоверението]	
Subject	C= (countryName)	Държава: Двубуквен код на държавата според ISO 3166. Указва общият контекст, в който трябва да се разбират други атрибути на полето Subject.
	CN= (commonName)	Пълно име: Пълно име от физическото лице на латиница по документ за самоличност.
	G= (givenName)	Собствено име: Име на физическото лице на латиница според документ за самоличност
	S= (surname)	Фамилно име: Фамилия на физическото лице на латиница според документ за самоличност
	name*= (id-at-name)	Пълно име: Пълно име от физическото лице на кирилица по документ за

		самоличност.		
	SERIALNUMBER= (serialNumber)	Национален идентификатор на физическото лице според ETSI EN 319 412-1 т.5.1.3, например: PNOBG-8310257645 за ЕГН или друг		
	gender*= (id-pda-gender)	Пол на физическото лице: М или F (мъжки/женски)		
	dateOfBirth*= (id-pda-dateOfBirth)	Рождена дата с точност до дни в ZULU формат, например: 19831231120000Z		
	stateOrProvinceName*= =	Текущ адрес по местоживееене: Наименование на област, щат или		
	localityName*= (id-at-localityName)	Текущ адрес по местоживееене: Наименование на населено място		
	streetAddress*= (id-at-streetAddress)	Текущ адрес по местоживееене: булевард, улица, блок, номер, етаж и т.н.		
	telephoneNumber*= (id-at-	Мобилен телефонен номер		
	emailAddress*	Имейл адрес		
	Title*= (id-at-title)	Занимание/длъжност/професия		
	description*= (id-at-description)	Данни от машинно четимите части на документа за самоличност на физическото лице (Machine-readable passport)		

По-зи-	Дъ лж	Сим-воли	Значение
--------	-------	----------	----------

		ци	ин			
		я	а			
		1	1	alpha	I, A или C	
		2	1	alpha <	Тип: Попълва се по преценка на издаващата държава или орган. Най-често се използва IP за паспорт и ID за национална лична карта.	
		3-5	3	alpha <	Код на страната, издаваща документа за самоличност според (ISO 3166-1 alpha-3 code with modifications)	
		6-14	9	alpha num <	Номер на документ за самоличност	
		15	1	num <	Контролно число на цифрите 6-14	
		16	1	:	Разделител	

		17	6	num	Година, месец и ден (YYMMDD), до която важи документа за самоличност
		18	1	:	Разделител
		19	6	num	Година, месец и ден (YYMMDD), която е издаден документа за самоличност
		Например: IDBGR6410202234:201013:251013			
Public Key Type/Length	RSA (2048/ 3072/ 4096 Bits)				
Subject Key Identifier	[Изчислена стойност за издаденото удостоверение]				
Authority Key Identifier	Key ID=7F3E6459852BDD2329C201E7CBC369C087932B08				
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://ca.evrotrust.com/crl/EvrotrustRSAOperationalCA.crl				
Authority Information Access	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://ca.evrotrust.com/aia/EvrotrustRSAOperationalCA.crt				

	[2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ca.evrotrust.com/ocsp														
Enhanced Key Usage	Secure Email (1.3.6.1.5.5.7.3.4)														
Certificate Policies	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.47272.2.2.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.evrotrust.com/cps [2]Certificate Policy: Policy Identifier=0.4.0.194112.1.2														
Key Usage (critical)	Non-repudiation (Bit 1) ^{iv}														
QCStatements	<table><tr><td>id-qcs-pkixQCSyntax-v2 (oid=1.3.6.1.5.5.7.1.2)</td><td>id-etsi-qcs-semanticId-Natural (oid=0.4.0.194121.1.1)</td></tr><tr><td colspan="2">id-etsi-qcs-QcCompliance (oid=0.4.0.1862.1.1)</td></tr><tr><td>id-etsi-qcs-QcLimitValueⁱⁱⁱ (0.4.0.1862.1.2)</td><td>[Сума в EUR]</td></tr><tr><td colspan="2">id-etsi-qcs-QcSSCD (oid=0.4.0.1862.1.4)</td></tr><tr><td>id-etsi-qcs-QcType</td><td>id-etsi-qct-esign (oid=0.4.0.1862.1.6.1)</td></tr></table>					id-qcs-pkixQCSyntax-v2 (oid=1.3.6.1.5.5.7.1.2)	id-etsi-qcs-semanticId- Natural (oid=0.4.0.194121.1.1)	id-etsi-qcs- QcCompliance (oid=0.4.0.1862.1.1)		id-etsi-qcs- QcLimitValue ⁱⁱⁱ (0.4.0.1862.1.2)	[Сума в EUR]	id-etsi-qcs- QcSSCD (oid=0.4.0.1862.1.4)		id-etsi-qcs- QcType	id-etsi-qct- esign (oid=0.4.0.1862.1.6.1)
id-qcs-pkixQCSyntax-v2 (oid=1.3.6.1.5.5.7.1.2)	id-etsi-qcs-semanticId- Natural (oid=0.4.0.194121.1.1)														
id-etsi-qcs- QcCompliance (oid=0.4.0.1862.1.1)															
id-etsi-qcs- QcLimitValue ⁱⁱⁱ (0.4.0.1862.1.2)	[Сума в EUR]														
id-etsi-qcs- QcSSCD (oid=0.4.0.1862.1.4)															
id-etsi-qcs- QcType	id-etsi-qct- esign (oid=0.4.0.1862.1.6.1)														

	(oid=0.4.0.1862.1.6)	
	id-etsi-qcs- QcPDS (oid=0.4.0.1862.1.5)	PdsLocations PdsLocation=https://www.evrotrust.com/ pds/pds_en.pdf language=en

*Маркираните със звездичка полета може да не присъстват в удостоверението

КУКЕП издадено от Оперативен удостоверяващ орган "Evrotrust RSA QOperational CA 2024":

Version	V3	
Serial number	[сериен номер]	
Signature Algorithm	SHA256RSA	
Issuer	CN=	Evrotrust RSA QOperational CA 2024
	OU=	Qualified Operational CA
	O=	Evrotrust Technologies JSC
	organizationIdentifier	NTRBG-203397356
	C=	BG
Valid from	[начална дата и час по UTC на валидност на удостоверението]	
Validit to	[крайна дата и час по UTC на валидност на удостоверението]	
Subject	C= (countryName)	Държава: Двубуквен код на държавата според ISO 3166. Указва общият контекст, в който трябва да се разбират други атрибути на полето Subject.
	CN= (commonName)	Пълно име: Пълно име от физическото лице на латиница по документ за самоличност.
	G= (givenName)	Собствено име: Име на физическото лице на латиница според документ за самоличност

	S= (surname)	Фамилно име: Фамилия на физическото лице на латиница според документ за самоличност
	name*= (id-at-name)	Пълно име: Пълно име от физическото лице на кирилица по документ за самоличност.
	SERIALNUMBER= (serialNumber)	Национален идентификатор на физическото лице според ETSI EN 319 412-1 т.5.1.3, например: PNOBG-8310257645 за ЕГН или друг
	gender*= (id-pda-gender)	Пол на физическото лице: М или F (мъжки/женски)
	dateOfBirth*= (id-pda-dateOfBirth)	Рождена дата с точност до дни в ZULU формат, например: 19831231120000Z
	stateOrProvinceName*= =	Текущ адрес по местоживееене: Наименование на област, щат или
	localityName*= (id-at-localityName)	Текущ адрес по местоживееене: Наименование на населено място
	streetAddress*= (id-at-streetAddress)	Текущ адрес по местоживееене: булевард, улица, блок, номер, етаж и т.н.
	telephoneNumber*= (id-at-	Мобилен телефонен номер
	emailAddress*	Имейл адрес
	Title*= (id-at-title)	Занимание/длъжност/професия

	description*= (id-at-description)	Данни от машинно четимите части на документа за самоличност на физическото лице (Machine-readable passport)			
		По-зи-ци-я	Дъ-лж-ин-а	Сим-воли	Значение
		1	1	alpha	I, A или C
		2	1	alpha <	Тип: Попълва се по преценка на издаващата държава или орган. Най-често се използва IP за паспорт и ID за национална лична карта.
		3-5	3	alpha <	Код на страната, издаваща документа за самоличност според (ISO 3166-1 alpha code with modifications)
		6-14	9	alpha num <	Номер на документ за

					самоличност	
		15	1	num <	Контролно число на цифрите 6-14	
		16	1	:	Разделител	
		17	6	num	Година, месец и ден (YYMMDD), до която важи документа за самоличност	
		18	1	:	Разделител	
		19	6	num	Година, месец и ден (YYMMDD), на която е издаден документа за самоличност	
		Например: IDBGR6410202234:201013:251013				
Public Key Type/Length	RSA (2048/ 3072/ 4096 Bits)					
Subject Key Identifier	[Изчислена стойност за издаденото удостоверение]					
Authority Key Identifier	Key ID=892b1433df16a3593cdefde203c89400dab9faa8					
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://ca.evrotrust.com/crl/EvrotrustRSAQOperationalCA2024.crl					
Authority Information	[1]Authority Info Access					

Access	Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://ca.evrotrust.com/aia/EvrotrustRSAQOperationalCA2024.crt [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ca.evrotrust.com/ocsp									
Enhanced Key Usage	Secure Email (1.3.6.1.5.5.7.3.4)									
Certificate Policies	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.47272.2.2.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.evrotrust.com/cps [2]Certificate Policy: Policy Identifier=0.4.0.194112.1.2									
Key Usage (critical)	Non-repudiation (Bit 1) ^{iv}									
QCStatements	<table><tr><td>id-qcs-pkixQCSyntax-v2 (oid=1.3.6.1.5.5.7.1.2)</td><td>id-etsi-qcs-semanticId-Natural (oid=0.4.0.194121.1.1)</td></tr><tr><td colspan="2">id-etsi-qcs-QcCompliance (oid=0.4.0.1862.1.1)</td></tr><tr><td>id-etsi-qcs-QcLimitValueⁱⁱⁱ (0.4.0.1862.1.2)</td><td>[Сума в EUR]</td></tr><tr><td colspan="2">id-etsi-qcs-QcSSCD</td></tr></table>		id-qcs-pkixQCSyntax-v2 (oid=1.3.6.1.5.5.7.1.2)	id-etsi-qcs-semanticId- Natural (oid=0.4.0.194121.1.1)	id-etsi-qcs- QcCompliance (oid=0.4.0.1862.1.1)		id-etsi-qcs- QcLimitValue ⁱⁱⁱ (0.4.0.1862.1.2)	[Сума в EUR]	id-etsi-qcs- QcSSCD	
id-qcs-pkixQCSyntax-v2 (oid=1.3.6.1.5.5.7.1.2)	id-etsi-qcs-semanticId- Natural (oid=0.4.0.194121.1.1)									
id-etsi-qcs- QcCompliance (oid=0.4.0.1862.1.1)										
id-etsi-qcs- QcLimitValue ⁱⁱⁱ (0.4.0.1862.1.2)	[Сума в EUR]									
id-etsi-qcs- QcSSCD										

	(oid=0.4.0.1862.1.4)	
	id-etsi-qcs- QcType (oid=0.4.0.1862.1.6)	id-etsi-qct- esign (oid=0.4.0.1862.1.6.1)
	id-etsi-qcs- QcPDS (oid=0.4.0.1862.1.5)	PdsLocations PdsLocation=https://www.evrotrust.com/ pds/pds_en.pdf language=en

*Маркираните със звездичка полета може да не присъстват в удостоверението

7.6.10 ПРОФИЛ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ ЗА АВТЕНТИЧНОСТ НА УЕБСАЙТ ЗА ДОМЕЙН „EVROTRUST SSL DOMAIN VALIDATED CERTIFICATE“

Издадено от Оперативен удостоверяващ орган "Evrotrust RSA Operational CA":

Version	V3	
Serial number	[сериен номер]	
Signature Algorithm	SHA256RSA	
Issuer	CN=	Evrotrust RSA Operational CA
	OU=	Qualified Operational CA
	O=	Evrotrust Technologies JSC
	organizationIdentifier	NTRBG-203397356
	C=	BG
Valid from	[начална дата и час по UTC на валидност на удостоверението]	
Validit to	[крайна дата и час по UTC на валидност на удостоверението]	
Subject	C= (countryName)	Държава: Двубуквен код на държавата според ISO 3166. Указва общият контекст, в който трябва да се разбират други атрибути на полето Subject.

