

 Regulation 910 / 2014 eIDAS	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017



ПРАКТИКА

ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ

Версия: 2.2

evrotrust	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

	Длъжност	Име, фамилия	Дата	Подпис
Утвърдил	Изпълнителен директор	Константин Безуханов	23.06.2017 г.	
Съгласувал	Представител на ръководството по СУСИ	Стефан Хаджистойчев	23.06.2017 г.	
Разработил	Консултант по СУСИ	Мария Владимирова	23.06.2017 г.	

Дата на регистрация на документа: 23.06.2017 г.

Оригиналът се съхранява: при Представител на ръководството по СУСИ

Вид на екземпляра и пореден №

Оригинал	<input checked="" type="checkbox"/>	Контролирано копие	<input type="checkbox"/>	Информационен	<input type="checkbox"/>
----------	-------------------------------------	--------------------	--------------------------	---------------	--------------------------

Разпространение на документа: Абонат:

Вътрешно:

Външно:

Този документ е част от Система за управление на сигурността на информацията на “ЕВРОТРЪСТ ТЕХНОЛЪДЖИС” АД. Всички потребители на този документ трябва да изпълняват изискванията на СУСИ за работа с чувствителна информация.

This document is part of the Information Security Management System of EVROTRUST TECHNOLOGIES INC. Everyone who uses this document shall carry out the ISMS requirements for work with sensitive information.

Не се разрешава неконтролирано копиране и размножаване! Всички права са запазени!
© Copyright. All Rights reserved!

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

СЪДЪРЖАНИЕ

1	ВЪВЕДЕНИЕ	8
1.1	ПРЕГЛЕД	8
1.2	ИМЕ И ИДЕНТИФИКАЦИЯ НА ДОКУМЕНТА.....	10
1.3	УЧАСТНИЦИ В ИНФРАСТРУКТУРАТА НА ЕВРОТРЪСТ	12
1.3.1	УДОСТОВЕРЯВАЩИ ОРГАНИ.....	12
1.3.2	РЕГИСТРИРАЩ ОРГАН	14
1.3.3	ПОТРЕБИТЕЛИ.....	15
1.3.4	ДОВЕРЯВАЩИ СЕ СТРАНИ.....	16
1.3.5	ДРУГИ УЧАСТНИЦИ	16
1.4	УПОТРЕБА НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ	19
1.4.1	ВИДОВЕ КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ И ПРЕПОРЪЧИТЕЛЕН ДИАПАЗОН НА ПРИЛОЖИМОСТ	20
1.4.2	УПОТРЕБА	20
1.5	УПРАВЛЕНИЕ НА ПРАКТИКАТА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНА УДОСТОВЕРИТЕЛНА УСЛУГА.....	21
2	ОТГОВОРНОСТ ЗА ПУБЛИКУВАНЕ И ХРАНИЛИЩЕ	21
2.1	ХРАНИЛИЩЕ.....	21
2.2	ИНФОРМАЦИЯ, ПУБЛИКУВАНА ОТ ЕВРОТРЪСТ	22
2.3	ЧЕСТОТА НА ПУБЛИКУВАНЕ	23
2.4	ДОСТЪП ДО ПУБЛИКАЦИИ	24
3	ИДЕНТИФИКАЦИЯ И УДОСТОВЕРЯВАНЕ НА САМОЛИЧНОСТ	24
3.1	ИМЕНА.....	25
3.1.1	ВИДОВЕ ИМЕНА	26
3.1.2	НЕОБХОДИМОСТ ОТ ОТГРАНИЧИМИ ИМЕНА.....	26
3.1.3	АНОНИМНОСТ НА ПОТРЕБИТЕЛИТЕ.....	27
3.1.4	ПРАВИЛА ЗА ТЪЛКУВАНЕ НА РАЗЛИЧНИ ФОРМИ НА ИМЕНА.....	27
3.1.5	УНИКАЛНОСТ НА ИМЕНАТА	27
3.1.6	ПОВЕРКА НА ИМЕНА И СПОРОВЕ ПО ПОВОД НА ТЯХ.....	28
3.2	ПЪРВОНАЧАЛНА РЕГИСТРАЦИЯ.....	28
3.2.1	ПРОВЕРКА ЗА ПРИТЕЖАНИЕ НА ЧАСТЕН КЛЮЧ	29
3.2.2	УСТАНОВЯВАНЕ НА ИДЕНТИЧНОСТ НА ЮРИДИЧЕСКО ЛИЦЕ	30
3.2.3	УСТАНОВЯВАНЕ НА САМОЛИЧНОСТ НА ФИЗИЧЕСКО ЛИЦЕ.....	30
3.2.4	ОСОБЕНИ АТРИБУТИ	31
3.2.5	НЕПОТВЪРДЕНА ИНФОРМАЦИЯ.....	31
3.2.6	ДЕЙСТВИЯ НА УДОСТОВЕРЯВАЩИЯ ОРГАН.....	32
3.2.7	ПРОВЕРКА НА ПРИТЕЖАНИЕ НА ДОМЕЙН	32
3.2.8	КРИТЕРИИ ЗА СЪОТВЕТСТВИЕ	32
3.3	ИДЕНТИФИКАЦИЯ И ПРОВЕРКА ЗА САМОЛИЧНОСТ ПРИ ПОДНОВЯВАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ.....	32
3.4	ИДЕНТИФИКАЦИЯ И ПРОВЕРКА НА САМОЛИЧНОСТ ПРИ СПИРАНЕ НА ДЕЙСТВИЕТО НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ.....	34
3.5	ИДЕНТИФИКАЦИЯ И ПРОВЕРКА НА САМОЛИЧНОСТ ПРИ ПРЕКРАТЯВАНЕ НА ДЕЙСТВИЕТО НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ.....	35
3.6	ИДЕНТИФИКАЦИЯ И ПРОВЕРКА ЗА САМОЛИЧНОСТ СЛЕД ПРЕКРАТЯВАНЕ ДЕЙСТВИЕТО НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ.....	35
4	ОПЕРАТИВНИ ИЗИСКВАНИЯ.....	35
4.1	ПОДАВАНЕ НА ИСКАНЕ ЗА ИЗДАВАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ.....	36
4.1.1	ЛИЦА, ПОДАВАЩИ ИСКАНЕ ЗА ИЗДАВАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ	36
4.1.2	ОБРАБОТКА НА ИСКАНЕТО ЗА ИЗДАВАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ	37
4.1.3	ПОТРЕБИТЕЛСКИ УДОСТОВЕРЕНИЯ	37
4.2	ОБРАБОТКА НА ИСКАНЕТО	42
4.2.1	ИДЕНТИФИКАЦИЯ И ПРОВЕРКА ЗА САМОЛИЧНОСТ.....	42
4.2.2	ИЗЧАКВАНЕ ИЗДАВАНЕТО НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ	44
4.3	ИЗДАВАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ	44

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

4.3.1	ОБРАБОТКА.....	44
4.3.2	ПРЕДОСТАВЯНЕ НА ИНФОРМАЦИЯ.....	45
4.4	ПРИЕМАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ.....	45
4.4.1	ПОТВЪРЖДЕНИЕ ЗА ПРИЕМАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ.....	46
4.4.2	ПУБЛИКУВАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ.....	46
4.4.3	ИНФОРМАЦИЯ ЗА ДРУГИ СТРАНИ.....	46
4.5	УПОТРЕБА НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ И НА ДВОЙКАТА КЛЮЧОВЕ.....	46
4.5.1	ОТ СТРАНА НА ТИТУЛЯРИТЕ/СЪЗДАТЕЛИТЕ.....	46
4.5.2	ОТ ДОВЕРЯВАЩИТЕ СЕ СТРАНИ.....	47
4.6	ПОДНОВЯВАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ (RENEWAL).....	47
4.7	ИЗДАВАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ С ГЕНЕРИРАНЕ НА НОВА ДВОЙКА КЛЮЧОВЕ (RE-KEY).....	48
4.7.1	ОБСТОЯТЕЛСТВА, ПРИ КОИТО СЕ ПРИЛАГА ИЗДАВАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ С ГЕНЕРИРАНЕ НА НОВА ДВОЙКА КЛЮЧОВЕ (RE-KEY).....	48
4.7.2	КОЙ МОЖЕ ДА ПОИСКА АКТУАЛИЗАЦИЯ НА КЛЮЧОВА ДВОЙКА?.....	49
4.7.3	RE-KEY И ОБРАБОТКА НА ИСКАНЕТО.....	49
4.7.4	ИНФОРМАЦИЯ ЗА ТИТУЛЯРЯ/СЪЗДАТЕЛЯ.....	49
4.7.5	ПОТВЪРЖДЕНИЕ ЗА ПРИЕМАНЕ НА НОВО УДОСТОВЕРЕНИЕ.....	50
4.7.6	ПУБЛИКУВАНЕ НА НОВО КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ.....	50
4.7.7	ИНФОРМАЦИЯ ЗА ДОВЕРЯВАЩИ СЕ СТРАНИ.....	50
4.8	ПРОМЯНА В КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ.....	50
4.8.1	ОБСТОЯТЕЛСТВА ЗА ПРОМЯНА В КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ.....	50
4.8.2	КОЙ МОЖЕ ДА ПОИСКА ПРОМЯНА НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ?.....	51
4.8.3	ОБРАБОТКА НА ИСКАНЕТО.....	51
4.8.4	ИНФОРМАЦИЯ ЗА ПОТРЕБИТЕЛЯ.....	51
4.8.5	ПОТВЪРЖДЕНИЕ ЗА ПРИЕМАНЕ НА НОВО КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ.....	52
4.8.6	ПУБЛИКУВАНЕ НА НОВО КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ.....	52
4.8.7	ИНФОРМАЦИЯ ЗА ДОВЕРЯВАЩИТЕ СЕ СТРАНИ.....	52
4.9	СПИРАНЕ И ПРЕКРАТЯВАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ.....	53
4.9.1	ОСНОВАНИЯ ЗА ПРЕКРАТЯВАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ.....	54
4.9.2	ЛИЦА, ЛЕГИТИМИРАНИ ДА ПОИСКАТ ПРЕКРАТЯВАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ?	55
4.9.3	ПРОЦЕДУРА ЗА ПРЕКРАТЯВАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ.....	56
4.9.4	ГРАТИСЕН ПЕРИОД НА ПРЕКРАТЯВАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ.....	57
4.9.5	СРОК ЗА ОБРАБОТКА НА ИСКАНЕТО ЗА ПРЕКРАТЯВАНЕ.....	58
4.9.6	ПРОВЕРКА НА СПИСЪКА СЪС СПРЕНИ И ПРЕКРАТЕНИ УДОСТОВЕРЕНИЯ (CRL).....	58
4.9.7	ЧЕСТОТА НА ИЗДАВАНЕ НА СПИСЪКА СЪС СПРЕНИ И ПРЕКРАТЕНИ УДОСТОВЕРЕНИЯ (CRL).....	59
4.9.8	МАКСИМАЛНО ЗАБАВЯНЕ НА ПУБЛИКУВАНЕТО НА CRL.....	59
4.9.9	ОНЛАЙН ПРОВЕРКА НА СЪСТОЯНИЕТО НА УДОСТОВЕРЕНИЕ.....	59
4.9.10	ИЗИСКВАНИЯ ЗА ОНЛАЙН ПРОВЕРКА НА СЪСТОЯНИЕТО НА УДОСТОВЕРЕНИЕ.....	60
4.9.11	СПЕЦИАЛНИ ИЗИСКВАНИЯ ПО ОТНОШЕНИЕ НА НАРУШЕНИЕ НА СИГУРНОСТТА НА КЛЮЧА.....	60
4.9.12	ОСНОВАНИЯ ЗА СПИРАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ.....	60
4.9.13	ЛИЦА, ЛЕГИТИМИРАНИ ДА ПОИСКАТ СПИРАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ.....	60
4.9.14	ПРОЦЕДУРА ЗА СПИРАНЕ И ВЪЗОБНОВЯВАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ.....	61
4.9.15	ГРАТИСЕН ПЕРИОД НА СПИРАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ.....	61
4.9.16	ВЪЗОБНОВЯВАНЕ ДЕЙСТВИЕТО НА СПРЯНО УДОСТОВЕРЕНИЕ.....	61
4.9.17	ПРОЦЕДУРА ЗА ВЪЗОБНОВЯВАНЕ НА ДЕЙСТВИЕТО НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ.....	62
4.10	ПРОВЕРКА НА АКТУАЛНОТО СЪСТОЯНИЕ (СТАТУСА) НА КВАЛИФИЦИРАНИТЕ УДОСТОВЕРЕНИЯ.....	62
4.10.1	ХАРАКТЕРИСТИКИ.....	62
4.10.2	ДОПЪЛНИТЕЛНИ ФУНКЦИИ.....	62
4.11	ПРЕКРАТЯВАНЕ НА ДОГОВОР ЗА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ ОТ ПОТРЕБИТЕЛ.....	63
4.12	ДОВЕРИТЕЛНО СЪХРАНЕНИЕ НА ЧАСТЕН КЛЮЧ (ЕСКРОУ).....	63
5	КОНТРОЛ НА ФИЗИЧЕСКАТА И ОРГАНИЗАЦИОННА СИГУРНОСТ.....	63
5.1	КОНТРОЛ НА ФИЗИЧЕСКАТА СИГУРНОСТ.....	63
5.1.1	ПОМЕЩЕНИЯ И КОНСТРУКЦИЯ НА ПОМЕЩЕНИЯТА.....	64
5.1.2	ФИЗИЧЕСКИЯТ ДОСТЪП.....	64

