ISO/IEC 27001:2022
ISO/IEC 27701:2019
ISO 20000-1:2018
ISO 22301:2019 ISO 9001:2015
Регламент (ЕС) 910/2014
Регламент (ЕС) 2016/679

ПОЛИТИКА И ПРАКТИКА НА УСЛУГА ЗА ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ ЕЛЕКТРОННИ ВРЕМЕВИ ПЕЧАТИ

СЪДЪРЖАНИЕ

1 ВЪВЕДЕНИЕ 4
1.1 ИЗИСКВАНИЯ КЪМ КВАЛИФИЦИРАНИТЕ ЕЛЕКТРОННИ ВРЕМЕВИ ПЕЧАТИ 4
1.2 ОБХВАТ 6
2 НОРМАТИВНИ ПОЗОВАВАНИЯ 6
3 ОПРЕДЕЛЕНИЯ И СЪКРАЩЕНИЯ 7
3.1 ОПРЕДЕЛЕНИЯ 7
3.2 СЪКРАЩЕНИЯ 8
4 ОБЩИ ПОНЯТИЯ 9
4.1 КВАЛИФИЦИРАНА УСЛУГА ЗА УДОСТОВЕРЯВАНЕ НА ВРЕМЕ (TIMESTAMPING SERVICE/TSS) 9
4.2 УДОСТОВЕРЯВАЩ ОРГАН ЗА ИЗДАВАНЕ НА КВАЛИФИЦИРАНИ ЕЛЕКТРОННИ ВРЕМЕВИ ПЕЧАТИ („EVROTRUST TSA“) 10
4.3 ПОТРЕБИТЕЛИ 11
4.4 ОБЩИ РАЗПОРЕДБИ НА „ПОЛИТИКА И ПРАКТИКА НА УСЛУГА ЗА ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ ЕЛЕКТРОННИ ВРЕМЕВИ ПЕЧАТИ“ 12
4.4.1 ПРЕДНАЗНАЧЕНИЕ 12
4.4.2 СПЕЦИФИКА НА ПОЛИТИКАТА И ПРАКТИКАТА 12
4.4.3 ПОДХОД 13
5 ПОЛИТИКА НА ОРГАНА ЗА УДОСТОВЕРЯВАНЕ НА ВРЕМЕ 13
5.1 ОБЩИ ПОЛОЖЕНИЯ 13
5.2 ПРОФИЛ НА УДОСТОВЕРЕНИЕТО, С КОЕТО СЕ ПОДПИСВА КВАЛИФИЦИРАНИЯ ЕЛЕКТРОНЕН ВРЕМЕВИ ПЕЧАТ 14
5.3 ЗАЯВКА ЗА ИЗДАВАНЕ НА ТОКЪН ЗА ЕЛЕКТРОНЕН ВРЕМЕВИ ПЕЧАТ (TIME STAMP QUERY/TSQ) 16
5.4 ТОКЪН ЗА ЕЛЕКТРОНЕН ВРЕМЕВИ ПЕЧАТ (TIMESTAMPING TOKEN/TST) 17
5.5 УДОСТОВЕРЯВАНЕ НА ВРЕМЕ (TIMESTAMPING) 19
5.6 ИДЕНТИФИКАТОР НА ПОЛИТИКАТА НА ОРГАНА ЗА УДОСТОВЕРЯВАНЕ НА ВРЕМЕ 19
5.7 ПРИЛОЖИМОСТ НА ЕЛЕКТРОНЕН ВРЕМЕВИ ПЕЧАТ 19
5.8 СЪОТВЕТСТВИЕ 20
6 ЗАДЪЛЖЕНИЯ, ГАРАНЦИИ И ОТГОВОРНОСТИ 20
6.1 ЗАДЪЛЖЕНИЯ 20
6.1.1 ОБЩИ ЗАДЪЛЖЕНИЯ 20
6.1.2 ЗАДЪЛЖЕНИЯ НА ЕВРОТРЪСТ 20
6.1.3 ЗАДЪЛЖЕНИЯ НА КВАЛИФИЦИРАНИЯ ОРГАН ЗА УДОСТОВЕРЯВАНЕ НА ВРЕМЕ 20
6.1.4 ЗАДЪЛЖЕНИЯ НА ПОТРЕБИТЕЛИ 22
6.1.5 ЗАДЪЛЖЕНИЯ НА ДОВЕРЯВАЩИ СЕ СТРАНИ 22
6.2 ГАРАНЦИИ НА ЕВРОТРЪСТ 23
6.3 ОТГОВОРНОСТИ 23
7 УПРАВЛЕНИЕ И КОНТРОЛ НА ТЕХНИЧЕСКАТА СИГУРНОСТ НА ОРГАНА ЗА УДОСТОВЕРЯВАНЕ НА ВРЕМЕ 24
7.1 ОБЩИ ИЗИСКВАНИЯ КЪМ ОРГАНА ЗА УДОСТОВЕРЯВАНЕ НА ВРЕМЕ 24
7.2 ВЪТРЕШНА ОРГАНИЗАЦИЯ 24
7.2.1 ДОСТЪПНОСТ НА УСЛУГАТА 25
7.3 УПРАВЛЕНИЕ НА ЖИЗНЕНИЯ ЦИКЪЛ НА ДВОЙКАТА КЛЮЧОВЕ НА TSU 25
7.3.1 ГЕНЕРИРАНЕ НА ДВОЙКА КЛЮЧОВЕ НА TSU 25

7.3.2 ЗАЩИТА НА ЧАСТНИЯ КЛЮЧ НА TSU 26
7.3.3 РАЗПРОСТРАНЕНИЕ НА ПУБЛИЧНИЯ КЛЮЧ НА TSU 26
7.3.4 ПРОДЪЛЖАВАНЕ НА СРОКА И/ИЛИ ПРЕИЗДАВАНЕ НА ЧАСТНИЯ КЛЮЧ НА TSU 27
7.3.5 УНИЩОЖЕНИЕ НА ЧАСТНИЯ КЛЮЧ НА TSU 27
7.3.6 УПРАВЛЕНИЕ НА ЖИЗНЕНИЯ ЦИКЪЛ НА ПОДПИСВАЩОТО КРИПТОГРАФСКО ОБОРУДВАНЕ 28
7.3.7 СИНХРОНИЗАЦИЯ НА ЧАСОВНИКА С КООРДИНИРАНОТО УНИВЕРСАЛНО ВРЕМЕ 29
7.4 УПРАВЛЕНИЕ И ДЕЙНОСТ НА ОРГАНА ЗА УДОСТОВЕРЯВАНЕ НА ВРЕМЕ 29
7.4.1 УПРАВЛЕНИЕ НА СИГУРНОСТТА 29
7.4.2 ОЦЕНКА НА РИСКА 29
7.4.3 ОПЕРАТИВНА СИГУРНОСТ 30
7.4.4 ФИЗИЧЕСКА СИГУРНОСТ 30
7.4.5 МРЕЖОВА СИГУРНОСТ 31
7.4.6 УПРАВЛЕНИЕ НА ДЕЙНОСТТА 32
7.4.7 УПРАВЛЕНИЕ НА ДОСТЪПА ДО СИСТЕМА 32
7.4.8 СИГУРНА СРЕДА 33
7.4.9 КОМПРОМЕТИРАНЕ НА ЧАСТНИЯ КЛЮЧ НА TSU 33
7.4.10 ПРЕКРАТЯВАНЕ НА ДЕЙНОСТТА НА ОРГАНА ЗА УДОСТОВЕРЯВАНЕ НА ВРЕМЕ 34
7.4.11 СПАЗВАНЕ НА ПРАВНИ ИЗИСКВАНИЯ 35
7.4.12 ЗАПИС НА ДОКАЗАТЕЛСТВА 35
7.5 ОРГАНИЗАЦИОННА СХЕМА 36

1 ВЪВЕДЕНИЕ

Този документ представлява „Политика и Практика на услуга за предоставяне на квалифицирани електронни времеви печати" на Доставчик на квалифицирани удостоверителни услуги „Евротръст Технолъджис" АД (Евротръст).