	CN= (commonName)	Домейн име, IP или Име на ресурс
Public Key Type/Length	RSA (2048/ 3072/ 4096 Bits)	
Subject Key Identifier	[Изчислена стойност за издаденото удостоверение]	
Authority Key Identifier	Key ID=7F3E6459852BDD2329C201E7CBC369C087932B08	
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://ca.evrotrust.com/crl/EvrotrustRSAOperationalCA.crl	
Authority Information Access	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://ca.evrotrust.com/aia/EvrotrustRSAOperationalCA.crt [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ca.evrotrust.com/ocsp	
Enhanced Key Usage	Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2)	
Subject Alternative Name	DNS Name=[Домейн име или IP]	
Certificate Policies	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.47272.2.4.1 [1,1]Policy Qualifier Info:	

	Policy Qualifier Id=CPS Qualifier: http://www.evrotrust.com/cps
Key Usage (critical)	Digital Signature (Bit 0), Key Encipherment (Bit 2)

Издадено от Оперативен удостоверяващ орган "Evrotrust RSA QOperational CA 2024":

Version	V3	
Serial number	[сериен номер]	
Signature Algorithm	SHA256RSA	
Issuer	CN=	Evrotrust RSA QOperational CA 2024
	OU=	Qualified Operational CA
	O=	Evrotrust Technologies JSC
	organizationIdentifier	NTRBG-203397356
	C=	BG
Valid from	[начална дата и час по UTC на валидност на удостоверението]	
Valid to	[крайна дата и час по UTC на валидност на удостоверението]	
Subject	C= (countryName)	Държава: Двубуквен код на държавата според ISO 3166. Указва общият контекст, в който трябва да се разбират други атрибути на полето Subject.
	CN= (commonName)	Домейн име, IP или Име на ресурс
Public Key Type/Length	RSA (2048/ 3072/ 4096 Bits)	
Subject Key Identifier	[Изчислена стойност за издаденото удостоверение]	
Authority Key Identifier	Key ID=892b1433df16a3593cdefde203c89400dab9faa8	
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name:	

	Full Name: URL= http://ca.evrotrust.com/crl/EvrotrustRSAQOperationalCA2024.crl
Authority Information Access	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://ca.evrotrust.com/aia/EvrotrustRSAQOperationalCA2024.crt [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL= http://ca.evrotrust.com/ocsp
Enhanced Key Usage	Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2)
Subject Alternative Name	DNS Name=[Домейн име или IP]
Certificate Policies	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.47272.2.4.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.evrotrust.com/cps
Key Usage (critical)	Digital Signature (Bit 0), Key Encipherment (Bit 2)

7.6.11 ПРОФИЛ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ ЗА КВАЛИФИЦИРАН ЕЛЕКТРОНЕН ПОДПИС НА ФИЗИЧЕСКО ЛИЦЕ „EVROTRUST REG.KE QUALIFIED NATURAL PERSON CERTIFICATE FOR QES”

КУКЕП издадено от Оперативен удостоверяващ орган "Evrotrust RSA REG.KE Operational CA 2025":

Version	V3	
Serial number	[сериен номер]	
Signature Algorithm	SHA256RSA	
Issuer	CN=	Evrotrust RSA REG.KE Operational CA 2025
	O=	Evrotrust Technologies JSC
	organizationIdentifier	NTRBG-203397356
	C=	BG
Valid from	[начална дата и час по UTC на валидност на удостоверението]	
Validit to	[крайна дата и час по UTC на валидност на удостоверението]	
Subject	C= (countryName)	Държава: Двубуквен код на държавата според ISO 3166. Указва общият контекст, в който трябва да се разбират други атрибути на полето Subject.
	CN= (commonName)	Обичайно име: Избрано от физическото лице име, с което то обичайно се представя. Когато не е избрано, се вписва пълното име на физическото лице.
	G= (givenName)	Собствено име: Име на физическото лице според документ за самоличност
	S= (surname)	Фамилно име: Фамилия на физическото лице според документ за самоличност
	или	
	2.5.4.65= (pseudonym)	Псевдоним: Псевдоним, избран от физическото лице

	SERIALNUMBER= (serialNumber)	Идентификатор на физическото лице (ETSI EN 319 412-1 т.5.1.3), например: - PNOBG-8310257645 за ЕГН; - PASSBG-12345678 за номер на паспорт; - IDCBG-195416023 за номер на лична карта; - TINBG-123434341 за ДДС номер. Ако лицето не желае да се вписва националният му идентификатор, се вписва клиентски номер, генерират от доставчика, с цел идентифициране на физическото лице при необходимост.
	O ⁱ = (organizationName)	Наименование на юридическо лице: Пълно наименованието по регистрацията или акт на вписване на юридическото лице, с което физическото лице е асоциирано.
	2.5.4.97 ⁱ = (organizationIdentifier)	Идентификатор на юридическо лице (ETSI EN 319 412-1 т.5.1.4), например: - VARBG-123456789 - ДДС; - NTRBG-123456789 - ЕИК (БУЛСТАТ). Вписва се националният идентификатор според местното законодателство на
	E ⁱⁱ = (e-mailAddress)	Имейл адрес на Титуляря
Public Key Type/Length	RSA (2048/ 3072/ 4096 Bits)	
Subject Key Identifier	[Изчислена стойност за издаденото удостоверение]	
Authority Key Identifier	Key ID=1e3c1d32408421b9f18da1eb5f4344175c33e6	
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name:	

	Full Name: URL= http://ca.evrotrust.com/crl/EvrotrustRSAREGKEOperationalCA2025.crl	
Authority Information Access	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://ca.evrotrust.com/aia/EvrotrustRSAREGKEOperationalCA2025.crt [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL= http://services.evrotrust.com/ocsp	
Subject Alternative Name	RFC822 Name=[Имейл адрес на Титуляря]	
Enhanced Key Usage	Secure Email (1.3.6.1.5.5.7.3.4)	
Certificate Policies	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.47272.2.24 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.evrotrust.com/cps [2]Certificate Policy: Policy Identifier=0.4.0.194112.1.2	
Key Usage (critical)	Non-repudiation (Bit 1) ^{iv}	
QCStatements	id-qcs-pkixQCSyntax-v2 ⁱ	id-etsi-qcs-semanticsId- Natural (oid=0.4.0.194121.1.1)

	(oid=1.3.6.1.5.5.7.11.2)	id-etsi-qcs-SemanticsId- Legal (oid=0.4.0.194121.1.2)
	id-etsi-qcs- QcCompliance (oid=0.4.0.1862.1.1)	
	id-etsi-qcs- QcLimitValue ⁱⁱⁱ (0.4.0.1862.1.2)	[Сума в EUR]
	id-etsi-qcs- QcSSCD (oid=0.4.0.1862.1.4)	
	id-etsi-qcs- QcType (oid=0.4.0.1862.1.6)	id-etsi-qct- esign (oid=0.4.0.1862.1.6.1)
	id-etsi-qcs- QcPDS (oid=0.4.0.1862.1.5)	PdsLocations PdsLocation=https://www.evrotrust.com/pds/pds_en.pdf language=en

7.6.12 ПРОФИЛ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ ЗА УСЪВЪРШЕНСТВАН ЕЛЕКТРОНЕН ПОДПИС НА ФИЗИЧЕСКО ЛИЦЕ „EVROTRUST REG.KE QUALIFIED NATURAL PERSON CERTIFICATE FOR AES”

КУУЕП издадено от Оперативен удостоверяващ орган "Evrotrust RSA REG.KE Operational CA 2025":

Version	V3	
Serial number	[сериен номер]	
Signature Algorithm	SHA256RSA	
Issuer	CN=	Evrotrust RSA REG.KE Operational CA 2025
	O=	Evrotrust Technologies JSC
	organizationIdentifier	NTRBG-203397356
	C=	BG

Valid from	[начална дата и час по UTC на валидност на удостоверението]	
Valid to	[крайна дата и час по UTC на валидност на удостоверението]	
Subject	C= (countryName)	Държава: Двубуквен код на държавата според ISO 3166. Указва общият контекст, в който трябва да се разбират други атрибути на полето Subject.
	CN= (commonName)	Обичайно име: Избрано от физическото лице име, с което то обичайно се представя. Когато не е избрано, се вписва пълното име на физическото лице.
	G= (givenName)	Собствено име: Име на физическото лице според документ за самоличност
	S= (surname)	Фамилно име: Фамилия на физическото лице според документ за самоличност
	Или	
	2.5.4.65= (pseudonym)	Псевдоним: Псевдоним, избран от физическото лице
	SERIALNUMBER= (serialNumber)	Идентификатор на физическото лице (ETSI EN 319 412-1 т.5.1.3), например: - PNOBG-8310257645 за ЕГН; - PASSBG-12345678 за номер на паспорт; - IDCBG-195416023 за номер на лична карта; - TINBG-123434341 за ДДС номер. Ако лицето не желае да се вписва националният му идентификатор, се вписва клиентски номер, генериран от доставчика, с цел идентифициране на физическото лице при необходимост.

	O ⁱ = (organizationName)	Наименование на юридическо лице: Пълно наименованието по регистрацията или акт на вписване на юридическото лице, с което физическото лице е асоциирано.
	2.5.4.97 ⁱ = (organizationIdentifier)	Идентификатор на юридическо лице (ETSI EN 319 412-1 т.5.1.4), например: - VARBG-123456789 - ДДС; - NTRBG-123456789 - ЕИК (БУЛСТАТ). Вписва се националният идентификатор според местното законодателство на юридическото лице, с което физическото
	E ⁱⁱ = (e-mailAddress)	Имейл адрес на Титуляря
Public Key Type/Length	RSA (2048/ 3072/ 4096 Bits)	
Subject Key Identifier	[Изчислена стойност за издаденото удостоверение]	
Authority Key Identifier	Key ID=1e3c1d32408421b9f18da1eb5f4344175c33e6	
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://ca.evrotrust.com/crl/EvrotrustRSAREGKEOperationalCA2025.crl	
Authority Information Access	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://ca.evrotrust.com/aia/EvrotrustRSAREGKEOperationalCA2025.crt [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)	

	Alternative Name: URL=http://services.evrotrust.com/ocsp	
Subject Alternative Name	RFC822 Name=[Имейл адрес на Титуляря]	
Enhanced Key Usage	Secure Email (1.3.6.1.5.5.7.3.4)	
Certificate Policies	[1]Certificate Policy: Policy Identifier=0.4.0.194112.1.0 [2]Certificate Policy: Policy Identifier=1.3.6.1.4.1.47272.2.25 [2,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.evrotrust.com/cps	
Key Usage (critical)	Non-repudiation (Bit 1) ^{iv}	
QCStatements	id-qcs-pkixQCSyntax-v2 ⁱ (oid=1.3.6.1.5.5.7.11.2)	id-etsi-qcs-semanticId- Natural (oid=0.4.0.194121.1.1) id-etsi-qcs-SemanticsId- Legal (oid=0.4.0.194121.1.2)
	id-etsi-qcs- QcCompliance (oid=0.4.0.1862.1.1)	
	id-etsi-qcs- QcLimitValue ⁱⁱⁱ (0.4.0.1862.1.2)	[Сума в EUR]
	id-etsi-qcs- QcType (oid=0.4.0.1862.1.6)	id-etsi-qct- esign (oid=0.4.0.1862.1.6.1)
	id-etsi-qcs- QcPDS (oid=0.4.0.1862.1.5)	PdsLocations

		PdsLocation=https://www.evrotrust.com/pds/pds_en.pdf language=en
--	--	---

7.6.13 ПРОФИЛ НА КВАЛИФИЦИРАНО АТРИБУТИВНО УДОСТОВЕРЕНИЕ ЗА КВАЛИФИЦИРАН ЕЛЕКТРОНЕН ПОДПИС НА ФИЗИЧЕСКО ЛИЦЕ „EVROTRUST REG.KE QUALIFIED NATURAL PERSON ATTRIBUTE CERTIFICATE FOR QES”

Квалифицираното атрибутивно удостоверение за квалифициран електронен подпис на физическо лице се издава при същите условия, както квалифицираното удостоверение за квалифициран електронен подпис на физическо лице, но се различава по вида и обема на удостоверенията в него данни. Използва се за идентификация на лицето пред Доверяваща се страна.

КУКЕП издадено от Оперативен удостоверяващ орган "Evrotrust RSA REG.KE Operational CA 2025":

Version	V3	
Serial number	[сериен номер]	
Signature Algorithm	SHA256RSA	
Issuer	CN=	Evrotrust RSA REG.KE Operational CA 2025
	O=	Evrotrust Technologies JSC
	organizationIdentifier	NTRBG-203397356
	C=	BG
Valid from	[начална дата и час по UTC на валидност на удостоверението]	
Valid to	[крайна дата и час по UTC на валидност на удостоверението]	
Subject	C= (countryName)	Държава: Двубуквен код на държавата според ISO 3166. Указва общият контекст, в който трябва да се разбират други атрибути на полето Subject.
	CN= (commonName)	Пълно име: Пълно име от физическото лице на латиница по документ за

		самоличност.
G= (givenName)		Собствено име: Име на физическото лице на латиница според документ за самоличност
S= (surname)		Фамилно име: Фамилия на физическото лице на латиница според документ за самоличност
name*= (id-at-name)		Пълно име: Пълно име от физическото лице на кирилица по документ за самоличност.
SERIALNUMBER= (serialNumber)		Национален идентификатор на физическото лице според ETSI EN 319 412-1 т.5.1.3, например: PNOBG-8310257645 за ЕГН или друг
gender*= (id-pda-gender)		Пол на физическото лице: М или F (мъжки/женски)
dateOfBirth*= (id-pda-dateOfBirth)		Рождена дата с точност до дни в ZULU формат, например: 19831231120000Z
stateOrProvinceName*= =		Текущ адрес по местоживееене: Наименование на област, щат или
localityName*= (id-at-localityName)		Текущ адрес по местоживееене: Наименование на населено място
streetAddress*= (id-at-streetAddress)		Текущ адрес по местоживееене: булевард, улица, блок, номер, етаж и т.н.
telephoneNumber*= (id-at-		Мобилен телефонен номер
emailAddress*		Имейл адрес

	Title*= (id-at-title)	Занимание/длъжност/професия			
	description*= (id-at-description)	Данни от машинно четимите части на документа за самоличност на физическото лице (Machine-readable passport)			
		По-зи-ци-я	Дъ-лж-ин-а	Сим-воли	Значение
		1	1	alpha	I, A или C
		2	1	alpha <	Тип: Попълва се по преценка на издаващата държава или орган. Най-често се използва IP за паспорт и ID за национална лична карта.
		3-5	3	alpha <	Код на страната, издаваща документа за самоличност според (ISO 3166-1 alpha code with modifications)