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

5.1.3	ЕЛЕКТРИЧЕСКО ЗАХРАНВАНЕ И КЛИМАТИЧНИ УСЛОВИЯ	65
5.1.4	НАВОДНЕНИЕ	65
5.1.5	ПРЕДОТВРАТЯВАНЕ НА ПОЖАР И ЗАЩИТА ОТ ПОЖАР	66
5.1.6	СЪХРАНЕНИЕ НА НОСИТЕЛИ НА ДАННИ	66
5.1.7	ИЗХВЪРЛЯНЕ НА ОТПАДЪЦИТЕ	66
5.1.8	СРОК НА УПОТРЕБА НА ТЕХНИЧЕСКИ КОМПОНЕНТИ	66
5.2	ОРГАНИЗАЦИОНЕН КОНТРОЛ	67
5.2.1	ДОВЕРЕНИ РОЛИ	67
5.2.2	ИЗИСКВАНИЯ ЗА РАЗДЕЛЯНЕ НА ОТГОВОРНОСТИТЕ	68
5.2.3	ИДЕНТИФИКАЦИЯ И ПРОВЕРКА ЗА САМОЛИЧНОСТ ЗА ВСЯКА РОЛЯ	68
5.3	КОНТРОЛ НА ПЕРСОНАЛА	69
5.3.1	КВАЛИФИКАЦИЯ НА ПЕРСОНАЛА	69
5.3.2	ПРОЦЕДУРИ ЗА ПРОВЕРКА НА ПЕРСОНАЛА	70
5.3.3	ИЗИСКВАНИЯ ЗА ОБУЧЕНИЕ НА ПЕРСОНАЛА НА ЕВРОТРЪСТ	70
5.3.4	ЧЕСТОТА НА ОБУЧЕНИЯТА И ИЗИСКВАНИЯ ЗА НАДГРАЖДАНЕ НА КВАЛИФИКАЦИЯТА НА СЛУЖИТЕЛИТЕ	71
5.3.5	СМЯНА НА РАБОТАТА	71
5.3.6	САНКЦИИ ЗА ИЗВЪРШВАНЕ НА НЕРАЗРЕШЕНИ ДЕЙСТВИЯ	71
5.3.7	ДОГОВОР С ПЕРСОНАЛА	71
5.3.8	ДОКУМЕНТАЦИЯ, ПРЕДОСТАВЕНА НА ПЕРСОНАЛА	72
5.4	ЗАПИСИ НА СЪБИТИЯ И ПОДДЪРЖАНЕ НА ЖУРНАЛИ	72
5.4.1	ВИДОВЕ ЗАПИСИ	72
5.4.2	ЧЕСТОТА НА СЪЗДАВАНЕ НА ЗАПИСИ	74
5.4.3	ПЕРИОД НА СЪХРАНЕНИЕ НА ЗАПИСИ	74
5.4.4	ЗАЩИТА НА ЗАПИСИТЕ	74
5.4.5	ПОДДЪРЖАНЕ НА РЕЗЕРВНИ КОПИЯ НА ЗАПИСИ НА СЪБИТИЯ	75
5.4.6	СИСТЕМА ЗА УВЕДОМЯВАНЕ СЛЕД АНАЛИЗ НА ЗАПИСИ	75
5.4.7	УЯЗВИМОСТ И ОЦЕНКА	75
5.5	АРХИВИРАНЕ	76
5.5.1	ВИДОВЕ АРХИВИ	76
5.5.2	ПЕРИОД НА СЪХРАНЕНИЕ НА АРХИВА	76
5.5.3	ЗАЩИТА НА АРХИВНА ИНФОРМАЦИЯ	76
5.5.4	ВЪЗСТАНОВЯВАНЕ НА АРХИВИРАНА ИНФОРМАЦИЯ	77
5.5.5	ИЗИСКВАНИЯ ЗА ОТБЕЛЯЗВАНЕ НА ВРЕМЕТО НА АРХИВИРАНЕ	77
5.5.6	СЪХРАНЯВАНЕ НА АРХИВА	77
5.5.7	ПРОЦЕДУРИ ЗА ДОСТЪП И ПРОВЕРКА НА АРХИВИРАНАТА ИНФОРМАЦИЯ	77
5.6	ПРОМЯНА НА КЛЮЧ НА ДОСТАВЧИКА	78
5.7	КОМПРОМЕТИРАНЕ НА КЛЮЧОВЕ И ВЪЗСТАНОВЯВАНЕ СЛЕД АВАРИИ	78
5.7.1	ДЕЙСТВИЯ ПРИ АВАРИИ	79
5.7.2	ИНЦИДЕНТИ, СВЪРЗАНИ СЪС СРИВОВЕ В ХАРДУЕРА, СОФТУЕРА И/ИЛИ ДАННИТЕ	79
5.7.3	КОМПРОМИТИРАНЕ ИЛИ СЪМНЕНИЕ ЗА КОМПРОМЕТИРАНЕ НА ЧАСТЕН КЛЮЧ НА УДОСТОВЕРЯВАЩИЯ ОРГАН НА ЕВРОТРЪСТ	80
5.7.4	НЕПРЕКЪСНАТОСТ НА БИЗНЕСА И ВЪЗСТАНОВЯВАНЕ СЛЕД АВАРИИ	81
5.8	ПРЕКРАТЯВАНЕ НА ДЕЙНОСТТА НА ЕВРОТРЪСТ	82
5.8.1	ИЗИСКВАНИЯ, СВЪРЗАНИ С ПРЕХОДА ДО ПРЕКРАТЯВАНЕ НА ДЕЙНОСТТА НА ДОСТАВЧИКА	82
5.8.2	ПРЕХВЪРЛЯНЕ НА ДЕЙНОСТ КЪМ ДРУГ ДОСТАВЧИК НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	83
5.8.3	ОТНЕМАНЕ НА КВАЛИФИЦИРАН СТАТУТ НА ЕВРОТРЪСТ ИЛИ НА КВАЛИФИЦИРАНИЯ СТАТУТ НА СЪОТВЕТНА УСЛУГА	84
6	УПРАВЛЕНИЕ И КОНТРОЛ НА ТЕХНИЧЕСКАТА СИГУРНОСТ	84
6.1	ГЕНЕРИРАНЕ И ИНСТАЛИРАНЕ НА ДВОЙКА КЛЮЧОВЕ	84
6.1.1	ГЕНЕРИРАНЕ НА ДВОЙКА КЛЮЧОВЕ НА УДОСТОВЕРЯВАЩ ОРГАН	85
6.1.2	ГЕНЕРИРАНЕ НА ДВОЙКА КЛЮЧОВЕ НА ТИТУЛЯР/СЪЗДАТЕЛ	86
6.1.3	ДОСТАВКА НА ЧАСТЕН КЛЮЧ НА ПОТРЕБИТЕЛЯ	87
6.1.4	ДОСТАВКА НА ПУБЛИЧЕН КЛЮЧ ОТ ПОТРЕБИТЕЛ НА ДОСТАВЧИК	88
6.1.5	ДОСТАВКА НА ПУБЛИЧЕН КЛЮЧ НА ДОСТАВЧИКА НА ДОВЕРЯВАЩИТЕ СЕ СТРАНИ	88
6.1.6	ДЪЛЖИНА НА КЛЮЧОВЕ	88
6.1.7	ПАРАМЕТРИ НА ПУБЛИЧЕН КЛЮЧ	89
6.1.8	ИЗПОЛЗВАНЕ НА КЛЮЧА	90

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

6.2	ЗАЩИТА НА ЧАСТЕН КЛЮЧ И КОНТРОЛ НА КРИПТОГРАФСКИЯ МОДУЛ	90
6.2.1	СТАНДАРТИ ЗА КРИПТОГРАФСКИ МОДУЛИ	91
6.2.2	КОНТРОЛ НА ИЗПОЛЗВАНЕ И СЪХРАНЕНИЕ НА ЧАСТЕН КЛЮЧ	91
6.2.3	ДОВЕРИТЕЛНО СЪХРАНЕНИЕ НА ЧАСТЕН КЛЮЧ (ЕСКРОУ)	92
6.2.4	СЪХРАНЕНИЕ НА ЧАСТЕН КЛЮЧ	92
6.2.5	АРХИВИРАНЕ НА ЧАСТНИЯ КЛЮЧ	92
6.2.6	ТРАНСФЕР НА ЧАСТЕН КЛЮЧ В КРИПТОГРАФСКИ МОДУЛ	93
6.2.7	СЪХРАНЕНИЕ НА ЧАСТЕН КЛЮЧ В КРИПТОГРАФСКИЯ МОДУЛ	93
6.2.8	МЕТОД ЗА АКТИВИРАНЕ НА ЧАСТЕН КЛЮЧ	93
6.2.9	МЕТОД ЗА ДЕАКТИВИРАНЕ НА ЧАСТЕН КЛЮЧ	94
6.2.10	МЕТОД ЗА УНИЩОЖАВАНЕ НА ЧАСТЕН КЛЮЧ	94
6.2.11	ОЦЕНКА НА КРИПТОГРАФСКИЯ МОДУЛ	94
6.3	ДРУГИ АСПЕКТИ НА УПРАВЛЕНИЕТО НА ДВОЙКАТА КЛЮЧОВЕ	94
6.3.1	АРХИВИРАНЕ НА ПУБЛИЧЕН КЛЮЧ	95
6.3.2	ПЕРИОД НА ВАЛИДНОСТ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ И УПОТРЕБА НА КЛЮЧОВЕ	95
6.4	ДАННИ ЗА АКТИВИРАНЕ	96
6.4.1	ГЕНЕРИРАНЕ И ИНСТАЛИРАНЕ НА ДАННИ ЗА АКТИВИРАНЕ	96
6.4.2	ЗАЩИТА НА ДАННИ ЗА АКТИВИРАНЕ	97
6.4.3	ДРУГИ АСПЕКТИ НА ДАННИТЕ ЗА АКТИВИРАНЕ	97
6.5	СИГУРНОСТ НА КОМПЮТЪРНИТЕ СИСТЕМИ	97
6.5.1	СТЕПЕН НА КОМПЮТЪРНА СИГУРНОСТ	98
6.6	СИГУРНОСТ НА ЖИЗНЕНИЯ ЦИКЪЛ НА ТЕХНОЛОГИЧНАТА СИСТЕМА	98
6.6.1	КОНТРОЛИ ЗА РАЗВИТИЕ НА ТЕХНОЛОГИЧНАТА СИСТЕМА	98
6.6.2	КОНТРОЛИ ЗА УПРАВЛЕНИЕ НА СИГУРНОСТТА НА ТЕХНОЛОГИЧНАТА СИСТЕМА	99
6.6.3	ОЦЕНКА НА ЖИЗНЕНИЯ ЦИКЪЛ НА СИГУРНОСТТА НА ТЕХНОЛОГИЧНАТА СИСТЕМА	99
6.7	МРЕЖОВА СИГУРНОСТ	99
6.8	УДОСТОВЕРЯВАНЕ НА ВРЕМЕ	100
7	ПРОФИЛИ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ, CRL И НА OCSP	102
7.1	ПРОФИЛ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ	105
7.1.1	ВЕРСИЯ	106
7.1.2	ДОПУСТИМИ РАЗШИРЕНИЯ ВЪВ ФОРМАТА НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ	106
7.1.3	ИДЕНТИФИКАТОРИ НА АЛГОРИТМИТЕ НА ЕЛЕКТРОНЕН ПОДПИС/ПЕЧАТ	107
7.1.4	ФОРМИ НА ИМЕНУВАНЕ	107
7.1.5	ОГРАНИЧЕНИЯ НА ИМЕНАТА	107
7.1.6	ИДЕНТИФИКАТОР НА ПОЛИТИКА	107
7.1.7	ИДЕНТИФИКАТОР ЗА ПРОДЪЛЖЕНИЕ	107
7.1.8	ОЗНАЧЕНИЕ НА КВАЛИФИЦИРАНОТО УДОСТОВЕРЕНИЕ	107
7.1.9	ИЗПОЛЗВАНЕ НА ИДЕНТИФИКАТОР ЗА РАЗШИРЕНИЕ НА КЛЮЧА „КРИТИЧНО“	110
7.2	ПРОФИЛ НА СПИСЪКА СЪС СПРЕНИ И ПРЕКЪСНАТИ УДОСТОВЕРЕНИЕ (CRL)	110
7.2.1	ВЕРСИЯ	111
7.2.2	ФОРМАТ	111
7.2.3	ОСНОВНИ АТРИБУТИ НА СПИСЪКА СЪС СПРЕНИ И ПРЕКРАТЕНИ УДОСТОВЕРЕНИЯ (CRL)	111
7.2.4	ДОПЪЛНИТЕЛНИ АТРИБУТИ В СПИСЪКА СЪС СПРЕНИ И ПРЕКРАТЕНИ УДОСТОВЕРЕНИЯ (CRL)	112
7.2.5	ФОРМАТ НА ЕЛЕМЕНТ В СПИСЪКА СЪС СПРЕНИ И ПРЕКРАТЕНИ УДОСТОВЕРЕНИЯ (CRL)	112
7.3	ПРОФИЛ НА ОТГОВОР ЗА ОНЛАЙН ПРОВЕРКА НА СТАТУСА НА УДОСТОВЕРЕНИЕ (OCSP/ONLINE CERTIFICATE STATUS PROTOCOL)	112
7.3.1	ВЕРСИЯ	113
7.3.2	ФОРМАТ	113
7.3.3	ОСНОВНИ АТРИБУТИ НА УДОСТОВЕРЕНИЯТА ЗА СТАТУС	113
7.4	ДРУГИ ПРОФИЛИ	115
7.4.1	ПРОФИЛ НА КВАЛИФИЦИРАН ЕЛЕКТРОНЕН ВРЕМЕВИ ПЕЧАТ	115
7.5	ОСНОВНИ ПОЛЕТА В ПРОФИЛА НА КВАЛИФИЦИРАНИ ЕЛЕКТРОННИ ВРЕМЕВИ ПЕЧАТИ:	115
8	ОДИТ	116
8.1	ЧЕСТОТА НА ОДИТА	116
8.2	КВАЛИФИКАЦИЯ НА ПРОВЕРЯВАЩИТЕ ЛИЦА	117
8.3	ОТНОШЕНИЯ НА ПРОВЕРЯВАЩИТЕ ЛИЦА С ЕВРОТРЪСТ	117