Настоящият документ определя общите правила, използвани от Органа за удостоверяване на време („Evrotrust TSA") за издаване на квалифицирани електронни времеви печати.

В „Политика и Практика на услуга за предоставяне на квалифицирани електронни времеви печати" се определят участниците в процеса на издаване и поддържане на потребителски квалифицирани електронни времеви печати, като се посочват техните отговорности, права и задължения. Определя се приложимият диапазон на действие на електронните времеви печати. Квалифицираният електронен времеви печат, издаден от Евротръст, се признава за такъв във всички държави-членки на Европейския съюз. 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.

Структурата и съдържанието на настоящата „Политика и Практика на услуга за предоставяне на квалифицирани електронни времеви печати" е изготвена в съответствие с техническата спецификация RFC 3161, ETSI EN 319 401 и EN 319 421. Документът е публично достъпен на адрес в интернет: https://www.evrotrust.com.

1.1 ИЗИСКВАНИЯ КЪМ КВАЛИФИЦИРАНИТЕ ЕЛЕКТРОННИ ВРЕМЕВИ ПЕЧАТИ

Евротръст издава квалифицирани електронни времеви печати в съответствие с изискванията на чл. 42 на Регламент (ЕС) № 910/2014 г.:

- обвързва датата и часа с данните по начин, който до голяма степен изключва възможността за незабелязана промяна на данните;
- основава се на източник на точно време, свързан с координираното универсално време (UTC);
- подписан е с усъвършенстван електронен подпис или е подпечатан с усъвършенстван електронен печат на доставчик на квалифицирани удостоверителни услуги или с друг равностоен метод.

Евротръст изпълнява следните допълнителни изисквания за квалифицирани

електронни времеви печати съгласно Регламент (ЕС) № 910/2014, относно TSU удостоверението за публичен ключ:

Удостоверението за публичен ключ на TSU е издадено от удостоверяващ орган, в съответствие с политика определена в ETSI EN 319 411-2. ETSI EN 319 411-2 включва изисквания от ETSI EN 319 411-1. Доверяващите се страни използват доверителен списък, за да установят дали времевият печат е квалифициран. Ако публичният ключ на TSU е включен в списъка и услугата, която той представлява е квалифицирана услуга, тогава времевите печати, издадени от TSU, могат да се считат за квалифицирани. QcStatement "esi4-qtstStatement-1", както е дефинирано в точка 9.1 на ETSI EN 319 422.

При предоставяне на квалифицирани електронни времеви печати, Евротръст отговаря на изискванията, предвидени в Регламент (ЕС) № 910/2014 и в член 21 от Директива (ЕС) 2022/2555. Целта на дружеството е да защити мрежовите и информационните системи, и физическата среда на тези системи от инциденти, като мерките включват поне следното:

а) политики за анализ на риска и сигурност на информационните системи;

б) действия при инцидент;

в) непрекъснатост на стопанската дейност, например управление на съхраняването на резервни копия на данните и възстановяване след бедствия, и управление на кризи;

г) сигурност на веригата за доставка, включително свързани със сигурността аспекти относно взаимовръзките между всеки субект и неговите преки снабдители или доставчици на услуги;

д) сигурност при придобиването на мрежови и информационни системи, разработване и поддръжка, включително предприемане на действия при уязвимости и оповестяването им;

е) политики и процедури за оценяване на ефективността на мерките за управление на риска в областта на киберсигурността;

ж) основни киберхигиенни практики и обучение в областта на киберсигурността;

з) политики и процедури относно използването на криптография и, когато е целесъобразно, криптиране;

и) сигурност на човешките ресурси, политики за контрол на достъпа и управление

на активи;

й) използването на многофакторни решения за удостоверяване на автентичността или непрекъснато удостоверяване на автентичността, защитени гласови, видео и текстови съобщения и защитени системи за спешна комуникация в рамките на субекта, когато е целесъобразно.

1.2 ОБХВАТ

Настоящият документ е публично достъпен на сайта на Евротръст и може да се използва от доверяващи се страни и потребители на квалифицирани удостоверителни услуги.

Предоставянето на услуга за издаване на времеви печати включва генериране на времеви печати и управление (следене и контролиране) на процеса по генериране на времеви печати, за да се гарантира, че се предоставя услуга, определена от „Evrotrust TSA". „Evrotrust TSA" носи отговорност за инсталирането и деинсталиране на услугата за предоставяне на времеви печати. „Evrotrust TSA" гарантира, че часовникът, използван за отпечатване на времето, е правилно синхронизиран с UTC.

2 НОРМАТИВНИ ПОЗОВАВАНИЯ

В настоящия документ се съдържат препратки към стандарти и стандартизационни документи, процедури, директиви, национално и европейско законодателство:

- 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 (ЕС) № 910/2014);
- Регламент (ЕС) 2024/1183 на Европейския парламент и на Съвета от 11 април 2024 година за изменение на Регламент (ЕС) № 910/2014 по отношение на създаването на европейска рамка за цифрова самоличност;
- Recommendation ITU-R TF.460-6 Standard-frequency and time-signal emissions;
- ISO/IEC 19790 Information technology -- Security techniques -- Security requirements for cryptographic modules;

- ISO/IEC 15408 (parts 1 to 3) Information technology -- Security techniques -- Evaluation criteria for IT security;
- ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers;
- ETSI EN 319 421 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Timestamps;
- ETSI EN 319 422 Electronic Signatures and Infrastructures (ESI); Timestamping protocol and Timestamp token profiles;
- ETSI TR 119 460 Electronic Signatures and Infrastructures (ESI); Survey of technologies and regulatory requirements for identity proofing for trust service subjects;
- ETSI TS 119 461 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects;
- FIPS PUB 140-2 Security Requirements for Cryptographic Modules;
- IETF RFC 3161 Internet X.509 Public Key Infrastructure: Timestamp Protocol (TSP).

3 ОПРЕДЕЛЕНИЯ И СЪКРАЩЕНИЯ

3.1 ОПРЕДЕЛЕНИЯ

Coordinated Universal Time (UTC) - Координирано универсално време, отчетено в съответствие с Recommendation ITU-R TF.460-6;

Network Time Protocol (NTP) - мрежов протокол, който се използва от програми за синхронизация на времето на една или мрежа от много информационни системи;

Доверяваща се страна (Relying Party) - физическо или юридическо лице, което приема електронен времеви печат и се доверява на удостоверените в него факти;

Потребител - физическо или юридическо лице, на което е предоставена услугата за издаване на квалифициран електронен времеви печат;

Електронен времеви печат (Time stamp) - 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;

Квалифициран електронен времеви печат (Qualified Time Stamp) - електронен времеви печат, който отговаря на изискванията на Регламент (ЕС) № 910/2014;

Орган за удостоверяване на време (Evrotrust TSA) – това е юридическото лице Евротръст, в качеството си на квалифициран доставчик на удостоверителни услуги, който предоставя услуга за издаване на квалифицирани електронни времеви печати и може да има един или няколко TSU;

Квалифицирана услуга за удостоверяване на време (Quaified Timestamping Service/TSS) – услуга за удостоверяване на датата и часа на предоставяне на електронен документ;

Профил на токън за електронен времеви печат (Timestamp token profiles/TST) - Информационен обект определен в препоръка IETF RFC 3161 (профил на електронно подписано удостоверение (отговор) от TSU за съществуване на цифрово съдържание на електронен документ преди определен момент, посочен в удостоверението и за непроменимост на това съдържание след този момент. Приложено към електронен подпис, удостоверението създава неотменимост на подписа във времето);

Timestamping Unit (TSU) - конфигуриран хардуер и софтуер, който се управлява като единна система и има активен секретен/частен ключ за подписване по време на предоставяне на квалифицираната удостоверителна услуга за време. Удостоверението на TSU съдържа публичния ключ на TSU и е подписано от частен ключ на Базовия удостоверителен орган.