		6-14	9	alpha num <	Номер на документ за самоличност	
		15	1	num <	Контролно число на цифрите 6-14	
		16	1	:	Разделител	
		17	6	num	Година, месец и ден (YYMMDD), до която важи документа за самоличност	
		18	1	:	Разделител	
		19	6	num	Година, месец и ден (YYMMDD), на която е издаден документа за самоличност	
		Например: I<KEN8858034424:250503:200503				
Public Key Type/Length	RSA (2048/ 3072/ 4096 Bits)					
Subject Key Identifier	[Изчислена стойност за издаденото удостоверение]					
Authority Key Identifier	Key ID=1e3c1d32408421b9f18da1eb5f4344175c33e6					
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name:					

	URL= http://ca.evrotrust.com/crl/EvrotrustRSAREGKEOperationalCA2025.crl			
Authority Information Access	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://ca.evrotrust.com/aia/EvrotrustRSAREGKEOperationalCA2025.crt [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://services.evrotrust.com/ocsp			
Enhanced Key Usage	Secure Email (1.3.6.1.5.5.7.3.4)			
Certificate Policies	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.47272.2.26 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.evrotrust.com/cps [2]Certificate Policy: Policy Identifier=0.4.0.194112.1.2			
Key Usage (critical)	Non-repudiation (Bit 1) ^{iv}			
QCStatements	<table><tr><td>id-qcs-pkixQCSyntax-v2 (oid=1.3.6.1.5.5.7.1</td><td>id-etsi-qcs-semanticId-Natural (oid=0.4.0.194121.1.1)</td></tr></table>		id-qcs-pkixQCSyntax-v2 (oid=1.3.6.1.5.5.7.1	id-etsi-qcs-semanticId- Natural (oid=0.4.0.194121.1.1)
id-qcs-pkixQCSyntax-v2 (oid=1.3.6.1.5.5.7.1	id-etsi-qcs-semanticId- Natural (oid=0.4.0.194121.1.1)			

	1.2)	
	id-etsi-qcs- QcCompliance (oid=0.4.0.1862.1.1)	
	id-etsi-qcs- QcLimitValue ⁱⁱⁱ (0.4.0.1862.1.2)	[Сума в EUR]
	id-etsi-qcs- QcSSCD (oid=0.4.0.1862.1.4)	
	id-etsi-qcs- QcType (oid=0.4.0.1862.1.6)	id-etsi-qct- esign (oid=0.4.0.1862.1.6.1)
	id-etsi-qcs- QcPDS (oid=0.4.0.1862.1.5)	PdsLocations PdsLocation=https://www.evrotrust.com/ pds/pds_en.pdf language=en

*Маркираните със звездичка полета може да не присъстват в удостоверението

7.7 ПРОФИЛ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ НА ПОДПИСВАЩ МОДУЛ ЗА ВРЕМЕ „TIMESTAMP SIGNING UNIT“

Квалифицираният удостоверяващ орган за време (Timestamp Authority/TSA) подписва удостоверенията за време използвайки своите подписващи модули за време (Timestamp Signing units/TSU).

Профилът на удостоверението на подписващия модули за време на услугата "Evrotrust TSA" е:

Version	V3
Serial number	35A94E0EE6AC1CBD42442DC8D5CACE52F2A4E684
Signature Algorithm	SHA256RSA
Valid from	Feb 6 14:04:34 2024 GMT
Valid to	Feb 4 14:04:33 2029 GMT

Issuer	CN=	Evrotrust Services CA
	O=	Evrotrust Technologies JSC
	OrganizationIdentifier(2.5.4.97)	NTRBG-203397356
	C=	BG
Subject	CN=	Evrotrust Timestamp TSU 2024
	O=	Evrotrust Technologies JSC
	OrganizationIdentifier (2.5.4.97)=	NTRBG-203397356
	C=	BG
Public Key	RSA(2048 Bits)	
Subject Key Identifier	C4728DB862587E9B47187524BEB149029710CD35	
Key Usage (critical)	Digital Signature, Non Repudiation	
Extended keyUsage (critical)	Time Stamping (1.3.6.1.5.5.7.3.8)	
Certificate Policies	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.47272.1.2 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.evrotrust.com/cps	
Authority Key Identifier	KEYID=1B3A9E6D3191A15B461984FE9C98602C09D3332E	
Subject alternative name (not critical)	URL= http://ts.evrotrust.com/tsa	
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://services.evrotrust.com/EvrotrustServicesCA.crl	
Authority Information Access	[1]Authority Info Access Access Method=Certification Authority Issuer	

	(1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://services.evrotrust.com/EvrotrustServicesCA.crt [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://services.evrotrust.com/ocsp	
Basic Constraints (critical)	Subject Type=End Entity Path Length Constraint=None	
QCStatements	id-qcs-pkixQCSyntax-v2 ⁱ (oid=1.3.6.1.5.5.7.11.2)	id-etsi-qcs-SemanticsId- Legal (oid=0.4.0.194121.1.2)
	id-etsi-qcs- QcCompliance (oid=0.4.0.1862.1.1)	
	id-etsi-qcs- QcSSCD (oid=0.4.0.1862.1.4)	
	id-etsi-qcs- QcType (oid=0.4.0.1862.1.6)	id-etsi-qct- eseal (oid=0.4.0.1862.1.6.2)
	id-etsi-qcs- QcPDS (oid=0.4.0.1862.1.5)	PdsLocations PdsLocation=https://www.evrotrust.com/pds/pds_en.pdf language=en

Thumbprint SHA256:

42a1b2cfaade274964dcd9c482eb9150fe33de3ce41f79396e58a4f91196518f

Thumbprint SHA1: 36e076d55521c7daba3a37e604ccf72cf59baec6

7.8 ПРОФИЛ НА ОПЕРАТИВЕН УДОСТОВЕРЯВАЩ ОРГАН „EVROTRUST RSA

QOPERATIONAL CA 2024"

Version	V3	
Serial number	38 00 00 00 11 c0 d7 74 88 1b c3 ec 6a 00 00 00 00 00 11	
Signature Algorithm	SHA256RSA	
Issuer	CN=	Evrotrust RSA Root CA
	OU=	Evrotrust Qualified Root
	O=	Evrotrust Technologies JSC
	organizationIdentifier	NTRBG-203397356
	C=	BG
Valid from	16 август 2024 г. 08:35:28 UTC	
Validit to	16 август 2034 г. 08:45:28 UTC	
Subject	CN=	Evrotrust RSA QOperational CA 2024
	OU=	Qualified Operational CA
	O=	Evrotrust Technologies JSC
	organizationIdentifier (2.5.4.97)=(2.5.4.97)	NTRBG-203397356
	C=	BG
Public Key Type/Length	RSA (4096 Bits)	
Subject Key Identifier	89 2b 14 33 df 16 a3 59 3c de fd e2 03 c8 94 00 da b9 fa a8	
Certificate Policies	[1]Certificate Policy: Policy Identifier=All issuance policies [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.evrotrust.com/cps	
Subject Alternative Name	URL= http://www.evrotrust.com RFC822 Name=ca2024@evrotrust.com	
Authority Key Identifier	KeyID=74 5c a1 40 73 2e 1f e6 f9 3b bc ab a0 a4 a7 54 44 74 4f 70	

CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://ca.evrotrust.com/crl/EvrotrustRSARootCA.crl
Authority Information Access	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://ca.evrotrust.com/aia/EvrotrustRSARootCA.crt [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ca.evrotrust.com/ocsp
Key Usage (critical)	Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86)
Basic Constrains (critical)	Subject Type=CA Path Length Constraint=0

Thumbprint SHA256:

fcba8818597d593bf2d57b04cbd12de5d232ad4640602de44714b3128ffce663

Thumbprint SHA1: b43c938f40842590d076de04f3f73f2ef5d22fd7

7.9 ПРОФИЛ НА ОПЕРАТИВЕН УДОСТОВЕРЯВАЩ ОРГАН „EVROTRUST RSA REG.KE OPERATIONAL CA 2025”

Version	V3		
Serial number	3800000014054d408b12ae311b000000000014		
Signature Algorithm	SHA256RSA		
Issuer	CN=	Evrotrust RSA Root CA	
	OU=	Evrotrust Qualified Root	
	O=	Evrotrust Technologies JSC	
	organizationIdentifier	NTRBG-203397356	

	C=	BG
Valid from	21 март 2025 г. 08:57:08 UTC	
Valid to	21 март 2035 г. 09:07:08 UTC	
Subject	CN=	Evrotrust RSA REG.KE Operational CA 2025
	O=	Evrotrust Technologies JSC
	organizationIdentifier (2.5.4.97)=(2.5.4.97)	NTRBG-203397356
	C=	BG
Public Key Type/Length	RSA (4096 Bits)	
Subject Key Identifier	1e3c1d32408421b9f18da1eb5f4344175c33e6	
Certificate Policies	[1]Certificate Policy: Policy Identifier=All issuance policies [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.evrotrust.com/cps	
Subject Alternative Name	RFC822 Name=evrotrustregkeoperca2025@evrotrust.com URL= http://www.evrotrust.com	
Authority Key Identifier	KeyID=745ca140732e1fe6f93bbcaba0a4a75444744f70	
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://ca.evrotrust.com/crl/EvrotrustRSARootCA.crl	
Authority Information Access	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://ca.evrotrust.com/aia/EvrotrustRSARootCA.crt	

	[2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ca.evrotrust.com/ocsp
Key Usage (critical)	Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86)
Basic Constrains (critical)	Subject Type=CA Path Length Constraint=0

Thumbprint SHA256:

693ae86123967f9ae3f9ad2512ef41da40df152c262507a74fae6241e6605914

Thumbprint SHA1: 714857d2e781dff936b27c2401ec17d57327ee23

8 ОДИТ

Одитите, извършвани в Евротръст се отнасят до обработката на информационните данни и управление на ключовите процедури. Те имат за цел да контролират „Практиката при предоставяне на квалифицирани удостоверителните услуги“ доколко е съвместима с внедрената интегрираната система за управление, която включва изискванията на стандартите ISO/IEC 27001, ISO 9001, ISO 22301, и ISO/IEC 20000-1, Регламент (ЕС) № 910/2014 и вътрешните управленски решения и мерки. Извършваните одити на Евротръст се отнасят за всички Удостоверителни органи, принадлежащи към базовия Удостоверяващ орган, Регистриращия орган, както и други елементи на инфраструктурата на публичния ключ, например OCSP сървър.

Евротръст ежегодно извършва най-малко един вътрешен одит.

Евротръст е обект на одит най-малко веднъж на 24 месеца от Орган за оценяване на съответствието. Целта на одита е да се потвърди, че Евротръст като доставчик на квалифицирани удостоверителни услуги и предоставяните от него квалифицирани удостоверителни услуги отговарят на изискванията, посочени в Регламент ЕС) № 910/2014. Доставчикът представя на Органа по надзор съответния доклад за оценяване на съответствието в срок от три работни дни след като го получи.

Органът по надзор може по всяко време да извърши одит или да поиска от Орган за оценяване на съответствието да направи оценяване на съответствието на Евротръст.

8.1 ЧЕСТОТА НА ОДИТА

Ръководството на Евротръст назначава периодични проверки за съответствие на текущата дейност с утвърдените Практика и Политика при предоставяне на квалифицирани удостоверителни услуги относно дейността на Евротръст.

Ръководството на Евротръст осъществява постоянен оперативен контрол за точното изпълнение на инструкциите при работа от персонала на Евротръст.

8.2 КВАЛИФИКАЦИЯ НА ПРОВЕРЯВАЩИТЕ ЛИЦА

Външен одит се извършва от акредитиран и независим от Евротръст Орган за оценяване на съответствието. Системата за акредитация и компетентност на одитора са определени в Регламент (ЕО) № 765/2008 за определяне на изискванията за акредитация и надзор на пазара във връзка с пускане на пазара на продукти и за отмяна на Регламент (ЕИО) № 339/93 и се регулира от ISO/IEC 17065:2012: Оценката на съответствието - изисквания за органите, удостоверяващите продукти, процесите и услугите.

Външна проверка от надзорен орган се извършва по всяко време от оправомощени служители на Органа по надзор – Комисията за регулиране на съобщенията.

Вътрешният одит се извършва от служители на Евротръст с нужния опит и квалификация.

За целите на одитната дейност, Евротръст е наел и оправомощил служители, които притежават необходимите технически познания, свързани с инфраструктурата на публичния ключ, с надеждната и сигурна работа на технологичната система, информационна сигурност, както и с наличие на голям практически опит в одитирането.

8.3 ОТНОШЕНИЯ НА ПРОВЕРЯВАЩИТЕ ЛИЦА С ЕВРОТРЪСТ

Проверяващите лица трябва да бъдат независими, да не са пряко или косвено свързани с него и да нямат конфликт на интереси с Евротръст.

Отношенията между Евротръст и проверяващо външно лице се уреждат с договор.

8.4 ОБХВАТ НА ОДИТА

Проверката от страна на Органа по надзор обхваща нормативно регламентирания изисквания към дейността на Евротръст съгласно приложимото законодателство в сектора на квалифицирани удостоверителни услуги.

Одитът от страна на Органа за оценяване на съответствието обхваща цялостната дейност на Евротръст по предоставяне на квалифицирани удостоверителни услуги и изпълнение на всички стандарти и стандартизационни документи, свързани с Регламент (ЕС) № 910/2014: документация; архиви; информационни данни, свързани с издаване и управление на квалифицирани удостоверения; физическа и информационна сигурност и надеждност на технологичната система и управление; Удостоверителни органи.

