ПОЛИТИКА

НА ОРГАНА ЗА УДОСТОВЕРЯВАНЕ НА ВРЕМЕ

Версия: 2.0

	Длъжност	Име, фамилия	Дата	Подпис
Утвърдил	Изпълнителен директор	Константин Безуханов	*13.04.2017 г.*	
Съгласувал	Представител на ръководството по СУСИ	Стефан Хаджистойчев	*13.04.2017 г.*	
Разработил	Консултант по СУСИ	Мария Владимирова	*13.04.2017 г.*	

Дата на регистрация на документа:	*13.04.2017 г.*
Оригиналът се съхранява:	*при Представител на ръководството по СУСИ*

Вид на екземпляра и пореден №

Оригинал	X	**Контролирано копие**		**Информационен**	

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.

СЪДЪРЖАНИЕ

1. ВЪВЕДЕНИЕ

Този документ представлява Политика и Практика за предоставяне на квалифицирана услуга за удостоверяване на време на Доставчик на квалифицирани удостоверителни услуги „ЕВРОТРЪСТ ТЕХНОЛЪДЖИС" АД (ЕВРОТРЪСТ/Доставчик).

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

В „Политиката и практиката на Органа за удостоверяване на време" 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. Подробно описание на тези правила са представени в документа „Практика при предоставяне на квалифицирани удостоверителни услуги".

Структурата и съдържанието на настоящата „Политика и практика за удостоверяване на време" е изготвена в съответствие с техническата спецификация ETSI TS 102 023.

ЕВРОТРЪСТ изпълнява „Политика и практика за удостоверяване на време" при предоставяне на електронни времеви печати и публично осигурява квалифицирана удостоверителна услуга по предоставяне на квалифицирани електронни времеви печати. Тя е достъпна на адрес в интернет: https://www.evrotrust.com.

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 отговаря на следните изисквания:

- 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 или квалифициран електронен подпис или е подпечатан с усъвършенстван или квалифициран електронен печат на ЕВРОТРЪСТ като квалифициран доставчик на квалифицирани удостоверителни услуги.

1.1. ОБХВАТ

Настоящият документ може да се използва от Доверяващи се страни и потребители на квалифицирани удостоверителни услуги.

ЕВРОТРЪСТ гарантира надеждността на предоставената квалифицирана удостоверителна услуга за време чрез своя Орган за удостоверяване на време, който е обособено и неделимо звено на Доставчика.

Предоставянето на квалифицирани електронни времеви печати се основава на инфраструктура с публичен ключ, източници на сигурно време и формат на удостоверения X.509.

2. ПРЕПРАТКИ

В настоящия документ се съдържат препратки към стандарти и стандартизационни документи, процедури, директиви, национално законодателство и 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), в това число:

- Recommendation ITU-R TF.460-6: „Standard-frequency and time-signal emissions";
- ISO/IEC 19790:2012: „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";
- FIPS PUB 140-2: „Security Requirements for Cryptographic Modules";
- IETF RFC 3161 „Internet X.509 Public Key Infrastructure: Timestamp Protocol (TSP)";
- IETF RFC 5816: „ESSCertIDV2 update to RFC 3161";
- Практика при предоставяне на квалифицирани удостоверителни услуги (Certification Practice Statement/CPS) на ЕВРОТРЪСТ ТЕХНОЛЪДЖИС” АД;

3. ОПРЕДЕЛЕНИЯ И АБРЕВИАТУРИ

3.1. ОПРЕДЕЛЕНИЯ

- Coordinated Universal Time (UTC) - Координирано универсално време, отчетено в съответствие с Recommendation ITU-R TF.460-6 [1];

- 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 (Титуляр/Създател), на което е предоставена услугата за издаване на квалифициран електронен времеви печат;
- Електронен времеви печат (Timestamp) - 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“) - вътрешна инфраструктурна единица в рамките на ЕВРОТРЪСТ, която издава квалифицирани електронни времеви печати;
- 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 от „Evrotrust TSA“ 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.

3.2. АБРЕВИАТУРИ

TSA - Timestamping Authority

TSS - Timestamping Service

TSU - Timestamping Unit

TST - Time Stamp Token

UTC - Coordinated Universal Time

PKI - Public Key Infrastructure

4. ОБЩИ ПОНЯТИЯ

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

Обменът на данни в инфраструктурата на ЕВРОТРЪСТ, която се използва за издаване и управление на квалифицирани електронни времеви печати се състои от два основни компонента:

- Технологична система, която издава квалифицирани електронни времеви печати, поддържа регистър и архив на генерираните токъни за електронен времеви печати;
- Управление на системата, чрез която се наблюдават и контролират операциите по приемане на онлайн заявки, издаване, проверка и утвърждаване на издадените токъни за електронни времеви печати.