3.2 СЪКРАЩЕНИЯ

TSA – Time Stamp Authority

TSS – Time Stamp Service

TSU – Time Stamp Unit

TST - Time Stamp Token

TSQ - Time Stamp Query

UTC - Coordinated Universal Time

PKI - Public Key Infrastructure

4 ОБЩИ ПОНЯТИЯ

4.1 КВАЛИФИЦИРАНА УСЛУГА ЗА УДОСТОВЕРЯВАНЕ НА ВРЕМЕ (TIMESTAMPING SERVICE/TSS)

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

Органът за издаване на квалифицирани електронни времеви печати „Evrotrust TSA" е юридическото лице Евротръст в качеството си на квалифициран доставчик на удостоверителни услуги. „Evrotrust TSS" (Time-stamping service/услуга по удостоверяване на време) е услуга на Органа за удостоверяване на време „Evrotrust TSA" и се предоставя в съответствие с ETSI EN 319 422. Чрез включването на обектен идентификатор: 1.3.6.1.4.1.47272.1.2.1 в издадените удостоверения за време/TST, Евротръст потвърждава съответствие с „Политика и Практика на услуга за предоставяне на квалифицирани електронни времеви печати". 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 електронно подписани удостоверения (time-stamp токъни) са според изискванията на RFC 3161.

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 потребител 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 TSS Евротръст използва няколко частни ключа. Едната двойка ключове (на базовия удостоверяващ орган) се използва за издаването на електронно удостоверение, използвано от TSU, в съответствие с ETSI EN 319 411-1. Една или повече двойки ключове се използва от TSU за подписване на потребителски удостоверения

за време. Генериращият алгоритъм, дължината на подписващия ключ и подписващия алгоритъм използван за подписване на удостоверенията за време е съобразно ETSI TS 119 312. Всички частни ключове се съхраняват в FIPS 140-2 Level 3 хардуерен модул за сигурност.

„Политика и Практика на услуга за предоставяне на квалифицирани електронни времеви печати" се отнася към ETSI EN 319 401 относно общите изисквания, обичайни за всяка една услуга на Евротръст. Документът е насочен 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.

Услугата по удостоверяване на време TSS 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 публичните 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 на издадените удостоверения.

Time stamp услугата е достъпна на адрес: http://ts.evrotrust.com/tsa.

4.2 УДОСТОВЕРЯВАЩ ОРГАН ЗА ИЗДАВАНЕ НА КВАЛИФИЦИРАНИ ЕЛЕКТРОННИ ВРЕМЕВИ ПЕЧАТИ („EVROTRUST TSA")

„Evrotrust TSA" е Удостоверяващ орган в структурата на Евротръст, който предоставя квалифицирана услуга за удостоверяване на време TSS. „Evrotrust TSA" се идентифицира според условията, посочени в този документ.

Доставчикът потвърждава, че „Evrotrust TSA" подлежи на одит, най-малко веднъж на 24 месеца от Орган за оценяване на съответствието. В рамките на 3 (три) дни, докладът за оценяване на съответствието се предава на Органа по надзор – Комисията за регулиране на съобщенията.

„Evrotrust TSA" осъществява дейност по издаване на квалифицирани електронни времеви печати както следва:

- Приема искания за удостоверяване на време на представено съдържание на

електронен документ от потребител или Доверяваща се страна;

- Използва технология за обвързване на датата и часа с данните по начин, който изключва възможността за незабелязана промяна на данните;
- Дейността му се основава на атомен източник на точно време, свързан с координираното универсално време;
- Подписва (чрез TSU) с усъвършенстван електронен печат;
- Осигурява възможност за доказване в последващ период във времето (след изтичане на периода на действие на квалифицирания електронен времеви печат) на факта на подписване на електронен документи или на друг електронен обект;
- Квалифицирани електронни времеви печати се издават на физически и на юридически лица, които са потребители на услугата. 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 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 документи и електронни транзакции, при архивиране на електронни данни, в електронни нотариати и др.

Евротръст разработва и публикува „Политика и Практика на услуга за предоставяне на квалифицирани електронни времеви печати".

4.3 ПОТРЕБИТЕЛИ

**Потребители са лицата, описани в документа „Практика при предоставяне на квалифицирани удостоверителни услуги".*

Когато потребителят е организация състояща се от няколко крайни потребителя или индивидуален краен потребител, някои от задълженията отнасящи се за организацията, ще бъдат прилагани и към крайните потребители. При всички положения организацията носи отговорност, ако задълженията на крайните потребители не са коректно изпълнени. Следователно, организацията следва да информира своите крайни потребители относно

отговорността и задълженията им.

Когато потребителят е краен клиент, той носи отговорност в случай, че не изпълнява задълженията си коректно, съгласно условията, произтичащи от този документ.

4.4 ОБЩИ РАЗПОРЕДБИ НА „ПОЛИТИКА И ПРАКТИКА НА УСЛУГА ЗА ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ ЕЛЕКТРОННИ ВРЕМЕВИ ПЕЧАТИ“

Настоящият документ определя набор от правила, които Евротръст спазва при издаването на квалифицирани електронни времеви печати.

Този документ допълва „Практиката при предоставяне на квалифицирани удостоверителни услуги“, която регулира дейността на Евротръст и предоставянето на квалифицирани удостоверителни услуги.

Доставчикът издава квалифицирани електронни времеви печати на всяка заинтересована страна, без никакви технически лимити. Издаването на квалифицирани електронни времеви печати може да бъде възмездно или безвъзмездно. Информация за такси, събирани от Доставчика, може да се намери на страницата на Евротръст в интернет на адрес: https://www.evrotrust.com.

4.4.1 ПРЕДНАЗНАЧЕНИЕ

„Политика и Практика на услуга за предоставяне на квалифицирани електронни времеви печати“ е публикуван на сайта на Евротръст и предназначен за всички заинтересовани страни.

**Документа е предназначен за потребители, доверяващи се страни и всички заинтересовани страни. Управлението и подбора на персонала, физическата и оперативна сигурност на дейността на Евротръст при предоставяне на квалифицирани удостоверителни услуги са описани в документа „Практика при предоставяне на квалифицирани удостоверителни услуги“.*

4.4.2 СПЕЦИФИКА НА ПОЛИТИКАТА И ПРАКТИКАТА

„Политика и Практика на услуга за предоставяне на квалифицирани електронни времеви печати“ описва само общите правила за издаване и управление на квалифицирани

електронни времеви печати. Подробно описание на технологичния процес се съдържа в допълнителни вътрешни документи за Евротръст, които не са публични. Непубличните документи, заедно с доклади, резултати от външни и вътрешни одити са достъпни единствено за упълномощени лица.

4.4.3 ПОДХОД

Този документ е разработен в общ план и не описва всеки технически детайл от информационния обмен на данни, организационната структура, оперативните процедури или техническа сигурност на дейността на Евротръст. Той определя условията и правилата, към които се придържа Евротръст, в качеството си на квалифициран доставчик на удостоверителни услуги и е неделима част от Общите условия на договора с потребителите, при предоставяне на квалифицирани електронни времеви печати.

5 ПОЛИТИКА НА ОРГАНА ЗА УДОСТОВЕРЯВАНЕ НА ВРЕМЕ

5.1 ОБЩИ ПОЛОЖЕНИЯ

Политиката на Органа за удостоверяване на време дефинира набор от правила, които Евротръст спазва при издаването на квалифицирани електронни времеви печати. Предоставяното точно калибровано време спрямо UTC (Coordinated Universal Time) е с точност до 0,5 секунди. Доставчикът гарантира публичен достъп за получаване и проверка на издадените квалифицирани удостоверения за време.

Политиката е с присвоен уникален идентификатор на обект: 1.3.6.1.4.1.47272.1.2.

Издадените времеви печати (TST) имат присвоен уникален идентификатор на обект: 1.3.6.1.4.1.47272.1.2.1.

Евротръст гарантира спазването на подходящи мерки за сигурност, в съответствие с общоприети в международната практика документи.