Обхватът на вътрешните одити включва: проверка на дейността на доставчика и съответствието ѝ Политиката и Практиката при предоставяне на квалифицирани удостоверителни услуги; съпоставка на практики и процедури посочени в този документ с тяхната практическа реализация при изпълнение на дейността на Евротръст; проверка на дейността на Регистриращия орган; други обстоятелства, факти и дейности, свързани с инфраструктурата Евротръст, по преценка на ръководството на Евротръст.

8.5 ДЕЙСТВИЯ, ПРЕДПРИЕТИ В РЕЗУЛТАТ НА ИЗВЪРШЕНИЯ ОДИТ

Докладите от вътрешни и външни одити се предават на Евротръст.

Докладът от Органа за оценяване на съответствието се предава на Органа по надзор в рамките на 3 (три) дни след връчването му на ръководството на Евротръст.

Въз основа на направените оценки от доклада, Ръководство на Евротръст набелязва мерки и срокове за отстраняване на констатираните пропуски и несъответствия.

Персоналът на Евротръст предприема конкретни действия за тяхното отстраняване в посочените срокове.

8.6 СЪХРАНЕНИЕ НА РЕЗУЛТАТИТЕ ОТ ОДИТИТЕ

Резултатите от извършените вътрешни и външни одити се съхраняват надлежно в архива на Евротръст.

Сертификационният документ получен от Органа за оценяване на съответствието може да бъде публикуван на страницата на Евротръст в интернет.

9 ДРУГИ БИЗНЕС И ПРАВНИ ВЪПРОСИ

9.1 ЦЕНИ И ТАКСИ

Евротръст поддържа документ „Тарифа за предоставяни удостоверителни, информационни, криптографски и консултантски услуги“ на страницата си в интернет на адрес: <https://www.evrotrust.com>.

Доставчикът има право да променя едностранно Тарифата по всяко време от действието на Договора, като уведомява за това Титуляря/Създателя посредством публикуване на промените на интернет страницата си.

Промяната има действие спрямо Титуляря/Създателя от деня, следващ деня на публикацията.

В 5 (пет) дневен срок от датата на промяната и доколкото е налице увеличение на цените, Титулярят/Създателят има право да прекрати едностранно договора с отправяне на писмено известие до Евротръст, считано от датата на изтичане на срока на последното удостоверение. В този случай договорът се счита отменен от датата на промяната, като платените по договора възнаграждения за ползване на услуги не подлежат на възстановяване. При липса на известие за отмяна се счита, че Титулярят/Създателят е съгласен с промяната.

Промяната на възнагражденията не може да засегне вече заплатени възнаграждения.

9.1.1 ВЪЗНАГРАЖДЕНИЯ

Стойността на договора може включва едно или няколко от следните възнаграждения:

- възнаграждение за издаване и поддържане на квалифицирано удостоверение;
- възнаграждение за подновяване на квалифицирано удостоверение;
- възнаграждение за извършени по искане на Титуляря/Създателя консултации и технологична помощ;
- цена за закупено или предоставено под наем от Евротръст оборудване;
- възнаграждение за персонализиране на физически носител;
- за извършване на отдалечени подписвания;
- възнаграждение за извършване на отдалечена идентификация;
- възнаграждения, свързани със сигурно връчване на електронни съобщения;

- други възнаграждения за предоставяни квалифицирани удостоверителни услуги.

Дължимите възнаграждения и суми се заплащат на Евротръст в размери, съгласно Тарифата за предоставяните от Евротръст квалифицирани удостоверителни, информационни, криптографски и консултантски услуги и в срокове по начини, посочени в Договора и приложенията към него.

Доколкото има уговорено авансово или абонаментно възнаграждение за използване на услуга, същото не подлежи на възстановяване, ако Титулярят/Създателят не е консумирал предоставяната услуга през съответния срок, за който се отнася авансовото или абонаментното възнаграждение.

Цената не включва начислените от телекомуникационните компании суми във връзка с ползвани от Титуляря/Създателя услуги от тях за целите на предоставяните услуги от Евротръст. Те се дължат изцяло от Титуляря/Създателя на съответната телекомуникационна компания. Доставчикът не дължи и не носи отговорност за заплащането на тези суми.

Всички разходи и такси за превеждане на дължимите суми по сметката на Евротръст, са за сметка на Потребителя.

9.1.2 ВЪЗНАГРАЖДЕНИЯ ЗА УДОСТОВЕРИТЕЛНИ, КРИПТОГРАФСКИ, ИНФОРМАЦИОННИ И КОНСУЛТАНТСКИ УСЛУГИ

За услугите по предоставяне и използване на квалифицирани удостоверения и свързаните с тях услуги се заплаща дължима сума при заявяване на услугата. В останалите случаи плащането се извършва в 10-дневен срок от получаване на фактурата или съгласно сключения договор.

Услугите, свързани с осъществяване на технологична помощ и предоставяне на консултации за изграждане и поддържане на инфраструктура и решения за информационна сигурност, се тарифират на база „човекочас“ и се заплащат въз основа на двустранно подписан протокол за извършена работа. Цените на часовата ставка в приложената Тарифа са валидни в рамките на установеното работно време. При работа в извън установеното работно време, цените се увеличават със съответен процент, съгласно Тарифата.

За услуга „Издаване на квалифицирани електронни времеви печати“ при съгласувано ниво на обслужване се заплаща съгласно договорните условия.

Цената на закупено или предоставено под наем от Евротръст оборудване се уговаря и

се дължи съгласно условията на договора. Правоотношенията между Евротръст и Титуляря/Създателя се уреждат съгласно общите правила на договора за продажба, респ. договора за наем.

При забавяне на плащанията след договорения срок Потребителя дължи на Евротръст законовата лихва за периода до окончателното изплащане на дължимите суми.

Ползването на публикувани документи в Интернет страницата на Евротръст е безплатно. За запис и предоставяне на тези документи върху физически носител се заплаща себестойността на този носител и куриерските разноски.

9.1.3 ФАКТУРИРАНЕ

Доставчикът издава на Потребителя фактура за предоставяните услуги.

Не получаването на фактура не освобождава Потребителя от задължението да заплати дължимите възнаграждения в уговорените срокове.

Всички дължими по договора суми се заплащат от Потребителя в брой или по банков път. Плащането по банков път се счита извършено със заверяването на банковата сметка на Евротръст в пълния размер на дължимите суми.

Всички банкови комисионни, такси и разноски във връзка с банковите преводи са за сметка на Потребителя.

9.1.4 ВРЪЩАНЕ НА УДОСТОВЕРЕНИЕ И ВЪЗСТАНОВЯВАНЕ НА ПЛАЩАНЕ

Титуляр/Създател може да възрази относно неточност или непълнота в съдържанието на издадено удостоверение в 3-дневен срок след публикуването му в регистъра на удостоверенията.

Ако причина за невярното съдържание на удостоверението е в Регистриращ орган, Евротръст прекратява удостоверението и издава безплатно ново, с вярно или възстановява направеното плащане за отмененото удостоверение с невярно съдържание.

Ако причина за невярното съдържание на удостоверението е невярно представяне на данни от страна на Титуляря/Създателя, Евротръст прекратява удостоверението и не възстановява направеното плащане. Той може да издаде ново, с вярно съдържание, за сметка на Потребителя.

Потребителят може да откаже да приеме издадено квалифицирано удостоверение с вярно съдържание. В този случай Евротръст го прекратява незабавно, без да възстановява направеното плащане.

9.1.5 БЕЗПЛАТНИ УСЛУГИ

Доставчикът предоставя безплатно услуги по регистрация и информационни услуги, свързани с ползване на регистъра на удостоверенията и уеб сайта, както следва:

- проверка на публикувано в регистъра удостоверение на електронен подпис;
- проверка за валидност на издадено удостоверение;
- проверка на статус на удостоверение в реално време;
- удостоверение за време на представено съдържание/електронно изявление без ниво на обслужване;
- изтегляне на актуален Списък със спрени и прекратени удостоверения (CRL) и достъп до CRL архив;
- изтегляне на оперативните удостоверения на Евротръст;
- изтегляне на публични документи на Евротръст;
- други услуги.

9.2 ФИНАНСОВИ ОТГОВОРНОСТИ

Евротръст е отговорен за предоставяните удостоверителни услуги пред потребителите, които разчитат на удостоверяванията.

Евротръст отговаря, ако вредите са по негова вина или на страните, на които той е възложил работа.

Ако Евротръст потвърди и приеме, че са настъпили вреди, той се ангажира да плати щетите. Максималната граница на плащане не може надвишава размера на вредите.

9.2.1 ЗАСТРАХОВКА НА ДЕЙНОСТТА

Евротръст сключва задължителна застраховка на дейността си като Доставчик на квалифицирани удостоверителни услуги. Във връзка с риска от отговорност за нанесени щети в съответствие с член 13 на Регламент (ЕС) № 910/2014 г. Евротръст сключва подходяща

застраховка за отговорност в съответствие с националното право. Задължителната застраховка е с непрекъсваем срок и се подновява ежегодно. Предмет на застраховката е отговорността на Евротръст за осъществяваната от него дейност, съгласно изискванията на приложимото законодателство. Задължителната застраховка покрива отговорността на Евротръст към потребители и доверяващи се страни за причинени имуществени и неимуществени вреди до границите определени в приложимото законодателство. След настъпване на събитие, което може да позволи предявяване на иск покрит от застраховката, засегнатото лице трябва да уведоми писмено Евротръст и Застрахователя в срок от 7 дни след като събитието му стане известно. Застрахователното покритие за нанесени неимуществени и/или имуществени вреди на Титуляр/Създател не надхвърля размера установен от приложимото законодателство.

9.2.2 ЗАСТРАХОВАТЕЛНО ПОКРИТИЕ

Застрахователното покритие за нанесени неимуществени и/или имуществени вреди на Титуляр/Създател не надхвърля размера установен от националното законодателство.

Застраховката не покрива случаите по отказ на отговорност, в частност за вреди причинени от:

- неспазване на задълженията на Титуляр/Създател;
- компрометиране или загуба на частен ключ на Титуляр/Създател поради не полагане на дължимата грижа за опазване на ключа при използване;
- неспазване на изискванията за проверка на валидността на електронния подпис/печат и на квалифицираното удостоверение от Доверяваща се страна;
- форсмажорни и други обстоятелства, извън контрола на Евротръст.

9.3 КОНФИДЕНЦИАЛНОСТ НА БИЗНЕС ИНФОРМАЦИЯ

Евротръст гарантира, че събирането, обработването и съхраняването на информация по време на дейността си като доставчик на квалифицирани удостоверителни услуги е в съответствие с националното законодателство.

Евротръст гарантира, че Доверяващи се страни имат достъп само до информацията, която е достъпна в регистъра на удостоверенията и уеб сайта на доставчика.

9.3.1 ОБХВАТ НА КОНФИДЕНЦИАЛНАТА ИНФОРМАЦИЯ

Конфиденциална информация за Титуляр/Създател е тази информация, която не е включена в издадените удостоверения и в Списъка със спрени и прекратени удостоверения (CRL). Тя съставлява лични данни по смисъла на Закона за защита на личните данни (ЗЗЛД).

Конфиденциалната информация се събира от Евротръст само доколкото е необходима за нуждите на издаване и поддържане на удостоверенията.

Конфиденциалната информация не може да бъде предоставяна на трети лица, без изрично съгласие на Титуляря/Създателя с изключение на случаите, при които Доставчикът е задължен по силата на закон.

Доставчикът може да събира допълнителна информация, която също не се включва в удостоверенията, но се използва за целите на качествено поддържане на квалифицираните удостоверителни услуги.

Конфиденциалната информация се съхранява на място, достъпът до което е ограничен само за лица от персонала на Евротръст, овластени да оперират с данните и се разкрива само след изрично съгласие на Титуляря/Създателя с изключение на случаите, при които Доставчикът е задължен по силата на закон.

Записи в журналите и логовете от системите на Евротръст се разглеждат като конфиденциална информация и са защитени от неправомерен достъп и въздействие.

9.3.2 НЕКОНФИДЕНЦИАЛНА ИНФОРМАЦИЯ

Неконфиденциална е всяка информация, съдържаща се в регистъра на удостоверенията по отношение на издадените квалифицирани удостоверения, както и в публикувания актуален Списък със спрени и прекратени удостоверения (CRL) и в архивните копия на този списък.

Следната информация в уеб сайта на доставчика е достъпна за обществеността:

- Политика и Практика при предоставяне на квалифицирани удостоверителни услуги;
- бланка на Договор между Евротръст и потребителите;
- ценоразпис на предоставените от Евротръст услуги;
- ръководства за потребители;
- адреси за контакт с Регистриращия орган и Удостоверяващия орган;
- потребителски удостоверения (единствено след одобрение на потребителите);

- Списъкът със спрени и прекратени удостоверения (CRL);
- извадки от доклади (документ за сертифициране) от Органа по оценяване на съответствието или друга упълномощена институция.

Публикуваните доклади информират обществеността за:

- обхвата на одита;
- общата оценка за одита;
- степента на изпълнение на препоръките.

9.3.3 ЗАЩИТА НА КОНФИДЕНЦИАЛНАТА ИНФОРМАЦИЯ

Доставчикът и Титулярят/Създателят нямат право да разпространяват или да допускат разпространяване на информация, станала им известна при или по повод изпълнение на задълженията им по Договора, включително относно плащания, без предварително изрично писмено разрешение от другата страна.

9.4 НЕПРИКОСНОВЕНОСТ НА ЛИЧНИТЕ ДАННИ

В качеството си на администратор на лични данни, Евротръст строго съблюдава изискванията за поверителност и неразпространение на личните данни на Титуляри/Създатели, станали му известни при изпълнение на дейността си като доставчик на квалифицирани удостоверителни услуги.