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

8.4	ОБХВАТ НА ОДИТА	117
8.5	ДЕЙСТВИЯ, ПРЕДПРИЕТИ В РЕЗУЛТАТ НА ИЗВЪРШЕНИЯ ОДИТ	118
8.6	СЪХРАНЕНИЕ НА РЕЗУЛТАТИТЕ ОТ ОДИТИТЕ	118
9	ДРУГИ БИЗНЕС И ПРАВНИ ВЪПРОСИ.....	118
9.1	ЦЕНИ И ТАКСИ	118
9.1.1	ВЪЗНАГРАЖДЕНИЯ	119
9.1.2	ВЪЗНАГРАЖДЕНИЯ ЗА УДОСТОВЕРИТЕЛНИ, КРИПТОГРАФСКИ, ИНФОРМАЦИОННИ И КОНСУЛТАНТСКИ УСЛУГИ.....	120
9.1.3	ФАКТУРИРАНЕ	120
9.1.4	ВРЪЩАНЕ НА УДОСТОВЕРЕНИЕ И ВЪЗСТАНОВЯВАНЕ НА ПЛАЩАНЕ.....	120
9.1.5	БЕЗПЛАТНИ УСЛУГИ.....	121
9.2	ФИНАНСОВИ ОТГОВОРНОСТИ	121
9.2.1	ЗАСТРАХОВКА НА ДЕЙНОСТТА.....	122
9.2.2	ЗАСТРАХОВАТЕЛНО ПОКРИТИЕ	122
9.3	КОНФИДЕНЦИАЛНОСТ НА БИЗНЕС ИНФОРМАЦИЯ.....	122
9.3.1	ОБХВАТ НА КОНФИДЕНЦИАЛНАТА ИНФОРМАЦИЯ	123
9.3.2	НЕКОНФИДЕНЦИАЛНА ИНФОРМАЦИЯ.....	123
9.3.3	ЗАЩИТА НА КОНФИДЕНЦИАЛНАТА ИНФОРМАЦИЯ.....	124
9.4	НЕПРИКОСНОВЕНОСТ НА ЛИЧНИТЕ ДАННИ.....	124
9.4.1	ДЕКЛАРАЦИЯ ЗА ПОВЕРИТЕЛНОСТ	124
9.4.2	ИНФОРМАЦИЯ ТРЕТИРАНА КАТО ЛИЧНА	124
9.4.3	ИНФОРМАЦИЯ, КОЯТО НЕ СЕ СЧИТА ЗА ЛИЧНА	125
9.4.4	ОТГОВОРНОСТ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ	125
9.4.5	СЪГЛАСИЕ ЗА ИЗПОЛЗВАНЕ НА ЛИЧНИ ДАННИ	125
9.4.6	ДРУГИ ОБСТОЯТЕЛСТВА ЗА РАЗКРИВАНЕ НА ИНФОРМАЦИЯ.....	125
9.5	ПРАВА ВЪРХУ ИНТЕЛЕКТУАЛНА СОБСТВЕНОСТ	125
9.5.1	ПРАВО НА СОБСТВЕНОСТ НА ДАННИ В КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ.....	126
9.5.2	ПРАВО НА СОБСТВЕНОСТ НА ИМЕНА И ТЪРГОВСКИ МАРКИ.....	126
9.5.3	ПРАВО НА СОБСТВЕНОСТ НА ДВОЙКА КЛЮЧОВЕ	126
9.6	ОБЩИ ПОЛОЖЕНИЯ.....	126
9.6.1	ЗАДЪЛЖЕНИЯ, ОТГОВОРНОСТ И ГАРАНЦИИ НА ЕВРОТРЪСТ	127
9.6.2	ЗАДЪЛЖЕНИЯ, ОТГОВОРНОСТ И ГАРАНЦИИ НА РЕГИСТРИРАЩИЯ ОРГАН.....	129
9.6.3	ЗАДЪЛЖЕНИЯ НА ПОТРЕБИТЕЛИТЕ	131
9.6.4	ДЪЛЖИМА ГРИЖА НА ДОВЕРЯВАЩА СЕ СТРАНА	132
9.6.5	ЗАДЪЛЖЕНИЯ НА ДРУГИ СТРАНИ	133
9.7	ОСВОБОЖДАВАНЕ ОТ ОТГОВОРНОСТ	136
9.8	ОГРАНИЧЕНИЯ НА ОТГОВОРНОСТТА	137
9.9	ОТГОВОРНОСТ НА ТИТУЛЯРЯ/СЪЗДАТЕЛЯ	138
9.9.1	ОТГОВОРНОСТ НА ТИТУЛЯРЯ/СЪЗДАТЕЛЯ КЪМ ЕВРОТРЪСТ	138
9.10	СРОК И ПРЕКРАТЯВАНЕ НА „ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ“	138
9.10.1	СРОКОВЕ	138
9.10.2	ПРЕКРАТЯВАНЕ.....	139
9.10.3	ЕФЕКТ НА ПРЕКРАТЯВАНЕ И ОЦЕЛЯВАНЕ	139
9.11	БЕЛЕЖКИ И СЪОБЩЕНИЯ МЕЖДУ СТРАНИТЕ.....	139
9.12	ИЗМЕНЕНИЯ В „ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ“	139
9.13	РЕШАВАНЕ НА СПОРОВЕ	140
9.14	ПРИЛОЖИМО ПРАВО	140
9.15	СЪОТВЕТСТВИЕ С ПРИЛОЖИМОТО ПРАВО.....	140
9.16	ДРУГИ РАЗПОРЕДБИ.....	140
10	ИЗПОЛЗВАНИ ТЕРМИНИ И СЪКРАЩЕНИЯ	141
10.1	ПРИЛОЖЕНИЕ 1: ТЕРМИНИ И СЪКРАЩЕНИЯ НА БЪЛГАРСКИ ЕЗИК.....	141
10.2	ПРИЛОЖЕНИЕ 2: ТЕРМИНИ И СЪКРАЩЕНИЯ НА АНГЛИЙСКИ ЕЗИК	146

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

1 ВЪВЕДЕНИЕ

„ЕВРОТРЪСТ ТЕХНОЛЪДЖИС“ АД (Евротръст/ЕВРОТРЪСТ) е юридическо лице, регистрирано в Търговския регистър към Агенцията по вписванията с ЕИК 203397356 със седалище и адрес на управление: гр. София, район Изгрев, жк Изток, ул. „Николай Хайтов“ 2 вх. Д ет. 2. Телефон за контакт: + 359 2 448 58 58. Интернет адрес: <http://www.evrotrust.com>.

Дружеството осъществява публични функции по смисъла на Закона за електронния документ и удостоверителни услуги.

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 във всички държави-членки на Европейския съюз.

Иновативен в своята дейност, ЕВРОТРЪСТ предоставя на своите потребители създаването на електронни подписи от разстояние. В този икономически изгоден метод на работа средата на създаване на електронен подпис се управлява от доставчика от името на титуляря на електронния подпис. ЕВРОТРЪСТ гарантира, че прилага специфични 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 на електронния подпис.

1.1 ПРЕГЛЕД

„Практика при предоставяне на квалифицирани удостоверителни услуги“ (Практиката/Certification Practice Statement/CPS) на „Евротръст Технолджис“ АД е публичен документ. Той може да бъде променян по всяко време от доставчика и всяка нова редакция се съобщава на заинтересованите лица, като 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 и печати, както и за квалифицирани електронни времеви печати. В хода на управление се събират необходимите документи при приемане и проверка на заявление за издаване на квалифицирани удостоверения за електронни подписи и печати, електронни времеви печати, както и тези, които се съхраняват от доставчика в зависимост от заявената услуга. В Практиката се описва реализирането на мерките за сигурност при предоставяне на предлаганите от ЕВРОТРЪСТ квалифицирани удостоверителни услуги. Този

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

документ определя правата и задължения, както на участниците в инфраструктурата на публичния ключ (PKI) на доставчика, така и на всички външни лица (ако има такива), участващи в дейността по предоставяне на квалифицирани удостоверителни услуги. Описват се отговорностите, правата и задълженията на титуляря, съответно създателя на квалифициран електронен подпис или печат при ползване на удостоверителни услуги, предоставяни от ЕВРОТРЪСТ.

Настоящият документ съдържа описание на следните предлагани услуги:

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

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, регистриращ орган, търговски агенти, потребители, крайни потребители и всички доверяващи се страни.

Съдържанието и структурата на Настоящия документ е в съответствие със следните стандарти и стандартизационни документи:

- 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;

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

- ETSI EN 319 411-1 v1.1.1: Policy and security requirements for Trust Service Providers issuing certificates General requirements;
- ETSI EN 319 411-2 v2.1.1: Policy and security requirements for Trust Service Providers issuing certificates Requirements for trust service providers issuing EU qualified certificates;
- EN 319 421 v1.1.1: Policy and Security Requirements for Trust Service Providers issuing Electronic Time-Stamps;
 - 319 412-1 v1.1.1: Certificate Profiles Overview and common data structures;
 - 319 412-2 v2.1.1: Certificate Profiles Certificate profile for certificates issued to natural persons;
 - 319 412-3 v1.1.1: Certificate Profiles Certificate profile for certificates issued to legal persons;
 - 319 412-4 v1.1.1: Certificate Profiles Certificate profile for web site certificates issued to organisations;
 - 319 412-5 v2.1.1: Certificate Profiles QCStatements;
 - EN 319 422 v1.1.1 Time-stamping protocol and electronic time-stamp profiles.

Удостоверителните услуги се предоставят в съответствие с Интегрираната система за управление, прилагана от ЕВРОТРЪСТ, която включва изискванията на ISO: 9001: 2009 и ISO/IEC 27001:2013, Регламент (ЕС) № 910/2014¹ и приложимото законодателство в Република България.

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 ИМЕ И ИДЕНТИФИКАЦИЯ НА ДОКУМЕНТА

Настоящият документ е с пълно наименование „Практика при предоставяне на квалифицирани удостоверителни услуги“ от „Евротръст Технолъджис“ АД и е публично достъпен в електронна версия на интернет страницата на ЕВРОТРЪСТ или се предоставя по предварително поискване, изпратено на електронен адрес: office@evrotrust.com.

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

Практиката е свързана с Политиката на предоставяне на квалифицирани удостоверения за електронни подписи и печати и квалифицирани удостоверителни услуги. Политиката включва:

- описание на условията, които Доставчикът спазва и следва при издаване на квалифицирани удостоверения, както и приложимостта на тези удостоверения с оглед

¹ 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 (Регламента)

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

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 и 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: NCP за QCP-I ; NCP+ за QCP-I-qscd; NCP за QCP-n; NCP+ за QCP-n-qscd, DVCP за QCP-w и OVCP за QCP-w.

Квалифицираните удостоверенията, издадени от ЕВРОТРЪСТ, съдържат идентификатори на политиките за издаването им, които могат да бъдат проверени в PolicyInformation и CertificatePolicies.

На всяка от политиките, в съответствие с които се издават квалифицираните удостоверения от ЕВРОТРЪСТ се присвоява идентификатор на обект (OID – Object Identifier). Стойностите на идентификаторите на обекти 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	1.3.6.1.4.1.47272.1.1
Evrotrust TSA	1.3.6.1.4.1.47272.1.2
Evrotrust RSA Operational CA	1.3.6.1.4.1.47272.2
Evrotrust RSA QS Validation	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 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

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

evrotrust	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

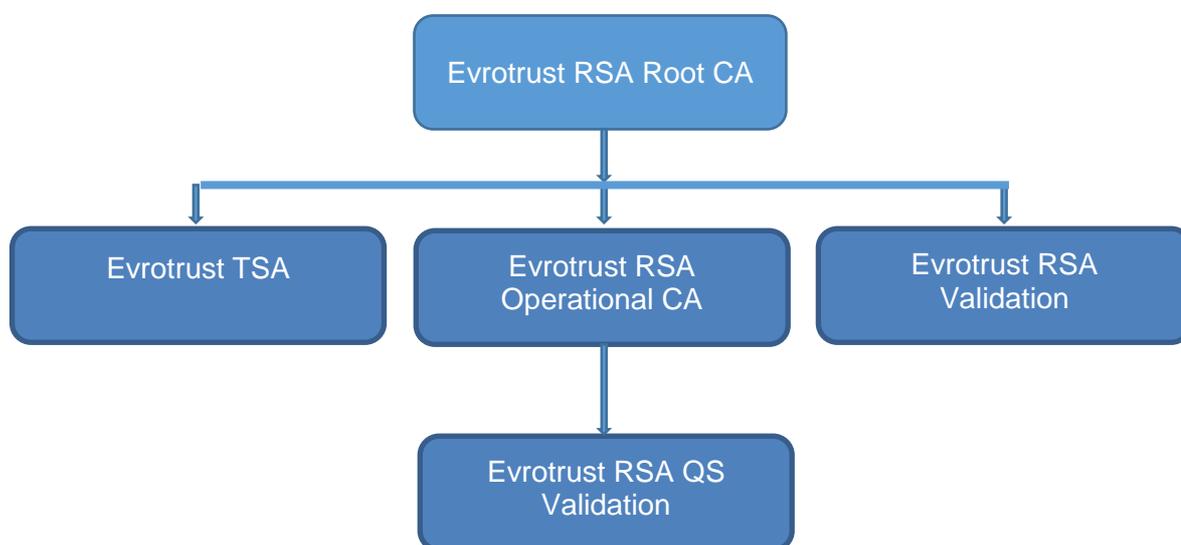
1.3 УЧАСТНИЦИ В ИНФРАСТРУКТУРАТА НА ЕВРОТРЪСТ

Практиката регулира най-важните отношения между лицата в структурата на ЕВРОТРЪСТ, неговите консултантски и одиторски екипи, както и отношенията между доставчика и потребителите на квалифицирани удостоверяващи услуги (доверяващи се страни и потребители). Изискванията и правилата описани в Практиката се прилагат за:

- Удостоверяващи органи;
- Регистриращи органи;
- Потребители;
- 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.

Йерархичния модел на технологичната система на ЕВРОТРЪСТ има следната последователност:



1.3.1 УДОСТОВЕРЯВАЩИ ОРГАНИ

1.3.1.1 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

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

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.

1.3.1.2 ОПЕРАТИВЕН УДОСТОВЕРЯВАЩ ОРГАН („EVROTRUST RSA OPERATIONAL CA“)

„Evrotrust RSA Operational CA“ издава потребителски квалифицирани удостоверения, съгласно Практиката и Политиката за предоставяне на квалифицирани удостоверителни услуги.

Потребителските квалифицирани удостоверения, които издава „Evrotrust RSA Operational CA“ в инфраструктурата на ЕВРОТРЪСТ биват :

- **Evrotrust Qualified Natural Person Certificate for QES/AES (E-Sign)** - издава се на физическо лице (Титуляр). Има характер на квалифицирано удостоверение за 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 КЕПечат/УсЕПечат. Може да се използва за да се гарантира произход и интегритет на изходящи от юридическото лице данни, напр.: електронни документи, снимки, архитектурни проекти, софтуер и други.

- **Evrotrust SSL Domain Validated/Organization Validated 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 Регламента и се използва за създаване на увереност у посетител, че титуляр на уебсайта е реален и легитимен субект. Чрез технологията се обезпечава 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 удостоверенията в тях данни.