Профилът на токън за електронни времеви печат е в съответствие със стандарт ETSI EN 319 422. Токънът за електронен времеви печат (TST) е издаден от TSS и съдържа информация за печата (TSTinfo структура), разположен в SignedData структура (виж RFC 2630). Той е подписан от TSU и има вградени в ContentInfo структура (виж RFC 2630). Издаваните времеви печати са съвместими с препоръките на RFC 3161.

5.2 ПРОФИЛ НА УДОСТОВЕРЕНИЕТО, С КОЕТО СЕ ПОДПИСВА КВАЛИФИЦИРАНИЯ ЕЛЕКТРОНЕН ВРЕМЕВИ ПЕЧАТ

Удостоверяващият орган издава квалифицирано удостоверение за електронен печат на TSS, с което тя подписва издадените от нея квалифицирани електронни времеви печати (Timestamp Tokens/TST). 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 услугата TSS единствено за целите на подписването на квалифицираните електронни времеви печати, издадени от този орган.

Системата за генериране на времеви печат отхвърля всеки опит за издаване на времеви печати, когато е достигнат краят на валидността на частния ключ на TSU.

Основни полета в профила на квалифицираното удостоверение:

- Version – версия (Version 3);
- Serial Number – уникален идентификационен код на времевия печат;
- Signature Algorithm – алгоритъм за създаване на електронния подпис (sha256WithRSAEncryption)
- 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.

„Evrotrust Timestamp TSU 2024" е квалифицирано удостоверение за квалифициран електронен печат на квалифицираната услуга за удостоверяване на време. Чрез него квалифицирана услуга за удостоверяване на време издава и електронно подписва квалифицирани удостоверения за време - токъни за електронен времеви печат (TST), чрез използване на модул за подписване/signing unit (SU).

Квалифицираното удостоверение за електронен печат на „Evrotrust Timestamp TSU" е:

Version	V3	
Serial number	35A94E0EE6AC1CBD42442DC8D5CACE52F2A4E684	
Signature Algorithm	SHA256RSA	
Valid from	Feb 6 14:04:34 2024 GMT	
Valid to	Feb 4 14:04:33 2029 GMT	
Issuer	CN=	Evrotrust Services CA
	O=	Evrotrust Technologies JSC
	OrganizationIdentifier(2.5.4.97)	NTRBG-203397356
	C=	BG
Subject	CN=	Evrotrust Timestamp TSU 2024
	O=	Evrotrust Technologies JSC
	OrganizationIdentifier (2.5.4.97)=	NTRBG-203397356
	C=	BG
Public Key	RSA(2048 Bits)	
Subject Key Identifier	C4728DB862587E9B47187524BEB149029710CD35	
Key Usage (critical)	Digital Signature, Non Repudiation	
Extended keyUsage (critical)	Time Stamping (1.3.6.1.5.5.7.3.8)	
Certificate Policies	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.47272.1.2 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.evrotrust.com/cps	
Authority Key Identifier	KEYID=1B3A9E6D3191A15B461984FE9C98602C09D3332E	

<table>
<tr><td>Subject alternative name (not critical)</td><td>URL=http://ts.evrotrust.com/tsa</td></tr>
<tr><td>CRL Distribution Points</td><td>[1]CRL Distribution Point
Distribution Point Name:
Full Name:

URL=http://services.evrotrust.com/EvrotrustServicesCA.crl</td></tr>
<tr><td>Authority Information Access</td><td>[1]Authority Info Access
Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)
Alternative Name:

URL=http://services.evrotrust.com/EvrotrustServicesCA.crt
[2]Authority Info Access
Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)
Alternative Name:
URL=http://services.evrotrust.com/ocsp</td></tr>
<tr><td>Basic Constraints (critical)</td><td>Subject Type=End Entity
Path Length Constraint=None</td></tr>
<tr><td>QCStatements</td><td>
<table>
<tr><td>id-qcs-pkixQCSyntax-v2[i] (oid=1.3.6.1.5.5.7.11.2)</td><td>id-etsi-qcs-SemanticsId-Legal (oid=0.4.0.194121.1.2)</td></tr>
<tr><td colspan="2">id-etsi-qcs-QcCompliance (oid=0.4.0.1862.1.1)</td></tr>
<tr><td colspan="2">id-etsi-qcs-QcSSCD (oid=0.4.0.1862.1.4)</td></tr>
<tr><td>id-etsi-qcs-QcType (oid=0.4.0.1862.1.6)</td><td>id-etsi-qct-eseal (oid=0.4.0.1862.1.6.2)</td></tr>
<tr><td>id-etsi-qcs-QcPDS (oid=0.4.0.1862.1.5)</td><td>PdsLocations

PdsLocation=https://www.evrotrust.com/pds/pds_en.pdf
language=en</td></tr>
</table>
</td></tr>
</table>

Thumbprint SHA256: 42a1b2cfaade274964dcd9c482eb9150fe33de3ce41f79396e58a4f91196518f

Thumbprint SHA1: 36e076d55521c7daba3a37e604ccf72cf59baec6

5.3 ЗАЯВКА ЗА ИЗДАВАНЕ НА ТОКЪН ЗА ЕЛЕКТРОНЕН ВРЕМЕВИ ПЕЧАТ (TIME STAMP QUERY/TSQ)

TSS приема заявки за удостоверяване на време, които да отговарят на спецификациите IETF RFC 3161 и ETSI EN 319 422. Заявката за издаване на квалифициран електронен времеви печат (Time Stamp Query/TSQ), която потребителя изпраща към TSS, трябва да съдържа алгоритъм на хеш функция, която потребителя използва. TSS приема

следните алгоритми: SHA256, SHA384 и SHA512. С цел съвместимост на услугата със съществуващи системи се приемат и алгоритмите SHA1 и MD5, като Евротръст не препоръчва тяхното използване и във всеки момент може да откаже тяхното приемане.

В заявката за квалифициран електронен времеви печат може да бъде указан и искания идентификатор OID=1.3.6.1.4.1.47272.1.2.1, който да бъде вписан в издадения TST.

Заявката може да съдържа и т.нар. NONCE, който да гарантира, че генерирания отговор TST (TSR) е в отговор точно на подадената от потребителя заявка (TSQ).

Заявката, която услугата приема и валидира, има следния профил:

Поле	**Атрибути**	**Значение/Стойност**
Version	1	
Message Imprint	Hash Algorithm:	OID на използван хеш алгоритъм
	Hash Value:	Хеш стойност на данните, изчислен с използване на хеш алгоритъм посочен в предходното поле
Requested Policy		Опционално
Nonce		Опционално
Certificate Request		Ако е TRUE се включва Квалифицираното удостоверение на Evrotrust TSA
Extensions		не се използва

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

5.4 ТОКЪН ЗА ЕЛЕКТРОНЕН ВРЕМЕВИ ПЕЧАТ (TIMESTAMPING TOKEN/TST)

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

Всеки токън за електронен времеви печат (TST), издаден от TSS, включва уникален идентификатор на настоящата политиката: OID=1.3.6.1.4.1.47272.1.2.1.

Услугата използва RSA 2048 битови частен ключ, с който електронно подписва удостоверенията за време с използване на SHA512 алгоритъм.

Профилът на отговорите на заявката (Time Stamp Response/TSR), която TSS връща на потребителя, е в съответствие с горепосочените технически спецификации и включва следните атрибути/параметри:

Поле	**Атрибути**	**Значение/Стойност**
Version	1	Версия
Policy		OID=1.3.6.1.4.1.47272.1.2.1 (съответства на политика с O.I.D.=0.4.0.2023.1.1)
Message Imprint	Hash Algorithm:	OID на използван хеш алгоритъм, подаден от потребителя на услугата
	Hash Value:	Хеш стойност на данните, подадени от потребителя на услугата, изчислен с използване на хеш алгоритъм посочен в предходното поле
Serial Number		Уникален сериен номер, определен от TSA на издадения токен за електронен времеви печат
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		Отличителното име на TSU, издал токена, както е записано в полето Subject на действащото удостоверение на TSU. За TSU в експлоатация към момента то е: DN=[CN=Evrotrust Timestamp TSU 2024, O=Evrotrust Technologies JSC, organizationIdentifier=NTRBG-203397356, C=BG].