Евротръст предприема подходящи технически и организационни мерки срещу неразрешена или незаконна обработка на лични данни и срещу случайна загуба или унищожаване на лични данни. Евротръст защитава поверителността и целостта на регистрационните данни, особено когато се обменят с потребителя/субекта или между разпределените системни компоненти на Евротръст. Като администратор на лични данни, Евротръст строго съблюдава изискванията за поверителност и неразпространение на личните данни на Титуляри/Създатели, станали му известни при изпълнение на дейността си като доставчик на квалифицирани удостоверителни услуги. Евротръст гарантира, че личните данни се събират, съхраняват и обработват в съответствие със Закона за защита на личните данни и РЕГЛАМЕНТ (ЕС) 2016/679 General Data Protection Regulation (GDPR). Евротръст събира количество информация пропорционално на нейното предназначение и употреба. Всеки потребител дава съгласие за обработването на личните му данни. Това съгласие се заявява с

подписването на Договор за удостоверителни услуги. Личните данни се използват само във връзка с предоставянето на удостоверителни услуги, което означава, че се обработват само тези данни, които са адекватни, подходящи и не са прекомерни за предоставяне на достъп онлайн до услугите. Личните данни са защитени в съответствие с правилата за поверителност, съдържащи се в политиката за сигурност на Евротръст.

9.4.1 ДЕКЛАРАЦИЯ ЗА ПОВЕРИТЕЛНОСТ

Личните данни, предоставени на Евротръст се съхраняват и обработват в съответствие със Закона за защита на личните данни и РЕГЛАМЕНТ (ЕС) 2016/679 General Data Protection Regulation (GDPR). Евротръст събира количество информация пропорционално на нейното предназначение и употреба. Всеки потребител дава съгласие за обработването на личните му данни. Това съгласие се заявява с подписването на Договор за удостоверителни услуги.

Личните данни се използват само във връзка с предоставянето на удостоверителни услуги.

Личните данни са защитени в съответствие с правилата за поверителност, съдържащи се в политиката за сигурност на Евротръст.

9.4.2 ИНФОРМАЦИЯ ТРЕТИРАНА КАТО ЛИЧНА

Всяка информация за потребителите, която не е публично достъпна, чрез съдържанието на издадените удостоверения, уеб сайта на доставчика или онлайн чрез Списъка със спрени и прекратени удостоверения (CRL) и OCSP се третира като лична.

9.4.3 ИНФОРМАЦИЯ, КОЯТО НЕ СЕ СЧИТА ЗА ЛИЧНА

Цялата информация, оповестена в удостоверенията, се счита, че не е лична, освен ако изрично не е предвидено друго в Закона за защита на личните данни и РЕГЛАМЕНТ (ЕС) 2016/679 General Data Protection Regulation (GDPR).

9.4.4 ОТГОВОРНОСТ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Евротръст и Регистриращия орган, които получават поверителна информация,

гарантират защитата на лични данни на потребителите. Евротръст не допуска компрометиране и разкриване на лични данни пред трети лица. Предоставяне на достъп до лична информация е единствено в съответствие с изискванията на Закона за защита на личните данни и Регламент (ЕС) 2016/679 General Data Protection Regulation (GDPR).

9.4.5 СЪГЛАСИЕ ЗА ИЗПОЛЗВАНЕ НА ЛИЧНИ ДАННИ

Освен, ако не е посочено друго в „Практиката при предоставяне на квалифицирани удостоверителни услуги“, приложимите правила за поверителност (освен в случаите на споразумение) изискват личните данни да не бъдат използвани без съгласието на Титуляря/Създателя, освен в случаите, предвидени в закон.

9.4.6 ДРУГИ ОБСТОЯТЕЛСТВА ЗА РАЗКРИВАНЕ НА ИНФОРМАЦИЯ

Практиката при предоставяне на квалифицирани удостоверителни услуги не посочва никакви други обстоятелства в това отношение.

9.5 ПРАВА ВЪРХУ ИНТЕЛЕКТУАЛНА СОБСТВЕНОСТ

Различни данни, включени в издаваните от Евротръст квалифицирани удостоверения или публикувани в регистъра на удостоверенията или на уеб сайта на Евротръст са обект на права върху интелектуалната собственост и други имуществени и неимуществени права.

Отношенията по повод на тези права между Евротръст и другите участници в инфраструктурата на Евротръст, като външни Регистриращи органи и др. се уреждат с договор.

Всички издадени квалифицирани удостоверения от Евротръст са обект на авторско право на Евротръст.

Всички права върху използвани от Евротръст бизнес марки (напр., EVROTRUST®), както и съдържащи се в удостоверенията търговски наименования използвани от Титулярите/Създателите, се запазват от титулярите им/създателите им и се използват само за нуждите на предоставяните удостоверителни услуги.

Двойката ключове, кореспондиращи на удостоверенията издадени от Евротръст, както и съответния секретен материал, са обект на права на Евротръст, независимо от собствеността на физическия носител на ключовете.

9.5.1 ПРАВО НА СОБСТВЕНОСТ НА ДАННИ В КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ

Евротръст запазва всички права на интелектуална собственост на включените данни в квалифицираните удостоверения.

9.5.2 ПРАВО НА СОБСТВЕНОСТ НА ИМЕНА И ТЪРГОВСКИ МАРКИ

Евротръст притежава регистрирана марка, състояща се от графичен знак и надпис, който представлява следното лого:



Логото е регистрирана търговска марка на Евротръст и не може да се използва от други страни без предварителното писмено одобрение на Евротръст.

Всички потребители запазват право на интелектуална собственост на търговска марка, марка за услуги, или търговско наименование, съдържащо се във всяко издадено квалифицирано удостоверение.

Право на интелектуална собственост е уникалното име (DN) в рамките на всяко удостоверение, издадено на Титуляр/Създател.

9.5.3 ПРАВО НА СОБСТВЕНОСТ НА ДВОЙКА КЛЮЧОВЕ

Двойката ключове на потребителите и свързаното с публичния ключ квалифицирано удостоверение издадено от Евротръст, както и съответния секретен материал е собственост на Евротръст, независимо от собствеността на физическата среда, в която ключовете се съхраняват и защитават.

Удостоверяващите органи са собственост на Евротръст.

9.6 ОБЩИ ПОЛОЖЕНИЯ

Тази част от Практика при предоставяне на квалифицирани удостоверителни услуги описва задълженията, гаранциите и отговорността на Евротръст, Регистриращия орган, потребителите и доверяващите се страни. Уредени са правата, задълженията и дължимата грижа на потребителите и доверяващи се страни. Задълженията и отговорността на

потребителите и Евротръст се уреждат чрез договорни спазвания. Отношенията с доверяващи се страни се уреждат по реда на общото деликтно право.

Договорите за предоставяне на удостоверителни услуги следва да бъдат сключвани в писмена или електронна форма, при спазване на разпоредбите на Регламент (ЕС) № 910/2014, РЕГЛАМЕНТ (ЕС) 2016/679 и приложимото законодателство в Република България.

9.6.1 ЗАДЪЛЖЕНИЯ, ОТГОВОРНОСТ И ГАРАНЦИИ НА ЕВРОТЪРЪСТ

Евротръст гарантира, че осъществява дейността си като:

- спазва точно условията в настоящия документ, изискванията на Регламент (ЕС) № 910/2014, РЕГЛАМЕНТ (ЕС) 2016/679 и националното законодателство при осъществяване на дейността си на Доставчик на квалифицирани удостоверителни услуги;
- предоставените услуги не нарушават авторските права и лицензирани права на трети страни;
- използва техническо оборудване и технологии, които осигуряват надеждност на системите и техническата и криптографска сигурност при осъществяване на процесите, в това число и сигурен и защитен механизъм/устройство за генериране на ключове и за създаване на електронен подпис/печат в своята инфраструктура;
- издава квалифицирани удостоверения за електронни подписи/печати след като провери с допустими от закона средства представената информация;
- сигурно съхранява и поддържа информация, свързана с издаваните удостоверения и оперативната работа на системите;
- спазва установените процедури за работа и правила за технически и физически контрол, в съответствие с условията в Практика и Политика при предоставяне на квалифицирани удостоверителни услуги;
- при искане издава съответните типове удостоверения, спазвайки условията и процедурите в този документ, съответните Политики и общоприети стандарти:
 - удостоверителни услуги - X.509, PKCS # 10, PKCS # 7, PKCS # 12;
 - удостоверяване на време - препоръка RFC 3161;
 - проверка статуса на удостоверение - препоръка RFC 2560;
- уведомява Потребителите за акредитацията си;
- създава възможност за незабавно спиране и прекратяване на действието на

квалифицирано удостоверение;

- прекратява и спира действието на удостоверения при условията и по реда на съответната Политика;
- уведомява незабавно заинтересованите лица след спиране на удостоверение;
- осигурява условия за точно определяне на времето на издаване, спиране, възобновяване и прекратяване на действието на удостоверенията;
- изпълнява процедури по идентификация и установяване на автентичност на Титуляря/Създателя;
- осигурява мерки срещу подправяне на удостоверенията и поверителността на данните, до които има достъп в процеса на създаването на подписа/печата;
- използва надеждни системи за съхраняване и управление на удостоверенията;
- само надлежно овластени служители имат достъп за внасяне на промени в данните, установяване на автентичността и валидността на удостоверенията;
- взема незабавни мерки при възникване на технически проблеми във връзка със сигурността;
- с изтичане на срока на валидност на квалифицираното удостоверение отменя валидността му;
- информира Титулярите/Създателите и доверяващите се страни за техните задължения и дължима грижа на поведение при използването и доверяването на предоставяните от Евротръст удостоверителни услуги, както и относно правилното и сигурно използване на издадените удостоверения и предоставени удостоверителни услуги, свързани с тях;
- използва и съхранява събраната лична и друга информация само за целите на своята дейност по предоставяне на удостоверителни услуги в съответствие с националното законодателство;
- не съхранява и не копира данни за създаване на потребителски частни ключове;
- поддържа разполагаеми средства, които осигуряват възможност за извършване на дейността му;
- сключва застраховка за времето на своята дейност;
- поддържа доверен персонал, притежаващ необходимите експертни знания, опит и квалификация за извършване на дейността;

- поддържа регистъра на удостоверенията, в който публикува издадените квалифицирани удостоверения;
- поддържа уеб сайт, в който публикува актуален Списък със спрени и прекратени удостоверения (CRL), други обстоятелства и електронни документи, съгласно този документ и националното законодателство;
- осигурява достъп без ограничения до регистъра на удостоверенията;
- осигурява защита срещу внасяне на промени в поддържания регистър на удостоверенията от нерегламентиран и неправилен достъп или поради случайно събитие;
- публикува незабавно издадените удостоверенията в регистъра на удостоверенията;
- създава условия на всяка доверяваща се страна да провери статуса на издадено и публикувано удостоверение в регистъра на удостоверенията;
- извършва периодични вътрешни одити на дейността на Удостоверяващия орган и Регистриращия орган;
- извършва външни одити от независими одитори и публикува на сайта си резултатите от проверката;
- използва в дейността си сертифициран софтуер и хардуер, както и сигурни и надеждни технологични системи;
- поддържа на сайта на Евротръст списък с Регистриращи органи, списък препоръчителен софтуер и хардуер за използване от потребителите, бланки, формуляри, типов Договор и др. документи в полза на потребителите;
- когато предоставя услуги, които не изискват защитено криптографско устройство, Евротръст прилага всички задължения, посочени за NCP в ETSI EN 319 411-1;
- когато предоставя услуги, които изискват защитено криптографско устройство, Евротръст прилага всички задължения, посочени за NCP + в ETSI EN 319 411-1;
- когато предоставя удостоверения в съответствие с политики QCP-n-qscd и QCP-l-qscd, Евротръст прилага всички задължения, посочени за NCP + в ETSI EN 319 411-1;
- когато издава удостоверение на юридическо лице в съответствие с политика QCP-w Евротръст прилага всички задължения, посочени за EVCP в ETSI EN 319 411-1;
- когато издава удостоверение на физическо лице в съответствие с политика QCP-w Евротръст прилага всички задължения, посочени за NCP в ETSI EN 319 411-1;

- Евротръст генерира и управлява частните ключове на потребителите по начин, по който тайната и целостта на ключовете не е компрометирана.
- В случаите, когато Евротръст има информация, че частният ключ на потребител е бил предоставен на неупълномощено лице или организация, която не е свързана с титуляря/създателя, Евротръст отменя всички удостоверения, които включват публичния ключ, съответстващ на съобщения компрометиран частен ключ.
- Евротръст не съхранява копия на частния ключ на титуляря/създателя.

Доставчикът носи отговорност пред Титуляр и Доверяваща се страна за причинени вреди от груба небрежност или умисъл:

- от неизпълнение на изискванията от Регламент (ЕС) № 910/2014 при осъществяване на дейността си по предоставяне на квалифицирани удостоверителни услуги;
- от неверни или липсващи данни в квалифицираното удостоверение към момента на издаването му;
- от вреди, които са причинени в случай, че по време на издаването на удостоверението лицето, посочено като Титуляр/Създател, не е разполагало с частния ключ, съответстващ на публичния ключ;
- от алгоритмичното несъответствие между частния ключ и публичния ключ, вписван в удостоверението.
- от неспазване на задълженията си по издаване и управление на квалифицирани удостоверения;
- от вписване на неверни или липсващи данни в удостоверенията;
- от пропуски в установяване на идентичността на Титуляря/Създателя.