Квалифицираният оперативен удостоверяващ орган на ЕВРОТРЪСТ изпълнява следните специфични задължения, включени в рамките на Политиката и Практиката на ЕВРОТРЪСТ:

- Приемане на електронно искане за квалифицирани удостоверения или

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

квалифицирани удостоверителни услуги;

- Издаване на квалифицирано удостоверение и квалифицирана удостоверителна услуга въз основа на исканията след идентификация на заявителите;
- Публикуване и поддържане на издадени квалифицирани удостоверения в съответствие с процедурите, описани в Политиката и Практиката на ЕВРОТРЪСТ;
- Приемане и изпълнение на искане за отмяна на квалифицирана удостоверителна услуга в съответствие с процедурите, посочени в Политиката и Практиката на ЕВРОТРЪСТ;
- Издаване на Списък със спрените и прекратени удостоверения (CRL);
- Публикуване на издадени Списък със спрените и прекратени удостоверения;
- Съхранява записите (логовете) по процеса на издаване на квалифицирани удостоверяващи 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 от Квалифицирания оперативен удостоверяващ орган.

1.3.2 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:

- Приема на искане за квалифицирана удостоверителна услуга;
- Проверява чрез подходящи средства и в съответствие с националното законодателство на самоличността/идентичността и, ако е приложимо, на всички специфични данни за физическото или юридическото лице, на което се издава квалифицирано удостоверение;
- Идентифицира лицето подало искане съгласно установените от ЕВРОТРЪСТ правила и процедури;
- Удостоверява верността и допустимостта на подадена електронно искане за квалифицирано удостоверение;
- Уведомява потребителите за издадено квалифицирано удостоверение;
- Осигурява надеждна среда за получаване на издадено квалифицирано удостоверение или използване на квалифицирана удостоверителна услуга;
- Инициира и предава на удостоверяващия орган заявки (може в електронна форма) за управление (спиране, възобновяване или отмяна) на издадени удостоверения;
- Извършва одобрение на заявки за продължаване действието на квалифицирано удостоверение от името на ЕВРОТРЪСТ;
- сключва договори за предоставяне на удостоверителни и други криптографски, информационни и консултантски услуги със Титулярите от името на ЕВРОТРЪСТ;

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

➤ 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.

1.3.3 ПОТРЕБИТЕЛИ

Всяко физическо или юридическо лице, което има сключен договор с ЕВРОТРЪСТ е потребител на квалифицирана удостоверителна услуга предоставена от ЕВРОТРЪСТ.

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

1.3.3.1 ТИТУЛЯР

Титулярят 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 квалифицираното удостоверение 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.

1.3.3.2 СЪЗДАТЕЛ НА ПЕЧАТ

Създателят на печат е юридическо лице, което създава електронен печат.

Създателят може подпечатва електронни обекти, независимо от тяхната същност (софтуер, снимки, музика, филми, книги, архитектурни проекти, бази данни, дизайн и др.), с което манифестира, 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).

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

Създателят е посочен в издаденото квалифицирано удостоверение за електронен печат като Създател.

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

1.3.4 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.

1.3.5 ДРУГИ УЧАСТНИЦИ

1.3.5.1 УДОСТОВЕРЯВАЩ ОРГАН ЗА ИЗДАВАНЕ НА КВАЛИФИЦИРАНИ ЕЛЕКТРОННИ ВРЕМЕВИ ПЕЧАТИ (EVROTRUST TSA)

Evrotrust TSA издава потребителски квалифицирани електронни времеви печати.

Evrotrust TSA осъществява следните дейности:

- Приема искания за удостоверяване на време на представено съдържание на електронен документ от Титуляря/Създателя или Доверяваща се страна;
- Използва технология за обвързване на датата и часа с данните по начин, който до голяма степен изключва възможността за незабелязана промяна на данните;

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

- Дейността му се основава на атомен източник на точно време, свързан с координираното универсално време;
- Подписва с усъвършенстван електронен подпис или подпечатва с усъвършенстван електронен печат от ЕВРОТРЪСТ;
- Осигурява възможност за доказване в последващ период във времето (след изтичане на периода на действие на квалифицирания електронен времеви печат) на факта на подписване/подпечатване на електронен документи или на друг електронен обект;
- Квалифицирани електронни времеви печати се издават на физически и на юридически лица, които са Титуляри/Създатели. Квалифицираният електронен времеви печат се ползва от презумпцията за точност на указаните от него дата и час и за цялост на данните, с които са обвързани датата и часът.
- Квалифицираният електронен времеви печат издаден от ЕВРОТРЪСТ, се признава за такъв във всички държави-членки на Европейския съюз.
- Квалифицираният електронен времеви печат може да се интегрира в процеса на създаване, изпращане или приемане на електронните подписи/печати, на електронно подписани/подпечатани документи и електронни транзакции, при архивиране на електронни данни, в електронни нотариати и др.
- ЕВРОТРЪСТ разработва и публикува отделна Политика на Органа за издаване на квалифицирани електронни времеви печати.

1.3.5.2 ОРГАНИ ЗА ВАЛИДИРАНЕ

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 базов удостоверяващ орган (Evrotrust RSA Root CA).
- Evrotrust RSA QS Validation – Използва се за валидиране на потребителски квалифицирани удостоверения и е издаден от оперативен удостоверяващ орган (Evrotrust RSA Operational CA).

Квалифицираната услуга се използва за валидирането на електронни подписи, електронни печати, услуги за електронна препоръчана поща, както и удостоверения, свързани с тези услуги. Валидиране се осъществява и на квалифицирани удостоверения за автентичност на уебсайт. Услугата по квалифицирано валидиране се предоставя от ЕВРОТРЪСТ, в качеството му на квалифициран доставчик на удостоверителни услуги.

В процеса на валидиране на квалифициран електронен подпис/печат, Органът за валидиране на ЕВРОТРЪСТ потвърждава валидността на квалифицирания електронен

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

подпис/печат, при условие че:

- удостоверението, придружаващо подписа/печата към момента на подписването/подпечатването е било квалифицирано удостоверение за електронен подпис/печат, отговарящо на изискванията на Регламент (ЕС) 910/2014;
- квалифицираното удостоверение, издадено от ЕВРОТРЪСТ е било валидно към момента на подписването/подпечатването;
- 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/подпечатването 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/подпечатани данни не е застрашена;
- изискванията на настоящия документ са били изпълнени към момента на подписването/подпечатването.

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 квалифицирано 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/подпечатани документи.

1.3.5.3 ОРГАН ЗА КВАЛИФИЦИРАНА УСЛУГА ЗА ЕЛЕКТРОННА ПРЕПОРЪЧАНА ПОЩА

Органът за квалифицирана услуга за електронна препоръчана поща предоставя услуга за електронна препоръчана поща, която позволява предаването на данни между трети страни по електронен път, предоставя доказателство във връзка с обработката на предаваните данни,

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

включително доказателство за изпращането и получаването на данните, и защитава предаваните данни срещу риск от загуба, кражба, повреда или непозволени изменения.

Квалифицираната услуга за електронна препоръчана поща на ЕВРОТРЪСТ отговаря на следните изисквания:

- предоставя се от ЕВРОТРЪСТ, в качеството му на квалифициран доставчик на квалифицирани удостоверителни услуги;
- гарантира с високо ниво на доверие идентификацията на изпращача;
- гарантира идентификацията на получателя преди доставянето на данните;
- изпращането и получаването на данни е обезпечено, чрез усъвършенстван електронен подпис или усъвършенстван електронен печат на доставчик на квалифицирани удостоверителни услуги по начин, който изключва всякаква възможност за незабелязана промяна на данните;
- всяка промяна на данните, необходима за целите на изпращането или получаването на данните, се обозначава ясно за подателя и за получателя на данните;
- датата и часът на изпращане и получаване, както и всяка промяна на данните се указват, чрез квалифициран електронен времеви печат.

1.4 УПОТРЕБА 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 изисквания.

Квалифицираните удостоверенията позволяват на лицата да се ползват от презумпция за наличие неопределени факти при участие в електронни трансакции. Те могат да бъдат използвани, когато се налага да се предпази даден обмен на електронна информация.

Квалифицирано удостоверение за публичен ключ е подписан от ЕВРОТРЪСТ електронен документ в X.509 стандарт, съдържащ предписани от Регламента реквизити, удостоверяващи връзката между Титуляря/Създателя и публичния му ключ, съответстващ на частния ключ, с който Титулярят/Създателят е създал електронния подпис/печат и служи за проверка на подписа/печата върху електронни документи и други електронни обекти.

Квалифицираните удостоверенията, издадени от ЕВРОТРЪСТ, могат да бъдат използвани за удостоверяване и създаване на високо ниво на доверие относно авторство/ източник и интегритет на определен електронен обект . Потребителите трябва да са запознати с изискванията за издаване на удостоверения и да формулират пред Евротръст целите на приложение, за да бъде издадено подходящо за тези цели удостоверение. При предоставяне на невярна информация от потребителите, те носят съответна отговорност.

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

1.4.1 ВИДОВЕ КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ И ПРЕПОРЪЧИТЕЛЕН ДИАПАЗОН НА ПРИЛОЖИМОСТ

➤ Квалифицирани удостоверения за електронен подпис на физически лица – те позволяват електронно подписване на електронни документи (PDF(PaDES), XML(XaDES), TXT(CaDES) и т.н.), включително пакети от документи (ASiC-E), както и на електронна поща (базирана на S/MIME (Secure/Multipurpose Internet Mail Extensions/Протокол за сигурно предаване на електронна поща през Интернет или криптографска система за защита на предаваните по електронна поща съобщения и на съхраняваните върху различни носители данни));

➤ Квалифицирани удостоверения за електронен печат на юридически лица/организации – те позволяват електронно подписване с електронен печат на различни активи на фирмата/организацията, например снимки, софтуер, видео и т.н.;

➤ SSL (Secure Socket Layer/Сигурен канал за предаване на данни) квалифицирани удостоверения за проверка на сървъра - те се използват от глобални интернет или екстранет услуги, опериращи по протокол SSL/TLS;

➤ квалифицирани удостоверения, използвани за проверка на автентичността на потребители (физически и юридически лица, хардуерни устройства) – използват се например в SSL/TLS /протокол;

➤ квалифицирани удостоверения, потвърждаващи статуса на удостоверения - те са издадени до сървърите, функциониращи в съответствие с OCSP протокол ;

➤ Квалифицирани електронни времеви печати - те са издадени на сървъри, в отговор на искане за определяне на точно време;

➤ Други – например атрибутивни удостоверения, удостоверяващи определени характеристики/атрибути на лице или обект.

1.4.2 УПОТРЕБА

Квалифицираните удостоверения на ЕВРОТРЪСТ не може да се използват по начин, несъвместим с обявената за тях цел, както и в приложения, които не отговарят на минималните изисквания, посочени в глава 1.4.1.

Удостоверенията, издавани и предоставяни от ЕВРОТРЪСТ могат да се използват за:

➤ Установяване на идентичност и самоличност на физическо лице или физическо лице, свързано с организация, в качеството му на неин законен или договорен представител, чрез атрибутивни удостоверения;

➤ Удостоверяване връзка между автор и публичния му ключ за проверка на авторство и

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

интегрет на електронно подписани документи;

- Удостоверяване на автентичност на уебсайт, с което посетител на уебсайт може да бъде уверен, че титуляр на уебсайта е реален и легитимен субект, както и за да се обезпечи сигурна комуникационна сесия с уебсайта по стандартизиран протокол;
- Доказателство, че даден електронен документ или друг информационен обект изхожда от юридическо лице, като се гарантира надеждния произход и целостта на обекта, чрез електронен печат, придружен от удостоверение за електронен печат, издадено от ЕВРОТРЪСТ;
- Подписване, криптиране и декриптиране на електронни данни, като електронни документи, бази данни, информационни обекти, електронна поща и други;
- Влизане и проверка на подписани данни, като документи, препоръчана електронна поща и други;
- Криптиране и декриптиране на данни и обмен на ключове, използвани за криптиране;
- Сигурно отдалечено съхраняване и използване на ключове за електронно подписване, респ. подпечатване;
- Други.

1.5 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, ЕВРОТРЪСТ се публикува.

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

2 ОТГОВОРНОСТ ЗА ПУБЛИКУВАНЕ И ХРАНИЛИЩЕ

2.1 ХРАНИЛИЩЕ

Публичният регистър на ЕВРОТРЪСТ представлява хранилище, в което са разположени актуални и предишни версии на електронни документи. В него се съдържат удостоверенията на инфраструктурата на публичния ключ (PKI/Public Key Infrastructure) и клиентски удостоверения. Хранилището се управлява и контролира от ЕВРОТРЪСТ. По тази причина ЕВРОТРЪСТ:

- гарантира, че всички удостоверения, публикувани в хранилището принадлежат на посочените в тях потребителите или на упълномощените от тях представители;

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

➤ гарантира, че удостоверенията на удостоверителните органи, принадлежащи на ЕВРОТРЪСТ и удостоверения на потребителите (по предварително тяхното одобрение) са публикувани;

➤ публикува актуални „Политика при предоставяне на квалифицирани удостоверителни услуги“, „Практика при предоставяне на квалифицирани удостоверителни услуги“, образци на документи, предназначени за потребителите и споразумения между страните, както и архивни версии;

➤ дава достъп до информацията относно статуса на удостоверенията, чрез публикуване на CRL, по OCSP или чрез въпроси, подадени чрез HTTP/HTTPS протокол (Протокол за пренос на хипертекст/ Hypertext Transfer Protocol);

➤ осигурява постоянен достъп до информацията в хранилището 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 хранилището.

Всички потребители, имат неограничен достъп до цялата информация в хранилището. Ограничения имат доверяващите се страни, но те са обичайно и единствено по отношение на удостоверенията на потребителите.

2.2 ИНФОРМАЦИЯ, ПУБЛИКУВАНА ОТ ЕВРОТРЪСТ

Публичният регистър е достъпен чрез интернет-страницата на ЕВРОТРЪСТ: <https://www.evrotrust.com>.