		Стойността се променя при подновяване на удостоверението на TSU.
Extensions		не се използва

5.5 УДОСТОВЕРЯВАНЕ НА ВРЕМЕ (TIMESTAMPING)

Сървърният софтуер, който използва TSS имплементира техническата спецификация ETSI EN 319 422 Time Stamp Profile и международната препоръка IETF RFC 3161 Time Stamp Protocol.

Системният софтуер, който използва TSS поддържа комуникация с потребителите на услугата по удостоверяване на време по протоколи: TCP/IP, HTTP/HTTPS.

5.6 ИДЕНТИФИКАТОР НА ПОЛИТИКАТА НА ОРГАНА ЗА УДОСТОВЕРЯВАНЕ НА ВРЕМЕ

Идентификаторът на тази Политика (OID) е: **1.3.6.1.4.1.47272.1.2**

Издадените времеви печати (TST) имат присвоен уникален идентификатор на обект: **1.3.6.1.4.1.47272.1.2.1.** Чрез включването на този обектен идентификатор в издадените токъни за електронен времеви печат, Евротръст потвърждава съответствие с настоящата политика.

Горепосоченият обектен идентификатор е в съответствие с ETSI BTSP (Best Practices Policy for Timestamps) OID=0.4.0.2023.1.1, съгласно стандарта ETSI EN 319 422.

5.7 ПРИЛОЖИМОСТ НА ЕЛЕКТРОНЕН ВРЕМЕВИ ПЕЧАТ

Политиката на Органа за удостоверяване на време е насочена към изпълнение на изискванията за квалифицирани електронни времеви печати с дълъг период на валидност (ETSI EN 319 122), но е приложима към всяка друга употреба на времеви печати с еквивалентни изисквания. Този документ не определя никакви ограничения в приложимостта на токъна за електронен времеви печат (TST), издаден в съответствие с тази политика. Квалифицираната услуга за удостоверяване на време, позволява за всеки подписан с електронен подпис/печат документ, да се удостовери датата и часа на представяне на електронния подпис/печат.

5.8 СЪОТВЕТСТВИЕ

Издаденият токън за електронен времеви печат (TST) включва идентификатора на Политиката, описан в т. 5.3. Услугата за удостоверяване на време TSS изпълнява само заявки за електронни времеви печати, издавани в съответствие на настоящия документ. „Evrotrust TSA" осъществява дейността си в съответствие с приложимото право и стандарти и по-специално: Регламент (ЕС) № 910/2014; ETSI EN 319 421; ETSI EN 319 422 и IETF RFC 3161. Удостоверението, с което е подписан издаденият токен, се идентифицира чрез атрибута signing-certificate по IETF RFC 3161. Актуализираният атрибут по IETF RFC 5816 не се включва с оглед на съвместимостта със софтуера за валидиране, използван от потребителите на услугата.

6 ЗАДЪЛЖЕНИЯ, ГАРАНЦИИ И ОТГОВОРНОСТИ

6.1 ЗАДЪЛЖЕНИЯ

6.1.1 ОБЩИ ЗАДЪЛЖЕНИЯ

Евротръст гарантира съответствие на процедурите в настоящия документ с изискванията на Регламент (ЕС) № 910/2014 и относимите към него нормативни актове, както и националното законодателство. Процедурите подлежат на контрол от Орган за оценяване на съответствието и Орган по надзор.

6.1.2 ЗАДЪЛЖЕНИЯ НА ЕВРОТРЪСТ

Евротръст гарантира постоянен достъп до квалифицираната услуга за удостоверяване на време (24/7/365), с изключение на времето за редовните технически профилактики на технологичната система.

Евротръст гарантира публичен достъп за получаване и проверка на издадените квалифицирани токъни за електронни времеви печати. Услугата по издаване на квалифицирани електронни времеви печати е с точност до 0,5 (половин) секунда и гарантира на потребителите точност, дори при множество едновременни връзки (например над 10 потребителя).

6.1.3 ЗАДЪЛЖЕНИЯ НА КВАЛИФИЦИРАНИЯ ОРГАН ЗА УДОСТОВЕРЯВАНЕ НА ВРЕМЕ

Квалифицираният орган за удостоверяване на време („Evrotrust TSA“) предоставя услуга TSS за издаване на квалифицирани електронни времеви печати и може да има един или няколко TSU, които подписват издадените квалифицирани удостоверения за 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;
- 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.
- 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“;
- 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.

6.1.4 ЗАДЪЛЖЕНИЯ НА ПОТРЕБИТЕЛИ

Потребителите са длъжни при извличане на токъна за електронни времеви печат (TST), да проверяват валидността на електронния подпис на Органа за удостоверяване на време и/или Списъка със спрени и прекратени удостоверения (CRL).

Текущите Списъци (CRL-и) са публикувани на интернет страницата на Евротръст. Проверка на удостоверението на TSU може да се направи и с използване на услугата за Онлайн проверка на статуса на удостоверение (OCSP): https://www.evrotrust.com.

**Допълнителни задължения на потребителите са описани в т. 9.6.3 на документа „Практика при предоставяне на квалифицирани удостоверителни услуги".*

6.1.5 ЗАДЪЛЖЕНИЯ НА ДОВЕРЯВАЩИ СЕ СТРАНИ

Доверяващата се страна трябва да има необходимия минимум от технически познания за използване на квалифицираната услуга за удостоверяване на време и да полага дължимата грижа. Основното задължение на Доверяващата се страна е да провери подписа върху токъна за електронния времеви печат (TST). Доверяващата се страна трябва да провери валидността на удостоверението на TSU, както и срока на валидност на това удостоверение. В случай на проверка на времеви печати, след изтичане на срока на валидност на удостоверението на TSU, доверяващите се страни трябва :

- да направят проверка в Списъка със спрени и прекратени удостоверения (CRL) за удостоверението на TSU;
- да направят проверка за приложимостта на използвания хеш алгоритъм;
- да се уверят в сигурността на използвания електронен подпис, като проверят приложимата комбинация на асиметрични и хеш алгоритми;

**Използването на времеви печати трябва да отговаря на изискванията на настоящия документ и „Практика при предоставяне на квалифицирани удостоверителни услуги".*

6.2 ГАРАНЦИИ НА ЕВРОТРЪСТ

Евротръст поема следните гаранции:

- за предоставяне на квалифицираната удостоверителна услуга, използва надеждно и сигурно технологично оборудване (хардуер и софтуер);
- извършва своята дейност законосъобразно;
- предоставяните удостоверителни услуги са съобразени с общоприети международни стандарти и документи, описани в „Практика при предоставяне на квалифицирани удостоверителни услуги"
- издадения електронен токън за електронен времеви печат (TST) не съдържа никакви неверни данни или грешки;
- не се нарушават лицензии, интелектуална собственост или други права в издаваните токъни за електронни времеви печати (TST);
- не допуска модифициране на цифровите данни след издаване на токъна на времевия печат (TST), без това да бъде установено.

6.3 ОТГОВОРНОСТИ

Отговорността на всяко лице, участник в дейността по предоставяне и ползване на квалифицирана удостоверителна услуга е уредена в закона или се уговаря в договора между Евротръст и потребителя.

Евротръст отговаря пред потребителите на удостоверителни услуги, които разчитат на неговата дейност за вреди, причинени от умисъл и тежка небрежност..

Отговорност на Евротръст се отнася само, ако вредите са пряка и непосредствена последица от виновно поведение на Евротръст или на лицата, на които е възложил осъществяване на функции във връзка с предоставяните удостоверителни услуги по удостоверяване на време.

Ако Евротръст потвърди и приеме, че са настъпили вреди, той се ангажира да овъзмезди увреденото лица. Евротръст отговаря до размера на реалните вреди.