Управлението на системата гарантира директен достъп до сигурен източник на координирано универсално време (UTC) и надеждно управление на компонентите на технологичната система.

Квалифицираната услуга за удостоверяване на време (Qualified Timestamp Service/TSS) се изпълнявана от вътрешно звено на Евротръст – Орган за удостоверяване на време („Evrotrust TSA“). Органът за удостоверяване на време издава квалифицирани електронни времеви печати (Qualified Timestamp), чрез които потребителите на Доставчика могат да удостоверят времето за представяне на електронни документи, електронни подписи, електронни транзакции и др. Квалифицираният електронен времеви печат е доказателство, че обектът от данни е съществувал към момента на поставяне на времевия печат.

За тази цел е необходимо „Evrotrust TSA“ да:

- потвърди съществуването на данните;
- осигури доказателство, че електронния подпис/печат е положен при валидна двойка криптографски ключове, използвани за подписване/подпечатване на електронния документ или електронното съобщение;
- не е страна по сделките, посочени и обозначени с удостоверението за време;
- издаде квалифициран електронен времеви печат в съответствие със стандарт ETSI EN 319 422;
- издаде квалифициран електронен времеви печат, който не съдържа грешки или неточна информация.

4.2. ОРГАН ЗА УДОСТОВЕРЯВАНЕ НА ВРЕМЕ

„Evrotrust TSA“ е Удостоверяващ орган в структурата на ЕВРОТРЪСТ, който предоставя квалифицирани услуги за удостоверяване на време. „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.

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 ЗА УДОСТОВЕРЯВАНЕ НА ВРЕМЕ“

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 за удостоверяване на време“ е публикуван на сайта на Доставчика и е на разположение на 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

„Политиката и практиката на органа за удостоверяване на време“ описва само общите правила за издаване и управление на квалифицирани електронни времеви печати.

Подробно описание на технологичния процес се съдържа в допълнителни документи, 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 ЕВОТРЪСТ, 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.

Дейността на ЕВРОТРЪСТ е организирана така, че издаването на квалифицирани електронни времеви печати е отделено от останалите дейности на Доставчика.

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), 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). Издаваните времеви печати са съвместими с препоръките на RFC 3161. Квалифицираната услуга за удостоверяване на време издава RSA 2048 битови криптирани квалифицирани електронни времеви печати, които се използва един от следните алгоритми: SHA1 и SHA256.

Профилът на удостоверението на „Evrotrust TSA“, с което се верифицира електронния времеви печат в издадения токън за електронен времеви печат (TST) е следния:

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
	O=	Evrotrust Technologies JSC
	OrganizationIdentifier(2.5.4.97)=	NTRBG-203397356
	C=	BG
Subject	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	Time Stamping (1.3.6.1.5.5.7.3.8)	

(critical)	
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	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	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://ca.evrotrust.com/crl/EvrotrustRSARootCA.crl
Authority Information Access	[[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://ca.evrotrust.com/aia/EvrotrustRSARootCA.crt [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ca.evrotrust.com/ocsp
Basic Constraints (critical)	Subject Type=End Entity Path Length Constraint=None

5.2. ИДЕНТИФИКАТОР НА ПОЛИТИКАТА НА ОРГАНА ЗА УДОСТОВЕРЯВАНЕ НА ВРЕМЕ

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

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.

5.3. 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 [6]), 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.

5.4. СЪОТВЕТСТВИЕ

Издаденият токън за електронен времеви печат (TST) включва идентификатора на Политиката, описан в т. 5.2. Органът за удостоверяване на време („Evrotrust TSA“) 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 TS 119 421;
- IETF RFC 3161;
- IETF RFC 5816.

6. ЗАДЪЛЖЕНИЯ И ОТГОВОРНОСТ НА ОРГАНА ЗА УДОСТОВЕРЯВАНЕ НА ВРЕМЕ

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 КЪМ ПОТРЕБИТЕЛИ

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.

Доставчикът 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 100 потребители).

Освен това, ЕВРОТРЪСТ гарантира, че:

- 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.

6.2. 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 на адрес: https://www.evrotrust.com.

Проверка на удостоверението на Органа за удостоверяване на време („Evrotrust TSA“) 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“.

6.3. 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 Органа за удостоверяване на време („Evrotrust TSA“), както и срока на валидност на това удостоверение. В случай на проверка на времеви печати, след изтичане на срока на валидност на удостоверението на „Evrotrust TSA“ , доверяващите се страни трябва :

- да направят проверка в Списъка със спрени и прекратени удостоверения (CRL) за удостоверението на Органа за удостоверяване на време („Evrotrust TSA“);
- 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“.