Достъп до публичния регистър 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 удостоверения за квалифициран електронен подпис/печат;

➤ Начин на използване на квалифициран електронен подпис/печат;

➤ Условия и ред за използване на квалифициран електронен подпис/печат, включително изисквания за съхраняване на частен ключ;

➤ Условия 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;

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

➤ Отговорност на ЕВРОТРЪСТ и на Титуляр/Създател на квалифициран електронен подпис/печат;

➤ Условия и ред, по които Титулярят/Създателят прави искане за отмяна 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 в хранилището си и:

➤ Базовото си удостоверение (Evrotrust RSA Root CA);

➤ Оперативните удостоверения на Удостоверяващите органи (Evrotrust RSA Operational CA);

➤ 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 на публичния Регистър 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 отмяна 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;

➤ Докладите от одити, извършени от оторизиран орган - всеки път, когато ЕВРОТРЪСТ ги получи;

➤ Допълнителна информация - при всяко настъпило събитие.

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

2.4 ДОСТЪП ДО ПУБЛИКАЦИИ

ЕВРОТРЪСТ предлага директорийни услуги за информацията съхранявана в хранилището (електронния регистър), като осигурява HTTP/HTTPS базиран достъп.

Цялата информация в хранилището, публикувана от ЕВРОТРЪСТ, е общодостъпна. Достъпът до тази информация не се ограничава от ЕВРОТРЪСТ, освен по искане на Титуляря/Създателя и само по отношение на негово валидно издадено удостоверение.

Информацията, публикувана в хранилището на ЕВРОТРЪСТ, е достъпна постоянно (24/7), 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 защитени Интернет страници на ЕВРОТРЪСТ се осъществяват чрез HTTPS протокол.

ЕВРОТРЪСТ е предприел мерки, логически и физически механизми, за защита срещу неоторизирано добавяне, премахване и промяна на информацията, публикувана в хранилището.

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

Тази част от Практиката представя общите правила за проверка на самоличността 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.

Доставчикът самостоятелно или чрез свой Регистриращ орган:

- 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;

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

- уведомява Удостоверяващия орган да издаде исканото удостоверение.

Доставчикът, съответно Регистриращият орган събира и получава необходимата информация за идентификация и

проверка на самоличността на Титуляря/Създателя.

Идентификацията и проверката на самоличността на Титуляря/Създателя се извършва преди да бъде издадено квалифицирано удостоверение. Тя изисква негово лично присъствие или присъствие на упълномощен представител на лицето подало искане пред служител на ЕВРОТРЪСТ или на негов Регистриращ орган.

ЕВРОТРЪСТ е разработило специализирана система за отдалечена видеоидентификация чрез мобилно приложение, инсталирано на смарт-устройство на потребителя. Същото гарантира идентификация на потребителя в реално време чрез автоматична видеоидентификация 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. Системата за видеоидентификация на физически лица, използвана от ЕВРОТРЪСТ, е сертифицирана за съответствие с изискванията на Регламент 910/2014 ЕС от орган за проверка на съответствие, като даваща същата степен на сигурност, както лично явяване, на основание чл. 24, т. 4 от Регламента.

Автоматизирана отдалечена идентификация на юридическите лица, от името на които Титулярят заявява издаване на удостоверение отдалечено, чрез инсталираното приложение на смарт-устройство и 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.

3.1 ИМЕНА

Квалифицираните удостоверения са с формат, съответстващ на стандарта X.509. Регистриращите органи проверяват и гарантират, че имената в исканията за издаване на

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

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 идентифицирано. Името може да съдържа и адрес на електронна поща на потребителя, който е в съответствие с препоръка RFC 822.

3.1.2 НЕОБХОДИМОСТ ОТ ОТГРАНИЧИМИ 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 използвано 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 абоната,
- поле SerialNumber – уникален идентификатор на на физическото лице,

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

➤ 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 обичайно име (Common Name, CN) съдържа име на физическото лице, с което то е обичайно обозначавано в дейността му.

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.

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 искане или от упълномощен представител при регистрация на първоначално искане за издаване на удостоверение и която се проверява от Регистрацията орган въз основа на представени документи, видеоидентификация и проверки в първични държавни регистри.

ЕВРОТРЪСТ гарантира уникалност на „DN“ на Титуляря/Създателя в неговей 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

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

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 права 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 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 Регламента.

Потребителят е длъжен 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, електронна поща и адрес.

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

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 електронна заявка 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 да го предаде 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 договора и заявяване издаването на квалифицирано удостоверение за квалифициран електронен подпис и незабавно автоматизирано подписване с него на договора с ЕВРОТРЪСТ след издаването му.

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 заявката.

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.

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

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

3.2.2 УСТАНОВЯВАНЕ НА ИДЕНТИЧНОСТ НА ЮРИДИЧЕСКО ЛИЦЕ

Установяването на идентичността на българско юридическо лице (Създател), се осъществява от представител на Регистриращия орган, чрез проверка в съответните регистри по предоставен ЕИК, съответно БУЛСТАТ по реда на ЗЕУ. За българските юридически лица, които не са търговци, както и за чуждестранните 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.

Списък с изискуеми документи се поддържа на сайта на ЕВРОТРЪСТ в интернет. След копиране на всички изискуеми документи, със съгласието на лицето подало искане, 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 самоличността на юридическо лице има две цели. Първата цел е да се докаже, че по време на разглеждане на заявката 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 българското законодателство.

3.2.3 УСТАНОВЯВАНЕ НА САМОЛИЧНОСТ НА ФИЗИЧЕСКО ЛИЦЕ

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

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 местоживееене 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 Регламента;

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.

ЕВРОТРЪСТ извършва проверка на достоверността на информацията 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 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 “Evrotrust 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.

3.2.5 НЕПОТВЪРДЕНА ИНФОРМАЦИЯ

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

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 тази информация.

3.2.6 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 Публичния регистър/Хранилището на издадените удостоверения или съответно 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.

3.2.7 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 - заявител.

3.2.8 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 Регламента формати на квалифицираните електронни подписи и печати квалифицираните удостоверения не надвишават задължителните изисквания, предвидени в Регламента. 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 ПРИ ПОДНОВЯВАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

ЕВРОТРЪСТ може да поднови валидно квалифицирано удостоверение, частният ключ за който е персонализиран върху устройство за сигурност създаване на подпис и което не е прекратено в срока му на валидност, по два начина:

- като запази генерираната двойка ключове за текущото удостоверение (“Renewal”);
- като генерира нова двойка ключове (“Re-key”).

Удостоверението се подновява за същата двойка асиметрични ключове (Renewal) на текущото удостоверение на Титуляря/Създателя, ако информацията за Титуляря/Създателя в удостоверението, което се подновява, е идентична с тази в текущото. Само периодът на валидност в подновеното удостоверение е различен от този в текущото.

ЕВРОТРЪСТ допуска многократно подновяване на квалифицираното удостоверение като запазва текущата двойка ключове (Renewal), но препоръчва тази практика да се ограничава с цел да се намали риска от компрометиране на частния ключ.

ЕВРОТРЪСТ подновява текущо удостоверение на Титуляря/Създателя с нова двойка ключове (Re-key), само ако същият подаде искане при Регистриращия орган и декларира, че няма настъпили промени в удостоверената информация в текущото квалифицирано удостоверение. Подновеното удостоверение има различен публичен ключ и нов период на валидност, като удостоверената информация за Титуляря/Създателя се запазва.

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

За идентификация и проверка на самоличност на Титуляря/Създателя на квалифицираното удостоверение, което се подновява, не се изисква неговото лично присъствие 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 и прекратява незабавно текущото квалифицирано удостоверение.

Подновяване на удостоверение на Удостоверяващ орган на ЕВРОТРЪСТ не се допуска. при всички обстоятелства, които налагат подмяна на удостоверението. Практиката налага винаги да се издава ново квалифицирано удостоверение на Удостоверяващия орган.

Доставчикът съблюдава следните времеви ограничения и изисквания за идентификация при подновяване на квалифицирано удостоверение за електронен подпис/печат:

Период	Подновяване	Изисквания
До 30 дни преди изтичане срока на	➤ чрез Renewal	➤ Да няма промяна в „DN“ на

валидност на квалифицираното удостоверение, което не е прекратено и което няма промяна в удостоверената в него информация	➤ чрез Re-key	удостоверението ➤ Удостоверението да е било издадено на SSCD ➤ 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 Renewal ➤ чрез Re-key	➤ Да няма промяна в „DN“ на удостоверението ➤ Удостоверението да е било издадено на SSCD ➤ 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, политиката за подновяване е винаги “re-key”, като задължително се издава ново удостоверение. В този случай проверка за самоличност и идентификация не се извършва.

3.4 ИДЕНТИФИКАЦИЯ И ПРОВЕРКА НА САМОЛИЧНОСТ 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.

Доставчикът, чрез Регистриращия орган, не извършва идентификация и проверка за самоличност 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.

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

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

Когато ЕВРОТРЪСТ, чрез Регистриращия орган или сам 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 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 СЛЕД ПРЕКРАТЯВАНЕ ДЕЙСТВИЕТО 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 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;

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

- 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 чрез “Renewal”;
- подновяване на квалифицирано удостоверение чрез “Re-key”;
- 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 лично 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

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

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

4.1.3 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 Регламента ;
- 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.

4.1.3.1 УДОСТОВЕРЕНИЯ НА УДОСТОВЕРЯВАЩ ОРГАН И РЕГИСТРИРАЩ ОРГАН

Регистриращите органи, които предоставят квалифицирани услуги, които не са в

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

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.

4.1.3.2 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,

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

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.

4.1.3.3 ПОДНОВЯВАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ (RENEWAL), ГЕНЕРИРАНЕ НА НОВА ДВОЙКА КЛЮЧОВЕ (REKEY) 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.

Подновяване на квалифицирано удостоверение, което не е било прекратено в периода му на валидност, може да се изпълни по два начина:

- запазва се генерираната двойка ключове за текущото удостоверение (Renewal);
- генерира се нова двойка ключове (Re-key).

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 лично да посети Регистриращия орган на ЕВРОТРЪСТ.

Титулярят/Създателят или упълномощеното лице може да поднови многократно свое квалифицирано удостоверение за електронен подпис/печат. ЕВРОТРЪСТ не препоръчва многократното подновяване на квалифицирано удостоверение, чрез Renewal, с цел да се намали риска от компрометиране на частния ключ.

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

ЕВРОТРЪСТ препоръчва на Титуляря/Създателя или упълномощеното лице да поднови свое квалифицирано удостоверение чрез Re-key.

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

Регистриращият орган ще поднови едно квалифицирано удостоверение за електронен подпис/печат чрез **Renewal** при съблюдаване на следните условия:

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

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.

Искане за подновяване на квалифицирано удостоверение, чрез Renewal или Re-key, 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 е използван преди това, в случай на подновяване или промяна на удостоверение или новия публичен ключ, в случай на Re-key), 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

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

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.

4.1.3.4 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.

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

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.

4.2 ОБРАБОТКА НА ИСКАНЕТО

ЕВРОТРЪСТ приема искания, 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

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

настоящия документ.

4.2.1.1 ПРИЕМАНЕ ИЛИ ОТХВЪРЛЯНЕ НА ИСКАНЕ

4.2.1.2 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.

4.2.1.3 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 :

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

- ако потребителят не може да докаже, своите права върху предложението 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.

4.2.2 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 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:

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

- 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 сървъра 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.

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 удостоверението 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.

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

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

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 удостоверението 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 публичния регистър/хранилището на ЕВРОТРЪСТ.

4.4.3 ИНФОРМАЦИЯ ЗА ДРУГИ СТРАНИ

След публикуването на издаденото удостоверение в Публичния регистър на издадените удостоверения, то става достъпно за всички заинтересовани страни.

4.5 УПОТРЕБА НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ И НА ДВОЙКАТА КЛЮЧОВЕ

4.5.1 ОТ СТРАНА НА ТИТУЛЯРИТЕ/СЪЗДАТЕЛИТЕ

Титулярите/Създателят трябва да използват частните ключове и квалифицираните

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

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 отмяна на валидността на даден ключ;
- когато удостоверението е спряно, доверяващата се страна не трябва да приема публичния ключ.

4.6 ПОДНОВЯВАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ (RENEWAL)

Подновяване на квалифицирано удостоверение с Renewal означава подмяна на валидно удостоверение с ново, без да се променя съществуващата информация в него, освен нов сериен номер и нов срок на валидност.

Подновяване се извършва само в рамките на срока на валидност на актуално удостоверение. 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.

Подновяване на квалифицирано удостоверение, което е заявено отдалечено, чрез използване на мобилното приложение на ЕВРОТРЪСТ, е недопустимо.

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

4.7 ИЗДАВАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ С ГЕНЕРИРАНЕ НА НОВА ДВОЙКА КЛЮЧОВЕ (RE-KEY)

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;
- Re-key се отнася до конкретно валидно удостоверение, посочено в искането. В следствие на това, новото удостоверение включва същото съдържание, като единствените разлики са: нов сериен номер, нов публичен ключ, нов срок на валидност и нов електронен подпис/печат.

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 (RE-KEY)

Едно потребителско искане за подновяване, предоставено пред ЕВРОТРЪСТ, може да се прилага само 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;
- няма никакво валидно удостоверение, издадено в рамките на политиката за удостоверяване, определена в настоящата Практика;
- удостоверението не е издадено отдалечено, чрез мобилното приложение на ЕВРОТРЪСТ

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

4.7.2 КОЙ МОЖЕ ДА ПОИСКА АКТУАЛИЗАЦИЯ НА КЛЮЧОВА ДВОЙКА?

Искането за издаване на квалифицирано удостоверение с генериране на нова двойка ключове (Re-key) се извършва единствено от Титуляр/Създател или упълномощено от него лице.

4.7.3 RE-KEY И ОБРАБОТКА НА ИСКАНЕТО

Подновяване на удостоверение за електронен подпис/печат с Re-key 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 лично Регистриращия орган на ЕВРОТРЪСТ. 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 незабавно известява потребителя за причината. В такъв случай потребителя с отхвърлено искане за подновяване, може да заяви издаване на ново удостоверение за електронен подпис/печат.

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 подновяването 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)

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

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/Създателят 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/Създателят 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 Публичния регистър/Хранилището.

4.7.7 ИНФОРМАЦИЯ ЗА ДОВЕРЯВАЩИ СЕ СТРАНИ

След незабавното публикуване на издадено квалифицирано удостоверение в Публичния регистър на издадените удостоверения, то става достъпно за всички заинтересовани страни.

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.