Във връзка с изпълнение на изискванията на PSD2, при поискване от страна на NCA на информация, свързана с издадени удостоверения с вписан в тях номер на лиценза на платежната институция на Payment service provider (PSP), регистриран от същия NCA, отговорност на Евротръст е да осигури тази информация, която се предлага срещу заплащане. След извършване на заплащането, Евротръст подава информация към NCA за издадените удостоверения, като посочва техният брой, вид, сериен номер и период на валидност.

В случай че, преди края на валидността на издадено удостоверение статусът на устройството за сигурно създаване на подпис/печат (QSCD/смарт карта), върху което то е

записано, бъде променен по начин, засягащ валидността на удостоверението, Евротръст предприема действия в съответствие с изискванията на ETSI EN 319 411-2 по прекратяване на всички активни удостоверения, засегнати от промяната. Лицата, чиито удостоверения са засегнати, ще бъдат своевременно уведомени за прекратяването чрез имейл, изпратен на електронния адрес, вписан в удостоверението или посочен за контакт. В тези случаи разходите по преиздаване или подновяване на удостоверението и замяна на устройството с такова, чийто статус позволява използването му за сигурно създаване на квалифициран електронен подпис/печат, са за сметка на клиента.

9.6.2 ЗАДЪЛЖЕНИЯ, ОТГОВОРНОСТ И ГАРАНЦИИ НА РЕГИСТРАЦИЯ ОРГАН

Евротръст гарантира, че Регистрация орган изпълнява своите функции и задължения в пълно съответствие с условията в този документ, с изискванията и процедурите в Политиката и издадените вътрешни оперативни инструкции.

Евротръст отговаря за действията на Регистрация орган в инфраструктурата на Евротръст.

Евротръст гарантира, че Регистрация орган:

- изпълнява своята дейност, като използва надеждни и сигурни устройства и софтуер;
 - предоставя услуги, които са в съответствие със националното законодателство и не нарушава авторските права и лицензирани права на потребителите;
 - полага нужните усилия, за да извършва правилна идентификация на потребителите, въвежда правилно и точно данните в базата данни на Евротръст и актуализира тази информация в момента на потвърждаване на данните;
 - не прави умишлени грешки или не внася неточности в информацията, съдържаща се в удостоверенията;
 - неговите услуги са в съответствие с общоприетите стандарти: X.509, PKCS # 10, PKCS # 7, PKCS # 12;
 - неговите услуги се предоставят въз основа на процедури, които са съобразени с препоръките на „Практика при предоставяне на квалифицирани удостоверителни услуги“;
- Това се отнася до:

- процедури за проверка на самоличността на потребителите,
- процедури за проверка, за доказване на частен ключ, свързан с публичен ключ;

- процедури за приемане, обработка и потвърждение или отхвърляне на искания на потребители за издаване, подновяване, спиране и прекратяване на удостоверения;
- процедури за искане на потвърждение от Удостоверяващ орган, въз основа на вече прието искане от потребител за издаване, подновяване, спиране или прекратяване на удостоверение;
- процедури за създаване на архив на събраните приложения и данни, получени от потребителите;
- процедури за генериране на ключове за потребители;
- процедури за персонализация и издаване на електронни криптографски карти, на които се съхраняват удостоверенията и двойката ключове;
- участват във външни и вътрешни одити на Евротръст .

Регистриращият орган се ангажира да:

- представя на Евротръст препоръки, особено тези, които произтичат от одитите;
- да осигури защита на личните данни в съответствие със Закона за защита на личните данни, GDPR и относимото законодателство;
- да съхранява на сигурно място частните ключове на операторите в съответствие с изискванията за сигурност, определени в настоящия документ;
- да не използва личните операторски ключове за цели, различни от тези, посочени в настоящия документ.

9.6.3 ЗАДЪЛЖЕНИЯ НА ПОТРЕБИТЕЛИТЕ

Титулярят/Създателят или надлежно овластеното от Създателя физическо лице, посочен в издаденото квалифицирано удостоверение, има следните задължения:

- да се запознае и да спазва условията на Договора, Политиките и Практиките при предоставяне на квалифицирани удостоверителни услуги от Евротръст, както и изискванията в останалите документи, публикувани на уеб сайта на Евротръст;
- при подаване на искания за издаване и управление на удостоверения да предостави вярна, точна и пълна информация, която Евротръст изисква съгласно Договора, нормативните изисквания, приложимите Политики и Практики;
- да генерира криптографски ключове, използвайки сигурен метод и алгоритъм,

съобразно изискванията на Регламент (ЕС) № 910/2014 и да използва одобрени от Евротръст устройства за създаване на електронен подпис/печат;

➤ да провери пълнотата и верността на съдържанието на предоставената от него информация за удостоверяване в поле DN (Distinguished Name) на издаваните удостоверения. В случай на несъответствие между представената информация и удостовереното съдържание, потребителя трябва да уведоми незабавно Евротръст;

➤ да преустанови използването на удостоверението в случай на съмнение за загуба или хранява копия

➤ на частния ключ и да подаде до Евротръст заявка за неговото спиране;

➤ да преустанови използването на удостоверението при наличие на остаряла, променена, неточна и/или невярна информация, включена в издадено удостоверение и да подаде искане за спиране на действието на удостоверението;

➤ преди да използва новото удостоверение, да промени досегашния ПИН за достъп до устройството за създаване на електронен подпис/печат, където се съхранява частният ключ;

➤ да приложи необходимата дължима грижа и да предприеме необходимите мерки за предотвратяване на частния ключ от компрометиране, загуба, разкриване, модификация или друго неразрешено действие;

➤ да използва издаденото от Евротръст удостоверение само за законни цели и в съответствие с указаната в него политика и практика;

➤ да одобрява условията, посочени в Договора между него и Евротръст; Това одобрение трябва да се състои на саморъчен подпис върху Договора;

➤ да одобрява издаденото за него удостоверение;

➤ да не разкрива паролата за достъп до устройството за създаване на електронен подпис/печат на неупълномощени лица;

➤ да не прави достъпен своя частен ключ за други лица;

➤ цифровите подписи да се създават само от QSCD устройство;

➤ частният ключ на потребителя да се поддържа (или съответно да се използва) под единствено негов контрол;

➤ да използва двойката ключове само за електронни подписи или печати.

9.6.4 ДЪЛЖИМА ГРИЖА НА ДОВЕРЯВАЩА СЕ СТРАНА

Лицата, които се доверяват на квалифицирано удостоверение за електронен подпис/печат трябва да притежават основни познания относно принципите на използване и приложимост на електронния подпис/печат и на услугите, свързани с употреба на квалифицирано удостоверение за електронен подпис/печат.

Доверяващата се страна следва да положи дължима грижа, като:

- се доверява на удостоверенията само с оглед на Политиката относно предназначението и на ограниченията, при които е издадено;
- извърши проверка на статуса на удостоверението в поддържания от Евротръст регистър на удостоверенията. Проверката на електронната автентичност и на интегритета на удостоверението извън регистъра на удостоверенията или в неактуален Списък със спрени и прекратени удостоверения (CRL) не осигурява проверка за неговата валидност и всички настъпили вреди от предприети действия, след осъществяване единствено на такава проверка, са за сметка на Доверяващата се страна;
- проверява валидността на електронния подпис/печат на електронно подписани изявления, както и валидността на електронния подпис на Евротръст по веригата от удостоверения до базовото удостоверение;
- се увери, че приложенията, с които се използва удостоверението са функционално приложими за предназначението, за които е издадено, както и с оглед нивото на сигурност, посочени в съответната Политика;
- да провери дали подписът/печатът, придружен от удостоверението, не е използван за цели и за стойност на транзакции, извън вписаните в удостоверението ограничения и цели;
- да се увери, че дължината на използваните ключове отговаря на изискванията за сигурност на Доверяващата се страна;
- да се увери, че удостоверението е било валидно към момента на създаване на електронния подпис/печат.

Дължима грижа на Доверяващата се страна е да използва механизъм за сигурна проверка на електронен подпис/печат, който гарантира, че:

- публичният ключ, който се използва за проверка на подписа/печата съответства на този, който се представя пред него;

- проверката за използване на частния ключ е надеждно потвърдена и резултатите от тази проверка коректно се представят;
- при необходимост може да се установи съдържанието на подписания електронен документ;
- автентичността и валидността на удостоверение кѐм момента на подписването надеждно се проверяват;
- резултатите от проверката и електронната идентичност на Титуляря/Създателя правилно се представят;
- всякакви промени, релевантни за сигурността са установими.

Проверката за предназначението на удостоверението се извършва по следните данни, съдържащи се в профила на удостоверението:

- Политика, в съответствие на която се издава и управлява удостоверение за електронен подпис/печат, посочена в поле „Certificate Policies“;
- предназначението и ограниченията на действието на удостоверението, описани в поле „Key Usage“ и „ExtendedKey Usage“;
- данни за Титуляря/Създателя на удостоверението, посочени в поле „Subject“.

Евротръст не носи отговорност за настъпили вреди на Доверяващата се страна от неполагане на дължимата грижа. Всеки документ с дефектен или съмнителен електронен подпис/печат следва да бъде отхвърлен или евентуално подложен на други процедури, които позволяват да се посочи неговата валидност. Всяко лице, което одобри такъв документ, носи отговорност за каквито и да било последици.

9.6.5 ЗАДЪЛЖЕНИЯ НА ДРУГИ СТРАНИ

9.6.5.1 ЗАДЪЛЖЕНИЯ НА КВАЛИФИЦИРАНИЯ ОРГАН ЗА УДОСТОВЕРЯВАНЕ НА ВРЕМЕ

Квалифицираният орган за удостоверяване на време („Evrotrust TSA“) издава квалифицирани удостоверения за удостоверяване на време, в съответствие с изискванията, установени в Регламент (ЕС) № 910/2014, стандарти и стандартизационни документи, технически и организационни условия в Евротръст, осигуряващи сигурни и надеждни условия за създаване и проверка на електронни времеви печати, удостоверителни Политики за

квалифицирано удостоверение. Издаването се извършва с помощта на подписващ модул (Signing Unit) „Evrotrust Timestamp TSU 2024“.

Евротръст гарантира, че:

- използва технологии, оперативни процедури и процедури за управление на сигурността, чрез които се предотвратява всякаква възможност за манипулиране на времето;
- използва параметри на криптографски алгоритми в съответствие с Регламент (ЕС) № 910/2014;
- осигурява технически и организационни условия за прилагане на необходимите Политики за издаване на квалифицирано удостоверение за електронен времеви печат и технически условия за устройствата за създаване и проверка на електронни времеви печати;
- дефинира поне една хеш функция, която може да се използва за създаване на хеш данни маркирани с време;
- използва координирано универсално време – UTC с максимално допустимо забавяне между момента на получаване на искането и издаването на удостоверението за време от 1 (една) секунда.

Евротръст гарантира, че:

- предоставя непрекъснат достъп (24/7/365) на поддържащи услуги, с изключение на времето за техническа профилактика, като достъпността и точността са гарантирани, дори и ако няколко потребителя са едновременно свързани с приложението;
- основава своята търговска дейност на надеждни устройства и софтуер в съответствие с изисквания, определени в: CAW 14167-1 „Security Requirements for Trustworthy Systems, Managing Certificates for Electronic Signatures - Part 1: System Security Requirements“ and ETSI TS 102 023 „Policy requirements for time-stamping authorities“;
- провежда своята дейност и услуги в съответствие с приложимото законодателство;
- издава електронни времеви печати (Timestamp Tokens) в съответствие с ETSI EN 319 422 Time-stamping protocol and time-stamp profiles.

9.6.5.2 ЗАДЪЛЖЕНИЯ НА КВАЛИФИЦИРАНИТЕ ОРГАН ЗА ВАЛИДИРАНЕ

Квалифицираните органи за валидиране на Евротръст осъществяват функциите си в съответствие с изисквания, определени в Регламент (ЕС) № 910/2014. Изискванията

определят техническите и организационни условия в дейността на Евротръст, политиките за удостоверяване на квалифицирано удостоверение, техническите изисквания за устройствата за създаване и проверка на електронни подписи/печати, електронни удостоверения за време и електронни удостоверения за автентичност на уебсайтове.

Евротръст гарантира, че:

- използва оперативни процедури и такива за управление на сигурността, които изключват всякаква възможност за манипулиране на състоянието на удостоверенията или данните;
- проверява валидността на електронни подписи/печати, електронни удостоверения за време и електронни удостоверения за автентичност на уебсайтове, използвани в съответствие с изискванията на Регламент (ЕС) № 910/2014;
- Квалифицираните органи за валидиране на Евротръст проверяват състоянието на удостоверенията в съответствие с RFC 2560 Online Certificate Status Protocol (OCSP) recommendation.

9.6.5.3 ЗАДЪЛЖЕНИЯ НА КВАЛИФИЦИРАНИЯ ОПЕРАТИВЕН УДОСТОВЕРЯВАЩ ОРГАН ЗА КВАЛИФИЦИРАНИ ЕЛЕКТРОННИ ПОДПИСИ/ПЕЧАТИ

Задълженията на Квалифицираните оперативни удостоверяващи органи за квалифицирани електронни подписи/печати на Евротръст „Evrotrust RSA Operational CA“, „Evrotrust RSA QOperational CA 2024“, „Evrotrust RSA REG.KE Operational CA 2025“, „Evrotrust Services CA“ осъществяват функциите си в съответствие с изисквания, определени в Регламент (ЕС) № 910/2014 за определяне на технически и организационни условия в дейността на доставчиците. Изискванията са свързани с Политиките за издаване на квалифицирано удостоверение и техническите изисквания за устройствата за създаване и проверка на електронни подписи/печати.