Евротръст сключва задължителна застраховка на дейността си като квалифициран доставчик на квалифицирани удостоверителни услуги. Задължителната застраховка покрива отговорността на Евротръст към Потребители, съответно Доверяващи се страни за причинени имуществени и неимуществени вреди до границите определени в националното

законодателство и тази практика.

7 УПРАВЛЕНИЕ И КОНТРОЛ НА ТЕХНИЧЕСКАТА СИГУРНОСТ НА ОРГАНА ЗА УДОСТОВЕРЯВАНЕ НА ВРЕМЕ

7.1 ОБЩИ ИЗИСКВАНИЯ КЪМ ОРГАНА ЗА УДОСТОВЕРЯВАНЕ НА ВРЕМЕ

Органът за удостоверяване на време („Evrotrust TSA“) осъществява контрол на дейността си, което позволява предоставянето на квалифицирана удостоверителна услуга в съответствие с разпоредбите на настоящия документ. За да се контролира ефективното функциониране на технологичната система за отчитане на времето, профилите на потребителите и дейността на персонала, всички събития в системата се регистрират.

Евротръст гарантира, че осъществява надеждно, сигурно и законосъобразно управление на дейността си, като контролира всички страни, свързани по някакъв начин с процедурите на отчитане на времето, записва информацията и управлява по подходящ начин персонала, за да извършва коректно задълженията си. Всички документи, свързани с регистрираната информация и събития се записват в журнали и се архивират. Съхранението на записите се осъществява по сигурен начин. Достъп до тези данни имат единствено оторизирани служители на Доставчика.

Органът за удостоверяване на време подлежи на ежегодна оценка на риска, за да се оценят бизнес активите и заплахите за тези активи, в следствие на което се определят необходимите мерки за сигурност и оперативни процедури.

7.2 ВЪТРЕШНА ОРГАНИЗАЦИЯ

**Процедури, механизми за контрол, управление на сигурността и поддръжка на инфраструктурата на Доставчика са подробно описани в документа „Практика при предоставяне на квалифицирани удостоверителни услуги“ и са в съответствие с ETSI EN 319 401.*

Контролите, които прилага Органа за удостоверяване на време позволяват непрекъсната проверка на целостта на технологичната система, своевременна актуализация и отстраняване на неизправности. Осъществяваният надзор на функционалността на технологичната система гарантира, че тя работи правилно и в съответствие с доставената

производствена конфигурация. Текущата конфигурация на технологичната система на Евротръст, както и всички изменения и актуализации, се записват и извършват контролирано.

Евротръст информира всички потребители и доверяващи се страни за условията и реда за използване на услугата си за удостоверяване на време.

7.2.1 ДОСТЪПНОСТ НА УСЛУГАТА

С оглед осигуряване достъпност на услугата, Евротръст прилага следните мерки:

- резервираност на компютърните системи;
- резервираност на интернет свързаността;
- употреба на непрекъсваеми електрозахранвания.

Евротръст предоставя TSS с непрекъснат достъп (24/7/365), като достъпността и точността са гарантирани, дори и ако няколко потребителя да са едновременно свързани с приложението. Всяко физическо, юридическо или друго лице, което има сключен договор с Евротръст за TSS е потребител на тази услуга. Когато това е практически осъществимо, предоставяната удостоверителни услуги TSS е достъпна и за хора с увреждания.

7.3 УПРАВЛЕНИЕ НА ЖИЗНЕНИЯ ЦИКЪЛ НА ДВОЙКАТА КЛЮЧОВЕ НА TSU

7.3.1 ГЕНЕРИРАНЕ НА ДВОЙКА КЛЮЧОВЕ НА TSU

Органът за удостоверяване на време („Evrotrust TSA“) отговаря за услугата за предоставяне на квалифицирани електронни времеви печати TSS. TSU, като част от TSS, подписва потребителските удостоверения за време с частен ключ, който съответства на удостоверение, издадено от Базовия удостоверяващ орган, който в случая е Органа за удостоверяване на време („Evrotrust TSA“) в архитектурата на Евротръст. Генерирането на подписващия ключ на TSU се извършва във физически защитена среда от лица с доверени роли. Достъпът е двуфакторен от минимум две оторизирани лица. Генерирането на подписващия ключ се извършва в криптографски модул (HSM) с ниво на сигурност FIPS 140-2, ниво 3. Генерираната двойка RSA ключове е с дължина 2048 бита. Изискванията за използваните алгоритми и дължината на подписващия частен ключ са съобразени с техническата спецификация ETSI TS 119 312.

7.3.2 ЗАЩИТА НА ЧАСТНИЯ КЛЮЧ НА TSU

Частният ключ на TSU се генерира и съхранява в криптографски модул (HSM) съответстващ на стандарт FIPS 140-2, ниво 3. Архивираното копие на частния ключ се съхранява в специален сейф. Съхраняването на копие на ключа е с цел при настъпване на бедствие или срив в системата, ключът да може да бъде възстановен. Съхраняването на ключа периодично се проверява от системния одитор. Начинът на съхранение е описан в процедури от вътрешната документация на Евротръст.

Когато се архивират частни ключове на TSU, те се копират, съхраняват и възстановяват само от персонал в доверени роли, като се използва поне двоен контрол във физически защитена среда.

TSU има един активен в даден момент ключ за подписване на времеви печат.

7.3.3 РАЗПРОСТРАНЕНИЕ НА ПУБЛИЧНИЯ КЛЮЧ НА TSU

Удостоверението на TSU, което е подписано от „Evrotrust TSA" и се използва от TSU за подписване на потребителски квалифицирани електронни времеви печати се публикува на страницата на Евротръст на адрес: https://www.evrotrust.com. Удостоверението на TSU е издадено от удостоверяващия орган „Evrotrust Services CA", който в архитектурата на Евротръст изпълнява ролята на „Evrotrust TSA".

TSA гарантира целостта и автентичността на ключовете за проверка на подписа на TSU (публични) с най-малко следните специфични изисквания:

а) Ключовете за проверка на подпис на TSU (публични) се предоставят на доверяващите се страни в удостоверението за публичен ключ;

б) Удостоверението на публичния ключ за проверка на подпис на TSU се издава от удостоверяващ орган, работещ съгласно ETSI EN 319 411-1;

в) TSU не издава времеви печат, преди неговото удостоверение за проверка на подписа (публичен ключ) да бъде заредено в TSU или в криптографското устройство.

При получаване на сертификат за проверка на подписа (публичен ключ), TSA проверява дали този сертификат е правилно подписан (включително проверка на веригата от сертификати до доверен сертифициращ орган).

7.3.4 ПРОДЪЛЖАВАНЕ НА СРОКА И/ИЛИ ПРЕИЗДАВАНЕ НА ЧАСТНИЯ КЛЮЧ НА TSU

Жизненият цикъл на частния ключ на TSU не може да бъде по-дълъг от времевия период, през който избраният алгоритъм или дължина на ключа удовлетворяват целта, за която са приети за използване. В съответствие с изискванията на ETSI EN 319 421 относно края на жизнения цикъл на ключа на TSU, частният ключ на TSU се използва за период от 3 (три) години. Периодът на валидност на удостоверението на TSU е 5 години. В рамките на 2 (две) години преди изтичане на този 5 (пет) годишен период се издава ново удостоверение. За новото удостоверение се генерира нова двойка ключове, частният ключ от която се съхранява в криптомодула (HSM), а публичният ключ се удостоверява, чрез издаване на ново удостоверение на TSU със същия 5 (пет) годишен период на валидност. Всички събития, свързани с жизненият цикъл на двойката ключове на удостоверението на TSU се съхраняват за период от 10 (десет) години.

Ако разширението "X.509 Private Key Usage Period (PKUP)" не е включено в удостоверението на TSU, TSA налага ограничението за използване на частния ключ чрез следните оперативни контроли:

- Политика за ротация на ключове: Нова ключова двойка ще бъде генерирана преди изтичане на 3-годишния период на използване на частния ключ;
- Административен и одитен контрол: TSA осигурява съответствие чрез вътрешен мониторинг, периодични одити на използването на ключовете и ръчно деактивиране на частния ключ след изтичане на 3-годишния период;
- Технически ограничения: Системата за подписване на TSA преустановява използването на частния ключ след 3(три) години, независимо от това, че удостоверението на TSU остава валидно.