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

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 или упълномощено от него лице може да поиска промяна на квалифицирано удостоверение при условие, че са изпълнени изискванията и условията за подновяване 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 лично Регистриращия орган на ЕВРОТРЪСТ. 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 удостоверението за електронен подпис/печат,

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

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 Публичния регистър/хранилището.

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

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

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 хранилището. 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 Органа 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 срыв 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.

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

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 обсег 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.

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

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“.

4.9.2 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;
- 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 лично 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 кратисен период. Впоследствие се изисква лично явяване при 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

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

отдалечено. В този случай се счита, че Титулярят е идентифициран, предвид активирането на ПИН за достъп до приложението или чрез друг биометричен идентификатор.

4.9.3 ПРОЦЕДУРА ЗА ПРЕКРАТЯВАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ

4.9.3.1 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 пред оторизиран 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 лично Регистриращия орган на ЕВРОТРЪСТ за последваща проверка на идентичността, респективно самоличността на потребителя.
- 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.

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

➤ 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.

4.9.3.2 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.

4.9.4 ГРАТИСЕН ПЕРИОД НА ПРЕКРАТЯВАНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ

Преди да прекрати действието на валидно квалифицирано удостоверение, ЕВРОТРЪСТ

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

спира действието му gratuitен период. В рамките на този gratuitен период ЕВРОТРЪСТ обработва 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 gratuitния период, ЕВРОТРЪСТ възобновява действието на удостоверението;

ЕВРОТРЪСТ допуска действието на удостоверението да бъде възобновено преди да изтече gratuitния 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 gratuitен 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 Регистрационния орган, както и засегнатите крайни потребители биват информирани автоматично за това прекратяване.

4.9.5 СРОК ЗА ОБРАБОТКА НА ИСКАНЕТО ЗА ПРЕКРАТЯВАНЕ

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

4.9.6 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 „Evrotrust RSA QS Validation“.

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

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

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

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

ЕВРОТРЪСТ, чрез своя оперативен Удостоверяващ орган, публикува в хранилището незабавно 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) на всеки 2 седмици, ако няма спиране или прекратяване на удостоверение през този период.

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

4.9.8 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).

4.9.9 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 „Evrotrust RSA QS Validation“ през Интернет. Като отговор за всяка заявка, OCSP сървъра, 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).

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

4.9.10 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 на страницата на ЕВРОТРЪСТ на адрес: <https://www.evrotrust.com>.

Доверяващите се страни трябва да проверяват публикуваната информация в хранилището, свързана с използваните удостоверения, на които те искат да разчитат. ЕВРОТРЪСТ не носи отговорност за настъпили вреди и последствия от неизпълнение на посочените изисквания.

4.9.11 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.

4.9.12 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.

4.9.13 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);

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

4.9.14 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.

4.9.15 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, но не по-дълго от 72 часа.

Гратисен период на спиране на квалифицирани удостоверения, издадени отдалечено, през мобилното приложение, не се допуска.

4.9.16 ВЪЗОБНОВЯВАНЕ ДЕЙСТИЕТО 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.

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

4.9.17 ПРОЦЕДУРА ЗА ВЪЗОБНОВЯВАНЕ 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 (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.

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

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 и ключовете са персонализирани върху преносими носители, 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 чрез ПИН-кода на потребителя вид 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 стандарта ISO/IEC 27001:2013 и ISO/IEC 19011:2011.

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

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

на:

- неразрешен достъп, нанасяне на щети и намеса в условията на работа;
- загуба, вреди или компрометиране на ресурси;
- компрометиране или кражба на информация или средства за обработка на информацията.

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 удостоверяващ орган на време – Evrotrust TSA;
- Квалифициран удостоверяващ орган за проверка на статуса на удостоверенията –

Evrotrust RSA QS Validation;

- Регистри и хранилища;
- 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 конструирано и оборудвано помещение 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

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

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 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.

5.1.4 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.

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

5.1.5 ПРЕДОТВРАТЯВАНЕ 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.

5.1.6 СЪХРАНЕНИЕ НА НОСИТЕЛИ НА ДАННИ

Всички носители съдържащи софтуер, архиви 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 сейфове.

5.1.7 ИЗХВЪРЛЯНЕ НА ОТПАДЪЦИТЕ

Доставчикът е създавал 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 унищожават, чрез изтриване или форматиране на устройството без възможност за възстановяване.

5.1.8 СРОК НА УПОТРЕБА НА ТЕХНИЧЕСКИ КОМПОНЕНТИ

Експлоатационният срок на физическите елементи в състава на всички критични компоненти

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

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.

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.

5.2.1.1 ДОВЕРЕНИ РОЛИ В ЕВРОТРЪСТ

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 Регламента, 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

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

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

Доверените дейности на персонала на ЕВРОТРЪСТ се изпълняват от различни лица.

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;

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

- 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;

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

- 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 ЕВРОТРЪСТ

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

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

„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

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

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.

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

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

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 Публичния регистър; 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 отговаря за 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

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

ЕВРОТРЪСТ.

5.4.2 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.

5.4.3 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 20 (двадесет) години.

5.4.4 ЗАЩИТА НА ЗАПИСИТЕ

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;

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

- 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.

5.4.5 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.

5.4.6 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.

5.4.7 УЯЗВИМОСТ И ОЦЕНКА

ЕВРОТРЪСТ класифицира и поддържа регистри на всички активи в съответствие с изискванията на ISO/IEC 27001:20013. 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

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

анализ се извършва от Съвета на директорите.

Администраторът по сигурността е отговорен за извършване на вътрешните одити. Той контролира опазване на записите по сигурността в журналите, коректното архивиране на резервните копия, дейностите, изпълнени в случай на заплахи и съответствието с настоящата Практика.

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 минимум 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 изтрити през периода на съхранение.

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

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 Регистриращия 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

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

възможно най-бързо, съгласно вътрешните процедури и правила в ЕВРОТРЪСТ.

5.6 ПРОМЯНА НА КЛЮЧ НА ДОСТАВЧИКА

Доставчикът може да промени ключа, съответстващ на издадено удостоверение, само като издаде ново удостоверение или поднови текущото с „Re-Key”.

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 частния 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.

5.7 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 заплаха 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

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

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.

5.7.1 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 сринове 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.

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

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

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 сригове в хардуера, софтуера или в данните, Доставчикът уведомява потребителите, възстановява компонентите на инфраструктурата и приоритетно възобновява достъпа до Публичния регистър и 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..

5.7.3 КОМПРОМИТИРАНЕ 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 удостоверения, като се посочва подходяща причина за прекратяването им;
 - издават се нови удостоверения на засегнатите потребители;

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

➤ 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.

5.7.4 НЕПРЕКЪСНАТОСТ НА БИЗНЕСА И ВЪЗСТАНОВЯВАНЕ СЛЕД АВАРИИ

ЕВРОТРЪСТ е разработил „План за непрекъсваемост на дейността“ за случаите на възникване на аварии, като например големи системни или мрежови прекъсвания. 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.

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;

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

- 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:

- 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.

5.8 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.

5.8.1 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

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

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.

5.8.2 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

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

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.

5.8.3 ОТНЕМАНЕ НА КВАЛИФИЦИРАН СТАТУТ НА ЕВРОТРЪСТ 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.

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. 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;

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

- 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 оперативния Удостоверяващи органи, съответно „Evrotrust RSA Root CA“ и „Evrotrust RSA Operational 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

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

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 отделно 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.

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. Титулярят 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. Титулярят/Създателят носи отговорност за пропуски или действия на упълномощени от тях лица, които са делегирани да генерират, пазят или съхраняват техните частни ключове.

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

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 заяване 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 с неговия ПИН-код за достъп вид.

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

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

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 и само за времето, през което се използва.

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 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 чрез страницата на ЕВРОТРЪСТ в интернет.

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 и достъпни в хранилището на ЕВРОТРЪСТ на адрес: <https://www.evrotrust.com> .

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

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

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 оперативните органи „Evrotrust TSA“, „Evrotrust RSA QS Validation“ и „Evrotrust RSA Validation“ 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, генерирана чрез инфраструктурата на ЕВРОТРЪСТ е 2048 бита, с приложима комбинация на асиметрични и хеш алгоритми: 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	sha256-with-RSA
Evrotrust Qualified Natural Person Attribute Certificate for QES	RSA 2048	sha256-with-RSA
Evrotrust Qualified Legal Person Certificate for QESeal	RSA 2048	sha256-with-RSA
Evrotrust SSL Domain Validated Certificate	RSA 2048	sha256-with-RSA
Evrotrust SSL Organization Validated Certificate	RSA 2048	sha256-with-RSA
Evrotrust Qualified Natural Person Certificate for AES	RSA 2048	sha256-with-RSA
Evrotrust Qualified Legal Person Certificate for AESeal	RSA 2048	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 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.

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

Използваната среда за генериране и съхраняване на ключовете на основните компоненти в инфраструктурата на ЕВРОТРЪСТ „Evrotrust RSA Root CA“, „Evrotrust RSA Operational CA“, „Evrotrust TSA“ и „Evrotrust RSA QS Validation“ е криптомодул (HSM) с удостоверяено 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.

6.1.8 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.

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.

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

6.2.1 СТАНДАРТИ ЗА КРИПТОГРАФСКИ МОДУЛИ

Основните компоненти в инфраструктурата на ЕВРОТРЪСТ „Evrotrust RSA Root CA“, „Evrotrust RSA Operational 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 криптосистемата (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 криптосистемата (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

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

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 СЪХРАНЕНИЕ НА ЧАСТЕН КЛЮЧ (ЕСКРОУ)**

Прилагат се правилата, описани по-горе.

6.2.4 **СЪХРАНЕНИЕ 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

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

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 Регистриращия 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 оперативната 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 СЪХРАНЕНИЕ НА ЧАСТЕН КЛЮЧ В КРИПТОГРАФСКИЯ 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.

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

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 унищожение на 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 FIPS 140-2 Level 3.

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

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

удостоверяващия орган.

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 в хранилището, достъпно на интернет-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 публичния регистър на действащи удостоверения. 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 Публичен регистър на интернет-страницата на ЕВРОТРЪСТ.

Публичните ключове на Титуляри/Създатели се съхраняват и периодично архивират в хранилището.

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	15 (петнадесет) години
Evrotrust TSA	5 (пет) години
Evrotrust RSA QS Validation	5 (пет) години

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

Титуляр/Създател	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 при 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.

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.

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

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 създава специален криpto-ключ, който се генерира от отговори на три тайни въпроса, зададени от потребителя към момента на регистрацията му чрез мобилното приложение. Отговорите на въпросите не се пазят 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

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

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.

За управление на сигурността на компютърните системи в ЕВРОТРЪСТ се взимат в предвид изискванията на ISO/IEC 27001:2015.

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.

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.

6.6 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.

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.

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

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 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.

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).

Компютърната система на ЕВРОТРЪСТ е защитена срещу отказ на услугите при наличие на атаки. Контролът за сигурност е разработен на базата на защитна стена (firewall) и филтриране на трафика на рутерите и прокси услугите. Опити за проникване в системата се наблюдават посредством изградената IDS/IPS система. Всички аларми включили се при проникване или потенциално проникване, както и атаки от тип „Отказ от достъп“ се изпращат към системните администратори за анализ.

Опитите за неправомерен достъп до системата се документират чрез Intrusion Prevention System (IPS).

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

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.

6.8 УДОСТОВЕРЯВАНЕ НА ВРЕМЕ

Evrotrust издава удостоверения за време съгласно Регламент (EU) № 910/2014 и в пълно съответствие с ETSI EN 319 422, ETSI TS 119 421, IETF RFC 3161 и IETF RFC 5816.

Органът за издаване на квалифицирани електронни времеви печати „Evrotrust TSA“ е обособено и неделимо звено към Удостоверяващия орган на ЕВРОТРЪСТ в структурата на Евротръст. „Evrotrust TSS“ (Time-stamping service/услуга по удостоверяване на време) издава Удостоверение за време в съответствие с ETSI EN 319 422. Чрез включването на обектен идентификатор: 1.3.6.1.4.1.47272.1.2 в издадените удостоверения за време, Евротръст потвърждава съответствие с „Политика и практика на органа за удостоверяване на време“. Обектният идентификатор е в съответствие с ETSI BTSP (best practices policy for time-stamp) OID=0.4.0.2023.1.1, съгласно ETSI EN 319 422.

Издаваните квалифицирани електронни времеви печати (time-stamp токъни) са съвместими с RFC 3161. Услугата издава RSA 2048 битови криптирани удостоверения за време, които приемат едни от следните алгоритми: SHA256 и SHA384.

Органът за издаване на квалифицирани електронни времеви печати „Evrotrust TSA“ приема заявки за издаване на квалифицирани електронни времеви печати на представено съдържание на електронен документ от Титуляря или Доверяваща се страна. Той изготвя квалифициран електронен времеви печат на представената хеш-стойност на електронен документ и осигурява възможност за последващо (след периода на валидност на квалифицираното удостоверение за електронен подпис/печат) доказване спрямо приемащата страна на факта на подписването на изявление или на електронен документ.

Квалифицирани електронни времеви печати могат да се интегрират в процеса на създаване или приемане на квалифициран електронен подпис/печат, на електронно подписани документи и електронни транзакции, при архивиране на електронни данни, в електронни нотариати и други.

За изпълнението на своята услуга „Evrotrust TSA“ използва няколко частни ключа. Едната двойка ключове (на базовия удостоверяващ орган) се използва за издаването на електронно удостоверение, използвано от TSU (Time-stamping Unit/набор от хардуер и софтуер, който се управлява като едно цяло и има активен един подписващ ключ по време на удостоверителната услуга). Една или повече двойки ключове се използва за генерирането на удостоверения за време от TSU.

Всички частни ключове се съхраняват в FIPS 140-2 Level 3 хардуерен модул за сигурност.

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

Политика и практика на органа за удостоверяване на време „Evrotrust TSA“ се отнася към ETSI EN 319 401 относно общите изисквания, обичайни за всяка една услуга на Евротръст. Политиката е насочена към изпълнение на изискванията за удостоверяване на време с дълъг период на валидност (ETSI EN 319 122), но е приложима към всяка употреба с еквивалентни изисквания към качеството.

Генериращият алгоритъм, дължината на подписващия ключ и подписващия алгоритъм използван за подписване на удостоверенията за време е съобразно ETSI TS 119 312.