Евротръст използва оперативни процедури и такива за управление на сигурността, които изключват всякаква възможност за манипулиране на състоянието на удостоверенията или данните.

9.6.5.4 ЗАДЪЛЖЕНИЯ НА ЕВРОТЪРЪСТ ПО ОТНОШЕНИЕ НА РЕГИСТЪРА НА УДОСТОВЕРЕНИЯТА И УЕБ САЙТА НА ДОСТАВЧИКА

Регистърът на удостоверенията и уеб сайта на доставчика се управляват и контролират от Евротръст, като той гарантира, че:

- публикува и архивира квалифицирани удостоверения на Квалифицирания базов удостоверяващ орган „Evrotrust RSA Root CA“, Квалифицирания валидиращ орган „Evrotrust RSA Validation“, Квалифицирания орган за удостоверяване на време „Evrotrust TSA“, Квалифицирани оперативни удостоверяващи органи „Evrotrust RSA Operational CA“, „Evrotrust RSA QOperational CA 2024“, „Evrotrust RSA REG.KE Operational CA 2025“, „Evrotrust Services CA“, Квалифицирания валидиращ орган „Evrotrust RSA QS Validation“, Квалифицирания валидиращ орган „Evrotrust Services Validation“, Квалифицирания валидиращ орган „Evrotrust RSA QOperational CA 2024 OCSP“ и други удостоверения на доставчика;
- публикува и архивира Политиките и Практиките при предоставяне на квалифицирани удостоверителни услуги, договори с клиентите, списъци с препоръчителни приложения и устройства, и списък на Регистриращи органи, както и други документи, свързани е дейността му;
- осигурява достъп до квалифицирани удостоверения, освен в случаите, когато Титуляря не е изразил съгласие и то само по отношение на неговото удостоверение;
- дава достъп до информацията относно статуса на удостоверенията, чрез публикуване на Списък със спрени и прекратени удостоверения (CRL) или чрез протокол за проверка статуса на удостоверенията в реално време (OCSP);
- осигурява постоянен достъп до информацията на уеб сайта на доставчика за Удостоверяващ орган, Регистриращ орган, клиенти и доверяващи се страни;
- публикува Списък със спрени и прекратени удостоверения (CRL) без забавяне и в съответствие със сроковете, определени в настоящия документ.

9.7 ОСВОБОЖДАВАНЕ ОТ ОТГОВОРНОСТ

Отговорността на Евротръст се основава на общите правила, посочени в настоящата Практика при предоставяне на квалифицирани удостоверителни услуги и е в съответствие с необходимите правни актове, които са в сила в Република България. Освобождаването от отговорност следва да се определи в договорите между потребителите и Евротръст.

Евротръст не носи отговорност в случаите, когато настъпилите вреди са следствие

от неполагане на дължима грижа, неизпълнение на задълженията или липса на познания в областта на PKI технологиите („инфраструктура с публичен ключ“/ Public Key Infrastructure) от страна на Титулярите или Доверяващите се страни.

Евротръст не носи отговорност и в случаи на вреди причинени от:

- използване на удостоверение извън пределите на вписаните в него предназначения и ограничения на неговото действие, по отношение на целите за използване и ограничения за стойността на транзакциите;
- незаконни действия от страна на Титуляри и Доверяващи се страни;
- предоставяне на начина на идентифициране на устройството за създаване на подпис/печат и достъп до частния ключ от страна на Титуляря/Създателя на трети лица;
- случайни събития, имащи характера на непреодолима сила, включително злоумишлени действия на трети лица (хакерски атаки, отнемане на устройството за създаване на подпис/печат, достъп до частния ключ, узнаване без знанието на титуляря на начина на идентифициране и др.)
- използване на удостоверение, което не е издадено или използвано в съответствие с изискванията и процедурите на Практиката и Политиката на Евротръст;
- използване на невалидно удостоверение (удостоверение, което е спряно или прекратено);
- не своевременно действие по прекратяване или спиране на удостоверение (следствие от забавено от страна на Титуляря/Създателя искане или поради причини извън контрола на Евротръст);
- компрометиран частен ключ, кореспондиращ на публичния ключ в удостоверението по вина на Титуляря/Създателя;
- лошо качество и функционалност на софтуерните продукти и хардуерни устройства използвани от Титуляря/Създателя и Доверяващи се страни.

Евротръст не отговаря за съдържанието на прикачените файлове. Всички рискове, които могат да възникнат при сваляне или изтегляне на прикачени файлове са отговорност на потребителите, които ги обменят.

9.8 ОГРАНИЧЕНИЯ НА ОТГОВОРНОСТТА

За издавани квалифицирани удостоверения за електронни подписи/печати, Доставчикът отговаря в рамките на вписаните в удостоверенията лимити на стойността на транзакциите.

9.9 ОТГОВОРНОСТ НА ТИТУЛЯРЯ/СЪЗДАТЕЛЯ

Титуляря/Създателя отговаря за пред Евротръст и всички доверяващи се лица, ако:

- при създаването на двойката частен-публичен ключ е използвал алгоритъм и устройства за създаване на електронен подпис/печат, които не отговарят на изискванията на Регламент (ЕС) № 910/2014;
- не изпълнява точно изискванията за сигурност, определени от Евротръст;
- не поиска от Евротръст спиране или прекратяване на действието на удостоверението след като е узнал, че частният ключ е бил използван неправомерно или съществува опасност от неправомерното му използване;
- е направил неверни изявления пред Евротръст, които имат и отношение към съдържанието или към издаването на квалифицираното удостоверение;
- когато удостоверението е издадено с вписан Създател и овластено от него лице, отговаря за неизпълнението от страна на овластения на задълженията му.

Клиентът, Титулярят/Създателят или упълномощеният представител на юридическо лице отговаря за съдържанието на прикачените файлове и последствията от тяхното използване.

9.9.1 ОТГОВОРНОСТ НА ТИТУЛЯРЯ/СЪЗДАТЕЛЯ КЪМ ЕВРОТРЪСТ

Титулярят/Създателят, отговаря спрямо Евротръст, ако той или овластеното от него лице, е предоставил неверни данни, съответно е премълчал данни, имащи отношение към съдържанието или към издаването на удостоверението, както и когато не е съхранявал правилно частния ключ, съответстващ на посочения в удостоверението публичен ключ.

9.10 СРОК И ПРЕКРАТЯВАНЕ НА „ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ“

9.10.1 СРОКОВЕ

Тази Практика влиза в сила от момента на нейното одобрение от Съвета на директорите на Евротръст и публикуването ѝ на уеб сайта на Евротръст. Допълнения към този документ влизат в сила след публикуването им на уеб сайта на Евротръст.

Разпоредбите в настоящия документ са валидни до издаване и публикуване на следваща версия на „Практика при предоставяне на квалифицирани удостоверителни услуги“ на уеб сайта на Евротръст.

9.10.2 ПРЕКРАТЯВАНЕ

С прекратяване на дейността на Евротръст, се прекратява актуалността на Практиката, както и на съдържащи се в този документ разпоредби.

Доставчикът съхранява надлежно и сигурно всички предишни версии/редакции на този документ.

9.10.3 ЕФЕКТ НА ПРЕКРАТЯВАНЕ И ОЦЕЛЯВАНЕ

При прекратяване на договора за удостоверителни услуги, Титулярите/Създателите и Доверяващите се страни остават обвързани от този документ, от гледна точка на издадените потребителски квалифицирани удостоверения, за остатък от периода на валидност на тези удостоверения.

9.11 БЕЛЕЖКИ И СЪОБЩЕНИЯ МЕЖДУ СТРАНИТЕ

Лицата, посочени в настоящата Практика могат да извършват изявления и да обменят информация с помощта на обикновена поща, електронна поща, факс, телефон, и мрежови протоколи (например TCP / IP, HTTP) и чрез мобилното приложение на Евротръст т.н.

Изборът на средствата може да бъде избран в зависимост от типа на информацията и начина на използване на услугите на Евротръст.

Информация за всеки пробив в сигурността на частните ключове на Удостоверяващите органи трябва да бъде публикувана на сайта на Евротръст, което ще я направи достъпна от всички заинтересовани страни.

9.12 ИЗМЕНЕНИЯ В „ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРИНИ

УДОСТОВЕРИТЕЛНИ УСЛУГИ

Измененията в Практиката може да бъдат резултат от наблюдавани грешки, актуализации и предложения от засегнатите страни. В случай на недействителна клауза от този документ, валидността на целия документ се запазва и не се нарушава договора с Титуляря/Създателя. Недействителната клауза се замества със законосъобразна норма.

Евротръст може да прави редакционни промени в този документ, които не засягат съдържанието на правата и задълженията в него.

Промени, които водят до нова версия/редакция на документа се публикуват на интернет страницата на Евротръст.

9.13 РЕШАВАНЕ НА СПОРОВЕ

Евротръст има процедура за подаване, разглеждане и решаване на предложения, жалби, сигнали и рекламации, получени от потребители, клиенти или доверяващи се страни относно предоставянето на услугите или други свързани с тях въпроси.

Предмет на спорове могат да бъдат единствено несъответствия или противоречия между лица, страни по договора с Евротръст. Спорове или жалби относно използване на удостоверения и удостоверителни услуги, предоставяни от Евротръст ще бъдат решавани, чрез посредничество, въз основа на писмено подадена информация. Всяка жалба трябва да съдържа описание на темата, причината или обстоятелствата, свързани с проблема, по който се отправя, както и пълното име, адрес, електронна поща и телефон за връзка с подателя. Към подадените жалби могат да се прилагат копия на документи, свързани с описаната тема.

При предявяване на рекламация потребителят посочва предмета на рекламацията, предпочитания от него начин за удовлетворяване на рекламацията, съответно размера на претендираната сума, и адрес за контакт. При подаване на рекламация потребителят задължително прилага и документите, на които се основава претенцията. При предявяване на рекламацията за услугата потребителят може да претендира за извършване на услугата в съответствие с договора, за отбив от цената или за възстановяване на заплатената сума.

Подаването на жалби, сигнали и рекламации се извършва по следните начини:

➤ Подават се лично, в писмен вид на хартия и собственоръчно подписани (по изключение се допуска устно подаване само и единствено на рекламации), в офис на адрес:

„Евротръст Технолъджис“ АД

гр. София, 1766

бул. „Околовръстен път“ № 251 Г, „ММ БИЗНЕС ЦЕНТЪР“, ет. 5

телефон, факс: + 359 2 448 58 58

електронен адрес: office@evrotrust.com

➤ На електронната поща на Евротръст (office@evrotrust.com или dpo@evrotrust.com), подписани с квалифициран електронен подпис.

Евротръст разглежда всяка постъпила жалба или рекламация и в 7-дневен срок изготвя писмен отговор с предложения за действия, които да се предприемат (ако е приложимо). Когато за решението на конкретна жалба или рекламация е необходимо събиране на допълнителна информация по случая, което изисква повече време, подателят се уведомява писмено, като се излагат съответните мотиви. Евротръст разглежда постъпила жалба или рекламация и изпраща окончателен отговор до подателя в срок до 1 (един) месец.

9.14 ПРИЛОЖИМО ПРАВО

За всички въпроси, неуредени в настоящия документ се прилагат разпоредбите на българското законодателство.

9.15 СЪОТВЕТСТВИЕ С ПРИЛОЖИМОТО ПРАВО

За да гарантира, че работи законно и надеждно, Евротръст прилага следните изисквания:

- Евротръст предоставя на потребителите и на всички заинтересовани страни политики, практики, сертификати и декларации за успешно извършвани проверки, като доказателства за това как отговаря на приложимите законови изисквания;
- Евротръст предоставя удостоверителни услуги и продукти за крайни потребители - хора с увреждания, когато това е възможно;
- Евротръст предоставя удостоверителни услуги, като взема предвид ETSI EN 301 549 свързан нуждата от достъпност на потребителите до ИКТ продукти и услуги;
- Евротръст гарантира, че е предприело подходящи технически и организационни мерки срещу неоторизиран достъп до информационната система, незаконно обработване на

лични данни или срещу случайна загуба, унищожаване или увреждане на лични данни. Евротръст обработва личните данни в съответствие с Регламент (ЕС) 2016/679. В това отношение, предоставянето на онлайн услуга и удостоверяване на онлайн данни се отнася единствено до обработката само на онези идентификационни данни, които са адекватни, подходящи и не прекомерно, за да се предостави достъп до тази услуга онлайн.

9.16 ДРУГИ РАЗПОРЕДБИ

Частите на Евротръст, свързани с генерирането и управлението на удостоверения са независими от други организации за решенията, свързани с установяването, осигуряването, поддържането и спирането на услуги в съответствие с приложимата политика.

В частност:

1. Висшето ръководство, старшият персонал и служителите с доверени роли на Евротръст, занимаващи се с генериране и управление на удостоверения е освободен от всякакъв търговски, финансов и друг натиск, който може да повлияе неблагоприятно на доверието в предоставяните услуги.

2. Частите на Евротръст, занимаващи се с генериране и управление на удостоверения, имат документирана структура, която защитава безпристрастността на операциите.