Всички използвани алгоритми се проверяват веднъж годишно или когато настъпят промени. В случай, че алгоритъмът бъде компрометиран или стане неподходящ, за целта се пристъпва към прегенерирането на всички засегнати ключове и издаване на нови удостоверения за TSU.

7.3.5 УНИЩОЖЕНИЕ НА ЧАСТНИЯ КЛЮЧ НА TSU

След изтичането на срока на валидност на частния ключ на TSU, същият се унищожава по начин, по който не може да бъде възстановен. Всички резервни копия на ключа,

включително и тези, съхранявани в HSM, се изтриват за постоянно или се архивират съгласно политиките за информационна сигурност на Евротръст.

7.3.6 УПРАВЛЕНИЕ НА ЖИЗНЕНИЯ ЦИКЪЛ НА ПОДПИСВАЩОТО КРИПТОГРАФСКО ОБОРУДВАНЕ

Прилагат се следните специални изисквания:

а) криптографският хардуер за подписване с времеви печат не се манипулира по време на изпращането на отговор ;

б) криптографският хардуер за подписване с времеви печат не се манипулира докато се съхранява;

в) Инсталирането, активирането и дублирането на ключовете за подписване на TSU в криптографския хардуер се извършва само от персонал с доверени роли, като се използва поне двоен контрол във физически защитена среда;

г) TSU ключовете за подписване, съхранявани в криптографския модул на TSU, се изтриват при оттегляне на устройството по начин, който практически е невъзможно да бъдат възстановени.

Използваният криптографски модул се инспектира от доверен персонал с двоен контрол по време на транспортиране и съхранение. Модулът се проверява за:

- повреди по стикерите за сигурност;
- повреди по кутията на модула (драскотини, вдлъбнатини);
- повреди по опаковката.

Допълнително се прилагат следните мерки:

- инсталацията, активацията и създаването на резервно копие на подписващия частен ключ на TSU в криптографския модул се извършва само от доверен персонал с двуфакторен контрол във физически защитена среда;
- в случай на бракуване на криптографския модул, съдържащите се на него частни ключове ще бъдат изтрити и унищожени в съответствие с препоръките на производителя.

7.3.7 СИНХРОНИЗАЦИЯ НА ЧАСОВНИКА С КООРДИНИРАНОТО УНИВЕРСАЛНО ВРЕМЕ

TSS използва хардуерен източник на точно калибровано време с висока точност. Синхронизацията на UTC с източника на време е автоматична, на база NTP-протокол, след установяване на разлика между източника и времето в системата. В случай на възникнал проблем в хардуерния източник на време и до подмяна на същия с резервен такъв, като източник на точно време се използват базирани в интернет сървъри на време. Синхронизацията е на базата на поне два източника на време, чрез протокол NTP.

Доставчикът гарантира, че осигурява физическа и информационна сигурност на технологичната система за предотвратяване на неоторизирани операции, насочени към нарушаване на калибрирането/точността на часовника или неговото физическо увреждане.

Евротръст има контроли, които позволяват откриване на всяка разлика между часовника и времето, включени в токъна за електронен времеви печат (TST).

7.4 УПРАВЛЕНИЕ И ДЕЙНОСТ НА ОРГАНА ЗА УДОСТОВЕРЯВАНЕ НА ВРЕМЕ

7.4.1 УПРАВЛЕНИЕ НА СИГУРНОСТТА

В Евротръст е въведена политика по информационна сигурност. Всички служители се задължават да спазват нормите на тази политика. Политиката по информационна сигурност се разглежда редовно и в случай на настъпили промени.

**Всички въпроси, свързани с управлението на сигурността, са описани в документа „Практика при предоставяне на квалифицирани удостоверителни услуги“.*

7.4.2 ОЦЕНКА НА РИСКА

С цел осигуряване на качество и надеждност на предоставяните услуги Евротръст редовно извършва оценка на риска. Проверките на сигурността, дефинирани в концепцията за сигурност на Доставчика се контролират на всеки три месеца с цел осигуряване ефективност на контрола.

**Описание на процедурите и плановете за постигане на непрекъснатост и сигурност на дейността на Доставчика са описани в документа „Практика при предоставяне на*

квалифицирани удостоверителни услуги" от „Евротръст Технолъджис" АД.

Всички системи, включени в издаването на квалифициран електронен времеви печат предлагат висока степен на надеждност. Технологичната система се намира във физически защитена среда, което минимизира риска от природни бедствия.

В случай, че частният ключ на Органа за удостоверяване на време бъде компрометиран, засегнатият криптомодул (HSM) бива незабавно изолиран от мрежата, след което се вземат коригиращи мерки:

- уведомяване на администратора по сигурността, с цел предприемане на бъдещи действия;
- в случай на компрометиране на частния ключ на TSU, съмнение за компрометиране или загуба на калибриране, TSU не издава времеви печати, докато не се предприемат стъпки за възстановяване;
- започване на одит по сигурността на останалите криптомодули (HSM-и) – проверка на интегритет и анализ на журнала;
- уведомяване на доверяващите се страни, които са засегнати от компрометирането;
- започване на процедура по подмяна.

7.4.3 ОПЕРАТИВНА СИГУРНОСТ

Евротръст поддържа квалифицирани служители на длъжности, които осигуряват изпълнения на задълженията си във всеки момент при осъществяването на дейността по издаване на квалифицирани електронни времеви печати, в съответствие с нормативната уредба.

**Характеристиката на персонала и доверените роли на Доставчика са в съответствие с документа „Практика при предоставяне на квалифицирани удостоверителни услуги" от „Евротръст Технолъджис" АД.*

7.4.4 ФИЗИЧЕСКА СИГУРНОСТ

Сигурното и надеждно извършване на операции от TSS се осъществява посредством

различни нива на сигурност на физическия и логически достъп до технологичната система.

Доставчикът осигурява:

- защитена физическа среда;
- разделяне на мрежови сегменти;
- разделяне на задълженията;
- наблюдение на мрежата и услугите;
- подсигуряване на компютърните системи.

В случай, че служител, който отговаря за дейности за удостоверяване на време, смени своята роля или напусне дружеството, всички принадлежащи му носители, свързани със сигурността се връщат или се инвалидират.

**Физическият контрол и контролът на достъпа са в съответствие с документа „Практика при предоставяне на квалифицирани удостоверителни услуги" от „Евротръст Технолъджис" АД.*

7.4.5 МРЕЖОВА СИГУРНОСТ

Мрежовата инфраструктура е разделена на зони, базирани на оценка на риска, отчитайки функционалното, логическото и физическото взаимоотношение между доверени системи и услуги.

Доставчикът ограничава достъпа и комуникациите между зоните до такъв, необходим за нормалната работа на удостоверителните услуги. Връзките и услугите, които не се отнасят към удостоверителните услуги са деактивирани. Установеното правило за достъп се разглежда на определен период.

Всички елементи на критичната инфраструктура се пазят в защитена зона.

Изградена е административна мрежа, която е отделена от мрежата за оперативни цели. Системите използвани за администрация не могат да бъдат използвани за неадминистративни дейности.

Тестовата и експлоатационната платформа са отделени от други среди нямащи отношение към работни операции.

Комуникацията между отдалечени доверени системи се извършва само през сигурни канали, които са логически отделени от останалите комуникационни канали и предоставят

идентификация на своите крайни точки. Осигурена е защита на данните по канала срещу разкриване или модификация.

Свързаността към интернет е резервирана.

Редовно се сканират за уязвимости публичните и частните IP адреси за достъп, след което се изготвя доклад.

Тест за проникване в системите се извършва в следните случаи: след първоначална настройка на системите и след инфраструктурни или надграждания на приложения и промени. След приключване на теста се изготвя доклад.