TSU удостоверението се издава от Базовия удостоверителен орган на Евротръст, отговарящ на ETSI EN 319 411-1.

Услугата по удостоверяване на време използва набор от Stratum -1 NTP (Network Time Protocol/протокол за синхронизиране на часовниците в компютърните системи) сървъри като независим източник на точно време. Посредством тази конфигурация TSS постига акуратност на времето в рамките на +/- 500ms(половин секунда) или по-добро спрямо UTC.

Evrotrust TSA гарантира интегритета и автентичността на TSU публичен ключ посредством TSU публични ключове, които са достъпни за доверяващите се страни в TSU удостоверенията на сайта на ЕВРОТРЪСТ на адрес: <https://www.evrotrust.com>

Удостоверенията за време се записват в регистър, който се публикува в хранилището на ЕВРОТРЪСТ на сайта в интернет.

Профилът на издаваното удостоверението за време е:

Поле	Атрибути	Значение/Стойност
Version		1
Policy		OID=1.3.6.1.4.1.47272.2.1 (съответства на политика с O.I.D.=0.4.0.2023.1.1)
Message Imprint	Hash Algorithm:	OID на хеша SHA-1, SHA-256
	Hash Value:	Хеш стойност на данните
Serial Number		Сериен номер на удостоверението
Generated Time		Времето на представяне на електронния подпис/печат (удостоверено време по UTC)
Accuracy		500ms
Ordering		Не се поддържа
Nonce		Само ако присъства в заявката
TSA		DN=[CN=Evrotrust TSA, OU=TSA, O=Evrotrust Technologies JSC, L=Sofia, S=Sofia, C=BG]
Extensions		не се използва

Връзка за достъп до Time stamp услугата: <http://ts.evrotrust.com/tsa> .

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

7 ПРОФИЛИ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ, CRL И НА OCSP

Профилът на базовия удостоверяващ орган Evrotrust RSA Root CA е:

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 Authority
	O=	Evrotrust Technologies JSC
	organizationIdentifier (2.5.4.97)=	NTRBG-203397356
	C=	BG
Valid from	20 май 2016 г. 15:39:19 UTC	
Validit to	20 май 2036 г. 15:49:19 UTC	
	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	

Профилът на органа за време „Evrotrust TSA“ е:

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	
Valid from	160521004013Z	
Validit to	210521005013Z	
Issuer	CN=	Evrotrust RSA Root CA
	OU=	Evrotrust Qualified Root Authority

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

Subject	O=	Evrotrust Technologies JSC
	OrganizationIdentifier(2.5.4.97)=	NTRBG-203397356
	C=	BG
	CN=	Evrotrust TSA
	OU=	Time Stamping Authority TSS/TSU
	O=	Evrotrust Technologies JSC
	OrganizationIdentifier(2.5.4.97)=	NTRBG-203397356
	C=	BG
Public Key	RSA(2048 Bits)	
Subject Key Identifier	03:BB:3B:42:27:8E:B8:80:90:1B:51:05:DF:52:C4:4B:0F:34:85:B9	
Key Usage (critical)	Digital Signature, Non Repudiation	
Extended keyUsage (critical)	Time Stamping (1.3.6.1.5.5.7.3.8)	
Certificate Policies	<p>[1]Certificate Policy:</p> <p>Policy Identifier=1.3.6.1.4.1.47272.1.2</p> <p>[1,1]Policy Qualifier Info:</p> <p>Policy Qualifier Id=CPS</p> <p>Qualifier:</p> <p>http://www.evrotrust.com/cps</p>	
Authority Key Identifier	74:5C:A1:40:73:2E:1F:E6:F9:3B:BC:AB:A0:A4:A7:54:44:74:4F:70	
Subject alternative name (not critical)	URL= http://www.evrotrust.com RFC822 Name=ca@evrotrust.com	
CRL Distribution Points	<p>[1]CRL Distribution Point</p> <p>Distribution Point Name:</p> <p>Full Name:</p> <p>URL=http://ca.evrotrust.com/crl/EvrotrustRSARootCA.crl</p>	
Authority Information Access	<p>[[1]Authority Info Access</p> <p>Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)</p> <p>Alternative Name:</p> <p>URL=http://ca.evrotrust.com/aia/EvrotrustRSARootCA.crt</p> <p>[2]Authority Info Access</p> <p>Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)</p> <p>Alternative Name:</p>	

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

	URL=http://ca.evrotrust.com/ocsp
Basic Constraints (critical)	Subject Type=End Entity Path Length Constraint=None

Профилът на валидиращия орган „Evrotrust RSA Validation“ е:

Version	V3
Serial number	38:00:00:00:02:46:4e:fc:a4:9d:94:68:e3:00:00:00:00:02
Signature Algorithm	SHA256RSA
Valid from	20160520154459Z
Valid to	20210521155459Z
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 Validation
	OU= OCSP Signing
	O= Evrotrust Technologies JSC
	OrganizationIdentifier(2.5.4.97)= NTRBG-203397356
	C= BG
Public Key	RSA(2048 Bits)
Subject Key Identifier	DA:40:9F:0A:F0:65:11:77:52:14:65:5F:AF:00:CA:D5:6E:D9:DC:2C
Key Usage (critical)	OCSP Signing
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
Application policies	[1]Application Certificate Policy: Policy Identifier=OCSP Signing

Профилът на валидиращия орган „Evrotrust RSA QS Validation“ е:

Version	V3
Serial number	2b:00:00:00:03:c3:3b:19:4b:08:91:37:24:00:00:00:00:03
Signature Algorithm	SHA256RSA

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

Valid from	20160521014614Z	
Valid to	20210520014614Z	
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 QS Validation
	OU=	OCSP QS Signer
	O=	Evrotrust Technologies JSC
	OrganizationIdentifier(2.5.4.97)=	NTRBG-203397356
	C=	BG
Public Key	RSA(2048 Bits)	
Subject Key Identifier	17:A2:1D:16:B0:BF:89:1F:A2:C5:86:BF:CB:DF:77:9F:35:76:7B:66	
Key Usage (critical)	OCSP Signing	
Extended Key Usage	OCSP Signing (1.3.6.1.5.5.7.3.9)	
Authority Key Identifier	7F:3E:64:59:85:2B:DD:23:29:C2:01:E7:CB:C3:69:C0:87:93:2B:08	
OCSP No Revocation Checking	NULL	
Application policies	[1]Application Certificate Policy: Policy Identifier=OCSP Signing	

Профилите на потребителските квалифицирани удостоверения и на Списъка със спрени и прекратени удостоверения (CRL) отговарят на формата, описан в стандарт ITU-T X.509 v.3. Удостоверение от тип X.509 v.3 представлява набор от данни, чрез който еднозначно се удостоверява принадлежност на публичния ключ към автора на квалифицирания електронен подпис/печат. Профила на OCSP отговаря на изискванията на RFC 2560, а профилът на квалифицираното удостоверение за времеви печат отговаря на RFC 3161.

7.1 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;

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

- Issuer: наименование на издателя 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 (notBefore) 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.

7.1.1 ВЕРСИЯ

Всички удостоверения, които издава ЕВРОТРЪСТ, са в съответствие с версия 3 (X.509 v.3).

7.1.2 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

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

създаване на електронен подпис (QSCD).

7.1.3 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.

7.1.4 ФОРМИ НА ИМЕНУВАНЕ

Формите на именуване са описани в частта „Видове имена“ на този документ.

7.1.5 ОГРАНИЧЕНИЯ НА ИМЕНАТА

Видовете ограничения на имената са описани в частта „Видове имена“ на този документ.

7.1.6 ИДЕНТИФИКАТОР НА ПОЛИТИКА

Квалифицирано удостоверение се издават съгласно Политика на ЕВРОТРЪСТ, която се вписва в атрибута „Certificate Policy“ на удостоверението.

7.1.7 ИДЕНТИФИКАТОР ЗА ПРОДЪЛЖЕНИЕ

Този идентификатор („Extensions“) дава специфична, свързана с услугата информация. За употребата му на този етап Практиката не поставя никакви ограничения.

7.1.8 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:

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

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 удостоверение за атрибутивен 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 печат на юридическо лице/организация	Evrotrust Qualified Legal Person Certificate for QESeal	OID=1.3.6.1.4.1.47272.2.3
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 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
Други идентификатори (OID), вписани в атрибута "Certificate Policy" в квалифицираните удостоверения		
Удостоверителна политика за квалифицирани удостоверения, издадена за публични услуги, която изисква използване на secure signature-creation device (SSCD)	qcp-public-with-sscd	OID=0.4.0.1456.1.1
Удостоверителна политика за	qcp-public	OID=0.4.0.1456.1.2

квалифицирани удостоверения, издадена за публични услуги		
QCP-n: Удостоверителна политика на Европейския съюз (ЕС) за Квалифицирани удостоверения, издавани на физически лица	qcp-natural	OID=0.4.0.194112.1.0
QCP-l: 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 съюз (ЕС) за удостоверения за автентичност на уебсайт	qcp-web	OID=0.4.0.194112.1.4
DVCP (Domain Validated Certificate Policy) според ETSI TS 102 042	dvcp	OID=0.4.0.2042.1.6
OVCP (Organizational Validation Certificate Policy) според ETSI TS	ovcp	OID=0.4.0.2042.1.7

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

102 042		
---------	--	--

7.1.9 ИЗПОЛЗВАНЕ НА ИДЕНТИФИКАТОР ЗА РАЗШИРЕНИЕ НА КЛЮЧА „КРИТИЧНО“

В Практиката няма изисквания за използване на „CRITICAL CERTIFICATE EXTENSIONS“.

7.2 ПРОФИЛ НА СПИСЪКА СЪС СПРЕНИ И ПРЕКЪСНАТИ УДОСТОВЕРЕНИЕ (CRL)

CRL профилът на базовия удостоверяващ орган Evrotrust RSA Root CA е:

Version	V2	
Issuer	CN=	Evrotrust RSA Root CA
	OU=	Evrotrust Qualified Root Authority
	O=	Evrotrust Technologies JSC
	organizationIdentifier (2.5.4.97)=	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]	
Next CRL Publish	[дата и час по UTC на планирано публикуване на следващ CRL]	

CRL профилът на оперативния удостоверяващ орган Evrotrust RSA operational CA е:

Version	V2	
Issuer	CN=	Evrotrust RSA Operational CA
	OU=	Qualified Operational CA
	O=	Evrotrust Technologies JSC
	organizationIdentifier (2.5.4.97)=	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	SHA256	

algorithm	
Authority Identifier	Key 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]
Next CRL Publish	[дата и час по UTC на планирано публикуване на следващ CRL]

7.2.1 ВЕРСИЯ

ЕВРОТРЪСТ, чрез своя Удостоверяващ орган издава, публикува и поддържа Списъци със спрени и прекратени удостоверения (CRL) във формата X.509 v.2. Версията се вписва в издадения CRL.

7.2.2 ФОРМАТ

ЕВРОТРЪСТ издава, публикува и поддържа Списък със спрени и прекратени удостоверения (CRL), чийто формат е в съответствие с изискванията в международната препоръка RFC 5280.

Удостоверяващият орган на ЕВРОТРЪСТ издава, публикува и поддържа самостоятелни пълни Списъци (CRL-и) като в тях записват само спрени удостоверения, които са издадени от съответния Удостоверяващ орган.

ЕВРОТРЪСТ не издава и не поддържа схема на „частичен“ (delta) Списък със спрени и прекратени удостоверения (CRL), но запазва право при необходимост да въведе такава схема.

7.2.3 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.

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

7.2.4 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.

7.2.5 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.

7.2.5.1 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.

7.2.5.2 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.

7.3 ПРОФИЛ НА ОТГОВОР ЗА ОНЛАЙН ПРОВЕРКА НА СТАТУСА НА УДОСТОВЕРЕНИЕ (OCSP/ONLINE CERTIFICATE STATUS PROTOCOL)

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

Удостоверяващите органи за валидация „Evrotrust RSA Validation“ на базовия удостоверяващ орган „Evrotrust RSA Root CA“ и „Evrotrust RSA QS Validation“ на оперативния удостоверяващ орган „Evrotrust RSA Operational 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.

7.3.1 ВЕРСИЯ

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.

7.3.2 ФОРМАТ

ЕВРОТРЪСТ издава удостоверения за статус, чийто формат е в съответствие с изискванията в международната препоръка RFC 6960.

7.3.3 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 настоящето 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;

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

- 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	<ul style="list-style-type: none"> • successful (0) - Валиден отговор на запитването; • malformedRequest (1) - Запитването на 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	Basic OCSP Response
Version	1 (0x0)
Responder Id	[Уникален идентификатор на инстанцията 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	<ul style="list-style-type: none"> • 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

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

Certificate:	[Квалифицираното удостоверение на органа за валидация]
--------------	--

7.4 ДРУГИ ПРОФИЛИ

7.4.1 ПРОФИЛ НА КВАЛИФИЦИРАН ЕЛЕКТРОНЕН ВРЕМЕВИ ПЕЧАТ

Удостоверяващият орган за квалифицирани електронни времеви печати „Evrotrust TSA“ издава квалифицирани електронни времеви печати (Timestamp Tokens/TST) с един или повече частни ключове запазени единствено за тази цел. Според препоръка RFC 3280 удостоверенията за квалифицирани електронни времеви печати в техните разширения на атрибути, съдържат поле за ограничаване на употребата им (Extended Key Usage), маркирани като критични. Това означава, че удостоверението може да се използва от „Evrotrust TSA“ единствено за целите на подписването на квалифицираните електронни времеви печати, издадени от този орган.

7.5 ОСНОВНИ ПОЛЕТА В ПРОФИЛА НА КВАЛИФИЦИРАНИ ЕЛЕКТРОННИ ВРЕМЕВИ ПЕЧАТИ:

- Version – версия (Version 3);
- Serial Number – уникален идентификационен код на времевия печат;
- Signature Algorithm – алгоритъм за създаване на електронния подпис (sha1WithRSAEncryption)
- Issuer (Distinguished Name) – наименование на издателя на времевия печат (Evrotrust TSA);
- Not before (validity period/beginning date) – дата и час на издаване (универсално координирано време, представено в Zulu);
- Not after (validity period ending/date) – дата и час на изтичане на срока на валидност;
- Subject (Distinguished Name) – наименование на Титуляря/Създателя;
- Subject Public Key Info - Кодирана поле в съответствие с RFC 3280, което съдържа информация за RSA публичния ключ (ключов идентификатор и стойност на публичния ключ);
- Signature - електронен подпис, генериран и кодиран в съответствие с изисквания, описани в RFC 3280;
- Basic Constraints – основни ограничения на времевия печат;
- Key Usage – предназначение на времевия печат;
- Extended Key Usage - Time Stamping Authority (TSA);
- Certificate Policies – политика, въз основа на която е издаден времевия печат;
- Authority Key Identifier – идентификатор на ключа на Удостоверяващия орган (SHA1 hash of the public key).