10 ИЗПОЛЗВАНИ ТЕРМИНИ И СЪКРАЩЕНИЯ

10.1 ПРИЛОЖЕНИЕ 1: ТЕРМИНИ И СЪКРАЩЕНИЯ НА БЪЛГАРСКИ ЕЗИК

Валидиране	Валидиране е процес на проверка и потвърждаване на валидността на електронен подпис или печат
Данни за валидиране	Данни за валидиране са данни, които се използват за валидиране на електронен подпис или електронен печат
Данни за идентификация на лица	Данни за идентификация на лица са набор от данни, които позволяват да се установи самоличността на физическо или юридическо лице, или на физическо лице, представляващо юридическо лице
Данни за създаване	Данни за създаване на електронен подпис са уникални данни, които се използват от Титуляря на електронния подпис за

електронен подпис	създаването на електронен подпис
Доверяваща се страна	Доверяваща се страна („Relying Parties“) са физически или юридически лица, които разчитат на електронна идентификация или удостоверителна услуга
Квалифициран доставчик на удостоверителни и услуги	Доставчик на удостоверителни услуги, който предоставя една или повече квалифицирани удостоверителни услуги и е получил квалифицирания си статут от Органа по надзор
ЕГН	Единен граждански номер
Електронен времеви печат	Електронен времеви печат са данни в електронна форма, които свързват други данни в електронна форма с конкретен момент във времето и представляват доказателство, че последните данни са съществували в съответния момент
Електронен документ	Електронен документ е всяко съдържание, съхранявано в електронна форма, по-специално текстов или звуков, визуален или аудио-визуален запис
Електронен печат	Електронен печат са данни в електронна форма, които се добавят към други данни в електронна форма или са логически свързани с тях, за да се гарантират произходът и целостта на последните. Електронният печат служи като доказателство, че даден електронен документ е издаден от юридическо лице и гарантира надеждния произход и целостта на документа. Освен при удостоверяването на автентичността на документ, издаден от юридическо лице, електронните печати могат да се използват за удостоверяване на автентичността на цифровите активи на юридическо лице, като софтуерен код или сървъри
Електронен	Данни в електронна форма, които се добавят към други данни

подпис	в електронна форма или са логически свързани с тях, и които титулярят на електронния подпис използва, за да се подписва
Електронна идентификация	Електронна идентификация е процес на използване на данни в електронна форма за идентификация на лица, които данни представляват по уникален начин дадено физическо или юридическо лице, или физическо лице, представляващо юридическо лице
Квалифициран електронен времеви печат	Квалифициран електронен времеви печат е електронен времеви печат, който отговаря на изискванията: а) обвързва датата и часа с данните по начин, който до голяма степен изключва възможността за незабелязана промяна на данните б) основава се на източник на точно време, свързан с координираното универсално време; и в) подписан е с усъвършенстван електронен подпис или с усъвършенстван електронен печат на доставчик на квалифицирани удостоверителни услуги или с друг равностоеен метод
Квалифициран електронен печат	Квалифициран електронен печат е усъвършенстван електронен печат, който е създаден от устройство за създаване на квалифициран електронен печат и се основава на квалифицирано удостоверение за електронен печат.
Квалифициран електронен подпис	Усъвършенстван електронен подпис, който е създаден от устройство за създаване на квалифициран електронен подпис и се основава на квалифицирано удостоверение за електронни подписи
Квалифицирано удостоверение за автентичност на уебсайт	Квалифицирано удостоверение за автентичност на уебсайт е удостоверение за автентичност на уебсайт, което се издава от доставчик на квалифицирани удостоверителни услуги

Квалифицирано удостоверение за електронен подпис	Квалифицирано удостоверение за електронен подпис е удостоверение за електронни подписи, което се издава от доставчик на квалифицирани удостоверителни услуги и отговаря на изискванията съгласно нормативната уредба
КРС	Комисия за регулиране на съобщенията
ПИН	Персонален идентификационен номер
Практика	Практика при предоставяне на удостоверителни услуги е документ, съдържащ правила относно издаване, спиране, възобновяване и прекратяване действието на удостоверенията, условията за предоставянето на достъп до удостоверенията
Политика	Политика за предоставяне на удостоверителни услуги е документ, описва политиката, която доставчикът следва при издаване на удостоверения, както и за всички предоставяни услуги
Регистриращ орган	Регистриращ орган („Registration Authority“, RA) е обособена структура на Доставчик, която осъществява някои от дейностите или всички по: приемане, проверка, одобряване или отхвърляне на искания и електронни заявки за издаване и управление на удостоверения, регистриране на подадените искания до Удостоверяващия орган за издаване и внасяне на промени в статута на удостоверения, осъществяване на съответни проверки за установяване на самоличността, съответно идентичността на Титулярите, както и на специфични данни за тях, с допустимите от закона средства и в съответствие с Политиката и Практиката при предоставяне на съответната удостоверителна услуга.
Служител по регистрацията	Оператор от РО, отговарящ за проверката на информацията, необходима за издаване на удостоверения и одобрение на исканията за удостоверяване

Служител по отмяна на удостоверенията	Лице, отговарящо за промените в статуса на оперативното удостоверение ISO/IEC 7498–2/ Препоръка ITU-T X.800
Регламент (ЕС) № 910/2014	Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета от 23 юли 2014 година относно Електронната идентификация и Удостоверителните услуги при електронни трансакции на вътрешния пазар и за отмяна на директива 1999/93/ЕО
Средство за електронна идентификация	Средство за електронна идентификация е материална и/или нематериална единица, която съдържа данни за идентификация на лица, която се използва за удостоверяване на автентичност за онлайн услуга
Създател на печат	Създател на печат е юридическо лице, което създава електронен печат
Титуляр	Титулярят („Signature Owner“) е физическо лице, което създава електронен подпис
Удостоверяване на автентичност	Удостоверяване на автентичност е електронен процес, който позволява електронната идентификация на физическо или юридическо лице или потвърждаването на произхода и целостта на данни в електронна форма
Удостоверение за време	Данни в електронна форма, които свързват други електронни данни към определен момент от време, предоставяйки доказателство, че тези данни съществуват към дадения момент
Удостоверение за електронен печат	Издава се на юридически лица и служи за валидиране на интегритет и оригинал на данните/документите.
Удостоверение за електронен	Удостоверение за електронен подпис е електронен атестат, който свързва данните за валидиране на електронен подпис

подпис	с физическо лице и потвърждава най-малко името или псевдонима на това лице
Удостоверителна услуга	Удостоверителни услуги са електронни услуги, предоставяни обикновено срещу възнаграждение от Доставчика удостоверителни услуги, които се състоят в: 1. създаването, проверката и валидирането на електронни подписи, електронни печати или електронни времеви печати, услуги за електронна препоръчана поща, както и удостоверения, свързани с тези услуги; или 2. създаването, проверката и валидирането на удостоверения за автентичност на уебсайт; или съхраняването на електронни подписи, печати или удостоверения, свързани с тези услуги
Удостоверителна услуга по удостоверяване на автентичност на уебсайт	Услугата по удостоверяване на автентичността на уебсайт осигурява средство, с което посетител на уебсайт може да бъде уверен, че зад уебсайта стои реален и легитимен субект
Удостоверяващ орган	Удостоверяващ орган („Certification Authority“, CA) е обособена структура на Доставчик, която осъществява дейностите по предоставяне на удостоверителни услуги. Удостоверяващият орган няма самостоятелна правосубектност и всички осъществени действия и актове на служителите му се извършват в качеството им на служители на Евротръст, в рамките на предоставените им правомощия
Устройство за създаване на електронен печат	Устройство за създаване на електронен печат е конфигуриран софтуер или хардуер, който се използва за създаването на електронен печат
Устройство за	Устройство за създаване на квалифициран електронен печат

създаване на квалифициран електронен печат	устройство за създаване на електронен печат, което отговаря на изискванията в Регламент (ЕС) № 910/2014
Устройство за създаване на квалифициран електронен подпис	Устройство за създаване на квалифициран електронен подпис е устройство за създаване на електронен подпис, което отговаря на изискванията на Регламент (ЕС) № 910/2014
Устройство за създаване на електронен подпис	Устройство за създаване на електронен подпис е конфигуриран софтуер или хардуер, който се използва за създаването на електронен подпис
Усъвършенстван електронен печат	Усъвършенстван електронен печат е електронен печат, който отговаря на изискванията: а) свързан е по уникален начин със създателя на печата б) може да идентифицира създателя на печата в) създаден е чрез данни за създаване на електронен печат, които създателят на електронния печат може да използва с висока степен на доверие и единствено под свой контрол; и г) свързан е с данните, за които се отнася, по начин, позволяващ да бъде открита всяка последваща промяна в тях
Усъвършенстван електронен подпис	Усъвършенстван електронен подпис е електронен подпис, който отговаря на изискванията: 1. -е свързан по уникален начин с Титуляря; 2. може да идентифицира Титуляря на подписа; 3. -е създаден чрез данни за създаване на електронен подпис, които титулярят на електронния подпис може да използва с висока степен на доверие и единствено под свой контрол, и

	4. -е свързан с данните, които са подписани с него, по начин, позволяващ да бъде открита всяка последваща промяна в тях
Юридически лица	Юридически лица, по смисъла на Договора за функционирането на Европейския съюз (ДФЕС), означава всички образувания, учредени или регламентирани съгласно правото на държава членка, независимо от тяхната правна форма
Краткосрочно удостоверение	Удостоверение, чийто срок на валидност е по-кратък от максималното време за обработка на искане за отмяна, както е посочено в практиката. Срок на валидност е определен от IETF RFC 5280.
Кръстосано удостоверение	Удостоверение, което се използва за установяване на отношения на доверие между два удостоверителни органа.

10.2 ПРИЛОЖЕНИЕ 2: ТЕРМИНИ И СЪКРАЩЕНИЯ НА АНГЛИЙСКИ ЕЗИК

ASN.1 Abstract Syntax Notation One	Абстрактен език за описание на обекти в удостоверенията
BG Bulgaria	България
C Country	Страна
CA Certification Authority	Удостоверяващ орган
CC Common Criteria	Общи критерии
CN Common Name	Общоприето име на лицето
CP Certificate Policy	Политика за предоставяне на удостоверителни услуги
CSP Cryptograph Services Provider	Криптографски модул към четящо устройство и смарт карта
CPS Certification Practice	Практика при предоставяне на удостоверителни

Statement	услуги
CRL, Certificate Revocation List	Списък със спрени и прекратени удостоверения
DSA, Digital Signature Algorithm	Вид криптографски алгоритъм за създаване на електронен подпис
DN, Distinguished Name	Отличително име на субект, вписан в удостоверението
E-mail	Електронна поща
Extended key usage	Разширени цели за използването на ключа
FIPS, Federal Information Processing Standard	Федерален стандарт за обработка на информация
HSM, Hardware Security Module	Хардуерен криптографски модул
ISO, International Standardization Organization	Международна организация за стандартизация
Issuer	Издател
IP, Internet Protocol	Интернет протокол
L, Location	Местонахождение
N, Number	Номер
NCA, National Competent Authority	Компетентен национален орган
O, Organization	Пълното наименование на юридическото лице по регистрацията или акт на вписване
OU, Organization Unit	Организационна единица, към която субект, вписан в удостоверението е свързан
OID, Object Identifier	Идентификатор на обект
OCSP, Online Certificate Status Protocol	Протокол за онлайн проверка на статуса на удостоверение
PKCS, Public Key Cryptography Standards	Криптографски стандарт за пренос на публичен ключ

PKI, Public Key Infrastructure	Инфраструктура на публичния ключ (съвкупност от хардуера, софтуера, персонала и документацията)
PSD2, Payment Services Directive 2	Ревизираната Директива за платежните услуги: „ДИРЕКТИВА (ЕС) 2015/2366 НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА от 25 ноември 2015 година за платежните услуги във вътрешния пазар, за изменение на директиви 2002/65/ЕО, 2009/110/ЕО и 2013/36/ЕС и Регламент (ЕС) № 1093/2010 и за отмяна на Директива 2007/64/ЕО“.
PSP, Payment Service Provider	Доставчик на платежна услуга
PSE, Personal Security Environment	Надеждна среда за генериране на двойка ключове при Титуляря
RA, Registration Authority	Регистриращ орган
RSA, Rivest-Shamir-Adelman	Вид асиметричен криптографски алгоритъм за създаване на електронен подпис
SSCD, Secure Signature Creation Device	Устройство за създаване на подпис/печат със защитен профил
SHA, Secure Hash Algorithm	Сигурен хеш алгоритъм за извличане на хеш идентификатор
SSL, Secure Socket Layer	Сигурен канал за предаване на данни
S Street	Улица
T Title	Титуляр („Signature Owner“) е физическо лице, което създава електронен подпис
Token	Токен, хардуерно устройство, съдържащо криптографска карта и четец
URL, Uniform Resource Locator	Единен ресурсен локатор/интернет връзка

Настоящият документ е публикуван на уебсайта на Евротръст в интернет на български и английски език. В случай на несъответствие между текстовете на български и английски език, приоритет има българския текст.

ⁱ Ако няма вписани атрибути за **organizationName** и **organizationIdentifier**, атрибута **id-etsi-qcs-SemanticsId-Legal** не се вписва.

ⁱⁱ Този атрибут **e-mailAddress** е остарял, но е разрешено неговото използване само за целите на съвместимост с по-стари системи. Ако липсва имейл адрес в издаденото удостоверение, то и полето **Subject Alternative Name** също няма да бъде използван

ⁱⁱⁱ Ако атрибута **id-etsi-qcs-QcLimitValue** присъства, в него се вписва максималния размер на ограничението на стойността на сделката, до която може да се използва удостоверението.

^{iv} Според изискванията на ETSI TS 119 412-2, разширението „Key Usage” трябва да бъде само от тип „A”, т.е. трябва да съдържа само стойността „Non-repudiation”. Поради контекста на приложимост на удостоверенията в Република България и други европейски страни, Евротръст допуска в разширението „Key Usage” използването и на тип „F” (стойности: „Non-repudiation”, „Digital Signature”, „Key Encipherment”) в случаите, когато удостоверенията се използват в ролята им на средство за установяване на криптирана TLS връзка и криптиране на данни.