7.4.6 УПРАВЛЕНИЕ НА ДЕЙНОСТТА

При всяка ново разработена система се прави анализ на изискванията по отношение на сигурността още по време на етапа на дизайн и планиране на функционалността. При пускането на нови версии се прилагат процедури по контрол на промените, включително и при неотложни промени в софтуера.

Целостта на системите и информацията са защитени срещу вируси, зловреден код и неоторизиран софтуер. Всички системи са защитени съобразно политиката на сигурност на Евротръст. Боравенето с външни носители в Евротръст се осъществява по сигурен начин с цел защитата им от повреда, кражба или остаряване. Въведени са процедури за всички доверени и административни роли, които имат отношение към предоставяне на удостоверителни услуги. В Евротръст са въведени политики, осигуряващи своевременно прилагане на пачове (patch/ поправки на софтуера) по сигурността. Изискванията към капацитета на компютърните системи се следят, с цел осигуряване на достатъчно количество изчислителна мощност и дисково пространство.

7.4.7 УПРАВЛЕНИЕ НА ДОСТЪПА ДО СИСТЕМА

Евротръст осигурява наблюдение върху достъпа до компютърните системи и потребителски заявки, относно:

- необичайни системни дейности, които показват потенциално нарушение на сигурността, включително проникване в мрежата на Евротръст и докладване, чрез система

за алармиране;

- стартиране и изключване на логващите функции;
- наличност и използване на услуги в мрежата на Евротръст.

При всяко нарушение на сигурността или загуба на интегритет, които имат значително влияние върху предлаганата доверена услуга, както и върху управляваните лични данни Евротръст съобщава на Органа по надзор. След откриването на критичен пробив в сигурността Органа по надзор се уведомява в срок от 24 ч.

7.4.8 СИГУРНА СРЕДА

Криптомодулът (HSM) с удостоверено ниво на сигурност FIPS 140-2 Level 3 е оперативната среда за съхраняване на частния ключ на TSU и за електронно подписване на токъни за електронни времеви печати (TST), които се доставят на потребителите.

Документите, свързани със сигурността на средата са предимно вътрешна документация на Евротръст и се преглеждат периодично от одитора.

7.4.9 КОМПРОМЕТИРАНЕ НА ЧАСТНИЯ КЛЮЧ НА TSU

Евротръст полага максимални грижи в рамките на възможностите и ресурсите си, да минимизира риска от компрометиране на частния ключ на TSU вследствие на човешка грешка, природни бедствия или аварии.

В случай на компрометиране или съмнение за компрометиране на частен ключ на Органа за удостоверяване на време на Евротръст, се предприемат следните действия:

- прекратява се незабавно удостоверението на TSU;
- „Evrotrust TSA" (Базовия удостоверяващ орган) генерира ново удостоверение за нова двойка ключове;
- всички потребители и доверяващи се страни се информират за случилото се незабавно, с информация на страницата на Евротръст;
- удостоверението, съответстващо на компрометирания ключ се поставя в Списъка със спрени и прекратени удостоверения (CRL), заедно с подходяща причина за

прекратяване;

- извършва се незабавен анализ и се изготвя доклад за причината за компрометирането.

Тези операции се извършват в съответствие с плана, разработен от Евротръст, за инциденти със сигурността.

7.4.10 ПРЕКРАТЯВАНЕ НА ДЕЙНОСТТА НА ОРГАНА ЗА УДОСТОВЕРЯВАНЕ НА ВРЕМЕ

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

- Следва актуализиран и одобрен от ръководството план и сценарий за прекратяване на дейността на удостоверяващ орган. Информирането може да се извърши чрез имейл или чрез публикуване;
- уведомява потребителите, Органа по надзор и третите страни за прекратяването на дейността на своя удостоверяващ орган. Информацията се предоставя чрез имейл или чрез публикуване на сайта на Евротръст;
- прекратява разрешението на всички лица, които имат договорни дейности да извършват дейности, свързани конкретния удостоверяващ орган;
- преди прекратяване на дейността на удостоверяващия орган, в разумен срок, прехвърля задълженията си по поддържане на цялата информация, необходима за предоставяне на доказателства на надеждна страна;
- преди да прекрати дейността, частните ключове, включително резервните копия, биват унищожени или изтеглени от употреба по такъв начин, че личните ключове да не могат да бъдат извлечени;
- при възможност прехвърля дейността си на друг квалифициран доставчик;
- Евротръст прилага мерки за покриване на разходите в случай на банкрут или поради други причини за прекратяване на действието на удостоверяващ орган. В случай, че не е в състояние да покрие разходите сам е предвидил мерки в рамките на приложимото законодателство;
- променя статуса на оперативното удостоверение;
- прекратява издаването нови удостоверения, но продължава да управлява активните удостоверения до края на тяхното действие;

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

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

**Всички процедури за непрекъснатост на дейността са описани в документа „Практика при предоставяне на квалифицирани удостоверителни услуги" на „Евротръст Технолъджис" АД.*

7.4.11 СПАЗВАНЕ НА ПРАВНИ ИЗИСКВАНИЯ

За всички въпроси, неуредени в „Политика и Практика на услуга за предоставяне на квалифицирани електронни времеви печати" се прилагат разпоредбите на Регламент 910/ЕС и приложимото законодателство.

Всички изисквания за предоставяне на квалифицирани електронни времеви печати, произтичащи от настоящия документ, са в съответствие с изискванията на стандартите и стандартизационни документи на ETSI, произтичащи от разпоредбите на Регламент (ЕС) № 910/2014.

Всяка претенция за удовлетворяване на изискванията на услугата за предоставяне на квалифицирани електронни времеви печати е съгласно националното законодателство. В общите условия за използване на услугата е оповестено времето на наличност на услугата.

7.4.12 ЗАПИС НА ДОКАЗАТЕЛСТВА

Всяко доказателство за състоянието на технологичната система и информационните данни се записва по сигурен и надежден начин. Евротръст записва и пази достъпна всяка информация, отнасяща се до издадени или получени данни, за съответния период от време. Тези записи се съхраняват дори и след прекратяване на услугата.

Евротръст осигурява:

- поддържане на конфиденциалност и интегритет на текущите и архивирани записи, отнасящи се до дейността на услугата съобразно добрите практики;

- записи, отнасящи се до дейността на услугата, могат да бъдат предоставени на компетентните органи за целите на съдопроизводството, в случай че е нужно доказателство за правилната й работа;
- водят се записи на всички събития, отнасящи се до жизнения цикъл на ключовете и удостоверенията на Органа за удостоверяване на време;
- водят се записи на всички събития свързани със синхронизацията на часовника на TSS с координираното универсално време (UTC). Това включва информация отнасяща се до нормалното прекалибриране или синхронизиране на часовниците, използвани при предоставянето на квалифицирани електронни времеви печати;
- записи за всички събития при установяването на загуба на синхронизация;
- всички събития са записват по начин, който ги прави трудни за изтриване.
- журналите на събития се пазят най-малко 3 месеца;
- журналът за издадените квалифицирани електронни времеви печати се пази 10 години.

7.5 ОРГАНИЗАЦИОННА СХЕМА

За правилната работа на Органа за удостоверяване на време, Евротръст поддържа вътрешни документи, които описват оперативния контрол отнасящ се до: сигурност на персонала, контрол на достъпа, оценка на риска и др. Тези вътрешни документи се анализират от независим Орган за оценяване на съответствието съгласно изискванията на техническа спецификация ETSI EN 319 421.

„Евротръст Технолъджис" АД е българско юридическо лице, акционерно дружество: вписано в Търговския регистър на Агенцията по вписванията под ЕИК: 203397356, със седалище и адрес на управление:

„Евротръст Технолъджис" АД
1766 София, България
бул. „Околовръстен път" № 251 Г
„ММ Бизнес център", ет. 5,
Телефон за контакт: + 359 2 4485858
уебсайт: http://www.evrotrust.com
адрес на електронна поща: office@evrotrust.com.

Настоящият документ е публикуван на уебсайта на Евротръст в интернет на български и английски език. В случай на несъответствие между текстовете на български и английски език, приоритет има българския текст.