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

Удостоверяващият орган „Evrotrust TSA“ приема заявки за удостоверяване на време, които да отговарят на спецификациите IETF RFC 3161 и ETSI EN 319 422:

- Заявката за квалифициран електронен времеви печат трябва да съдържа алгоритъма на хеш функция SHA256;
- Заявката за квалифициран електронен времеви печат указва идентификатора на политиката на Evrotrust TSA Policy OID.

Квалифицираният електронен времеви печат, издаден от „Evrotrust TSA“ съдържа информация за печата (TSTinfo структура), разположен в SignedData структура (виж RFC 2630), подписан от Evrotrust TSA и вградени в ContentInfo структура (виж RFC 2630).

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 стандарта IEC 27001:2013, 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.

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

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 упълномощени 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 регламентираните изисквания към дейността на ЕВРОТРЪСТЕВРОТРЪСТ 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.

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

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.

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

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.

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

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.

Неполучаването 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

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

Титуляр/Създател може да възрази относно неточност или непълнота в съдържанието на издадено удостоверение в 3-дневен срок след публикуването му в Публичния регистър.

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 Публичния регистър/хранилището, 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 удостоверенията.

ЕВРОТРЪСТЕВРОТРЪСТ 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 обезвредата. Максималната граница на плащане не може надвишава размера на вредите.

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

9.2.1 ЗАСТРАХОВКА НА ДЕЙНОСТТА

ЕВРОТРЪСТ сключва задължителна застраховка на дейността си като доставчик на квалифицирани удостоверителни услуги.

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 националното законодателство.

Задължителната застраховка покрива отговорността на ЕВРОТРЪСТ към Титуляри/Създатели, съответно Доверяващи се страни за причинени имуществени и неимуществени вреди до границите определени в националното 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.

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 обществено достъпна в Публичния регистър/хранилището.

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

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 неправилен достъп и въздействие.

9.3.2 НЕКОНФИДЕНЦИАЛНА ИНФОРМАЦИЯ

Неконфиденциална е всяка информация, съдържаща се в Публичния регистър/хранилището 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 хранилището 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 (възможно най-подробно).

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

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

ЕВРОТРЪСТ е регистриран като администратор на лични данни по реда на Закона за защита на лични данни.

В качеството си на Администратор на лични данни, Доставчикът 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.

9.4.1 ДЕКЛАРАЦИЯ ЗА ПОВЕРИТЕЛНОСТ

Личните данни, предоставени на ЕВРОТРЪСТ се съхраняват и обработват в съответствие със Закона за защита на личните данни. 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, хранилището или онлайн чрез Списъка със спрени и прекратени

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

удостоверения (CRL) 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.

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.

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 Публичния регистър/хранилище 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.

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

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

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

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 споразумения. 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 и приложимото законодателство в Република България.

9.6.1 ЗАДЪЛЖЕНИЯ, ОТГОВОРНОСТ И ГАРАНЦИИ НА ЕВРОТРЪСТ

ЕВРОТРЪСТ гарантира, че осъществява дейността си като:

- спазва точно условията в настоящия документ, изискванията на Регламент (ЕС) № 910/2014 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, ако има такава;

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

- 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 дължимата 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 Публичен регистър/хранилище, в който публикува издадените квалифицирани удостоверения, актуален Списък със спрени и прекратени удостоверения (CRL), други обстоятелства и електронни документи, съгласно този документ и националното законодателство;
- осигурява постоянен достъп до Публичния регистър по електронен път (24/7);
- осигурява защита срещу внасяне на промени в поддържания Публичен регистър от

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

нерегламентиран и неправиномерен достъп или поради случайно събитие;

- публикува незабавно в Публичния регистър издадените и подписани удостоверения;
- създава условия на всяка доверяваща се страна да провери статуса на издадено и публикувано удостоверение в публичния Регистър на удостоверения;
- 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;

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.

9.6.2 ЗАДЪЛЖЕНИЯ, ОТГОВОРНОСТ И ГАРАНЦИИ НА РЕГИСТРИРАЩИЯ ОРГАН

ЕВРОТРЪСТ гарантира, че Регистриращия 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 Регистриращия орган в инфраструктурата на

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

ЕВРОТРЪСТ.

ЕВРОТРЪСТ гарантира, че Регистриращия 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 .

Всеки Регистриращ 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 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

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

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 в Публичния регистър 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 компрометиране 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;

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

- да не прави достъпен своя частен ключ за други лица.

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 употребата на квалифицирано удостоверение за електронен подпис/печат.

Доверяващата се страна следва да положи дължимата 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 Публичен регистър/хранилище. Проверката на електронната автентичност и на интегритета на удостоверението извън Публичния регистър 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 трансакции, 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.

Дължимата 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;

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

- при необходимост може да се установи съдържанието на подписания електронен документ;
- автентичността и валидността на удостоверението към 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.

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;

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

➤ 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 КВАЛИФИЦИРАНИЯ ОРГАН ЗА ВАЛИДИРАНЕ

Квалифицираният орган за валидиране („Evrotrust RSA QS Validation“) на ЕВРОТРЪСТ осъществява 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 уеб сайтове.

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 уеб сайтове, използвани в съответствие с изискванията на Регламент (ЕС) № 910/2014;

➤ „Evrotrust RSA QS Validation“ проверява състоянието на удостоверенията в съответствие

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

c RFC 2560 Online Certificate Status Protocol (OCSP) recommendation.

9.6.5.3 ЗАДЪЛЖЕНИЯ НА КВАЛИФИЦИРАНИЯ ОРГАН ЗА КВАЛИФИЦИРАНА УСЛУГА ЗА ЕЛЕКТРОННА ПРЕПОРЪЧАНА ПОЩА

Квалифицираният орган за квалифицирана услуга за електронна препоръчана поща „Evrotrust Qualified ERDS“ (Electronic registered delivery service) на ЕВРОТРЪСТ, осъществява функциите си в съответствие с изискванията, определени в Регламент (ЕС) № 910/2014 и политиките и практиките за удостоверяване на сигурно връчване на съобщения, чрез препоръчана електронна поща.

ЕВРОТРЪСТ гарантира, че:

- използва оперативни процедури и такива за управление на сигурността, които изключват възможността за подмяна на данните, доказващи моментите на изпращане и получаване на поща, изпращача и получателя, както и контролните суми за установяване съдържанието на изпращаните съобщения;
- използва параметри на криптографски алгоритми в съответствие с изискванията, определени в Регламент (ЕС) № 910/2014;
- издава квалифицирано удостоверение за получаване на електронна препоръчана поща, включително официални доказателства за получаване на съобщения, само след проверка на автентичността на данните от получените електронни документи, тяхната формална коректност и само след като ЕВРОТРЪСТ ги е доставил в надеждно място, от което те ще бъдат достъпни за получателя;
- доказателствата, издадени от ЕВРОТРЪСТ отговарят на изискванията на ISO/IEC 13888-3:1999 Information technology -- Security techniques -- Non-repudiation -- Part 3: Mechanisms using asymmetric techniques;
- ЕВРОТРЪСТ осигурява при поискване възможност на третите страни да проверят и тества издаваните от него удостоверения и удостоверителни услуги, като осигурява тестови удостоверения, например във формат PKCS#12 на своя сайт и достъп до тестови услуги. В тестовите удостоверения ясно е посочено, че те са издадени за тестови цели.

9.6.5.4 ЗАДЪЛЖЕНИЯ НА КВАЛИФИЦИРАНИЯ ОПЕРАТИВЕН УДОСТОВЕРЯВАЩ ОРГАН ЗА КВАЛИФИЦИРАНИ ЕЛЕКТРОННИ ПОДПИСИ/ПЕЧАТИ

Задълженията на Квалифицирания оперативен удостоверяващ орган за квалифицирани електронни подписи/печати на ЕВРОТРЪСТ „Evrotrust RSA Operational CA“, осъществява функциите си в съответствие с изисквания, определени в Регламент (ЕС) № 910/2014 за

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

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.

9.6.5.5 ЗАДЪЛЖЕНИЯ НА ЕВРОТРЪСТ ПО ОТНОШЕНИЕ НА ПУБЛИЧНИТЕ РЕГИСТРИ / ХРАНИЛИЩЕТО

Публичните регистри 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 оперативен удостоверяващ орган за електронен подпис/печат „Evrotrust RSA Operational CA“, Квалифицирания удостоверяващ орган за време (Evrotrust TSA), Квалифицирания удостоверяващ орган за проверка статуса на удостоверенията „Evrotrust RSA QS Validation“;

- 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 с дейността му;

- осигурява достъп до квалифицирани удостоверения, само в случаи, когато те са публично достъпни и доколкото потребителят не е изразил несъгласие, а когато удостоверението съдържа личен идентификатор – с неговото изрично съгласие;

- 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 в публичния регистър 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. Освобождането от отговорност следва да се определи в договорите между потребителите и ЕВРОТРЪСТ.

ЕВРОТРЪСТ не носи отговорност в случаите, когато настъпилите вреди са следствие от

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

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.

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

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 в Публичния му регистър/хранилището на ЕВРОТРЪСТ. Допълнения към този документ влизат в сила след публикуването им в хранилището.

Разпоредбите в настоящия документ са валидни до издаване и публикуване на следваща версия на „Практика при предоставяне на квалифицирани удостоверителни услуги“ в хранилището на сайта на ЕВРОТРЪСТ.

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

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 остатъка 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 Удоверяващите 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 КВАЛИФИЦИРАНИ 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.

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

9.13 РЕШАВАНЕ НА СПОРОВЕ

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. Исканията трябва да бъдат направени в писмен вид на адреса на ЕВРОТРЪСТ:

“Евротръст Технолъджис” АД
София, бул. Цариградско шосе 101
Бизнес център "АКТИВ", ет. 6
Телефон, факс: + 359 2 448 58 58

Жалбите ще бъдат разгледани от правния отдел на ЕВРОТРЪСТ. Жалбоподателят ще получи отговор в рамките на 2 работни дни след получаване на жалбата. В случай, че не се намери решение на спора в рамките на 30 дни от началото на процедурата по споразумение, същият се отнася за разрешаване по съдебен ред.

9.14 ПРИЛОЖИМО ПРАВО

За всички въпроси, неуредени в настоящия документ се прилагат разпоредбите на българското законодателство.

9.15 СЪОТВЕТСТВИЕ С ПРИЛОЖИМОТО ПРАВО

Настоящият документ е разработен в съответствие с националното законодателство.

9.16 ДРУГИ РАЗПОРЕДБИ

Практиката не посочва никакви други разпоредби.

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

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 на електронен подпис	Данни за създаване на електронен подпис са уникални данни, които се използват от Титуляря на електронния подпис за 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 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,

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

	като софтуерен код или сървъри
Електронен подпис	Данни в електронна форма, които се добавят към други данни 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
ЗУУ	Звено за удостоверителни услуги
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 е подпечатан с усъвършенстван електронен печат на доставчик на квалифицирани удостоверителни услуги или с друг равностоен 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
Квалифицирана услуга за електронна препоръчана поща	Квалифицирана услуга за електронна препоръчана поща е услуга за електронна препоръчана поща, която се предоставя от доставчик на квалифицирани удостоверителни услуги.
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

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

КРС	Комисия за регулиране на съобщенията
МОЛ	Материално отговорно лице
ПИН	Персонален идентификационен номер
Практика	Практика при предоставяне на удостоверителни услуги е документ, съдържащ правила относно издаване, спиране, възобновяване и отмяна действието на удостоверенията, условията за предоставянето на достъп до удостоверенията
Политика	Политика за предоставяне на удостоверителни услуги е документ, описващ 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.
Регламент	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
Схема за електронна идентификация	Схема за електронна идентификация е система, при която средства за електронна идентификация се издават на физически или юридически лица, или физически лица, представляващи юридически лица
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

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

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 подпис	Удостоверение за електронен подпис е електронен атестат, който свързва данните за валидиране на електронен 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 Доставчик на удостоверителни услуги, които се състоят в: 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 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 уеб сайт	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
Услуга за електронна препоръчана поща	Услуга за електронна препоръчана поща е услуга, която позволява предаването на данни между трети страни по електронен път, предоставя доказателство във връзка с обработката на предаваните данни, включително доказателство за изпращането и получаването на данните, и защитава предаваните данни срещу риск от загуба, кражба, повреда или неправомерни изменения
Устройство за създаване на	Устройство за създаване на електронен печат е конфигуриран софтуер или хардуер, който се използва за създаването на електронен печат

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

електронен печат	
Устройство за създаване на квалифициран електронен печат	Устройство за 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: -е свързан по уникален начин с Титуляря; може да идентифицира Титуляря на подписа; -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 -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

	ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ	eIDAS-CPS For public use
Regulation 910 / 2014 eIDAS	CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES	Version – 2.2 23.06.2017

10.2 ПРИЛОЖЕНИЕ 2: ТЕРМИНИ И СЪКРАЩЕНИЯ НА АНГЛИЙСКИ ЕЗИК

ASN.1 Abstract Syntax Notation One	Абстрактен език за описание на обекти в удостоверенията
A Actuality	Актуалност
BG Bulgaria	България
C Country	Страна
CA Certification Authority	Удостоверяващ орган
CC Common Criteria	Общи критерии
CN Common Name	Публично име
CP Certificate Policy	Политика за предоставяне на удостоверителни услуги
CSP Cryptograph Services Provider	Криптографски модул към четящо устройство и смарт карта
CPS Certification Practice Statement	Практика при предоставяне на удостоверителни 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 удостоверението
E E-mail	Електронна поща
e-ID	Електронна идентификация
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
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

OCSF, 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)
JSC, Joint Stock Company	Акционерно дружество
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
SMIME, Secure Multipurpose Internet Mail Extensions	Протокол за сигурно предаване на електронна поща през интернет
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

Регистриране на измененията															
Страница															
Валидно изменение															