6.4. ОТГОВОРНОСТ

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 Доставчика 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. 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 настоящата Политика. 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.

7.1. ПРАКТИКА И ПРОЦЕДУРИ НА ОРГАНА ЗА УДОСТОВЕРЯВАНЕ НА ВРЕМЕ

7.1.1. ПРАКТИКА

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“.

Задълженията и отговорността на Органа за удостоверяване на време са описани в т. 6 на настоящия документ и са в основата на функциониране на Удостоверяващия орган.

Контролите 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.

7.1.2. 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.

Документът „Политика и практика за удостоверяване на време“ е публично достъпен. Настоящият документ е публикуван на сайта на Доставчика в интернет на адрес: https://www.evrotrust.com.

7.2. УПРАВЛЕНИЕ НА ЖИЗНЕНИЯ ЦИКЪЛ НА ДВОЙКАТА КЛЮЧОВЕ НА ОРГАНА ЗА УДОСТОВЕРЯВАНЕ НА ВРЕМЕ

7.2.1. ГЕНЕРИРАНЕ НА ДВОЙКА КЛЮЧОВЕ НА ОРГАНА ЗА УДОСТОВЕРЯВАНЕ НА ВРЕМЕ

Генерирането на подписващия ключ на Органа за удостоверяване на време („Evrotrust TSA“) 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.

7.2.2. ЗАЩИТА НА ЧАСТНИЯ КЛЮЧ НА ОРГАНА ЗА УДОСТОВЕРЯВАНЕ НА ВРЕМЕ

Частният ключ на Органа за удостоверяване на време („Evrotrust TSA“) се генерира и съхранява в криптографски модул (HSM) съответстващ на стандарт FIPS 140-2, ниво 3.

Архивираните копия на частния ключ на „Evrotrust TSA“ се съхраняват 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 одитора на Доставчика. Начинът на съхранение е описан в процедури от вътрешната документация на ЕВРОТРЪСТ.

7.2.3. РАЗПРОСТРАНЕНИЕ НА ПУБЛИЧНИЯ КЛЮЧ НА ОРГАНА ЗА УДОСТОВЕРЯВАНЕ НА ВРЕМЕ

Удостоверението на Органа за удостоверяване на време („Evrotrust TSA“) заедно със съответния публичен ключ се публикува на страницата на ЕВРОТРЪСТ в интернет: https://www.evrotrust.com.

Удостоверението на „Evrotrust TSA“ е издадено от Базовия удостоверяващ орган („Evrotrust RSA Root CA“).

7.2.4. ПРОДЪЛЖАВАНЕ НА СРОКА И/ИЛИ ПРЕИЗДАВАНЕ НА ЧАСТНИЯ КЛЮЧ НА ОРГАНА ЗА УДОСТОВЕРЯВАНЕ НА ВРЕМЕ

Жизненият цикъл на частния ключ на Органа за удостоверяване на време („Evrotrust TSA“) не може да бъде по-дълъг от периода на време, през който избраният алгоритъм или дължина на ключа удовлетворяват целта, за която са приети за използване. Периодът на валидност на удостоверението на „Evrotrust TSA“ е 5 години. След изтичане на този период, срокът на валидност на удостоверението се продължава за период от 5 години. След този период 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 „Evrotrust TSA“. Двойката ключове с изтекъл период на валидност се съхранява, както следва:

- частен ключ – съхранява се за период от 10 години;
- публичен ключ – съхранява се за период от 10 години.

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.

7.2.5. УНИЩОЖЕНИЕ НА ЧАСТНИЯ КЛЮЧ НА ОРГАНА ЗА УДОСТОВЕРЯВАНЕ НА ВРЕМЕ

След изтичането на срока на валидност на частния ключ на „Evrotrust TSA“, същият се унищожава по начин, по който не може да бъде възстановен.

7.2.6. УПРАВЛЕНИЕ НА ЖИЗНЕНИЯ ЦИКЪЛ НА ПОДПИСВАЩОТО КРИПТОГРАФСКО ОБОРУДВАНЕ

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 „Evrotrust TSA“ 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. УДОСТОВЕРЯВАНЕ НА ВРЕМЕ (TIMESTAMPING)

Сървърният софтуер на „Evrotrust TSA“ имплементира техническата спецификация „ETSI TS 101 861 v.1.3.1 (2006-01) Time Stamp Profile“ и международната препоръка IETF RFC 3161 (Time Stamp Protocol).

Системният софтуер на „Evrotrust TSA“ поддържа комуникация с клиентите на услугата по удостоверяване на време по протоколи: TCP/IP, HTTP/HTTPS.

7.3.1. ТОКЪН ЗА ЕЛЕКТРОНЕН ВРЕМЕВИ ПЕЧАТ (TIMESTAMPING TOKEN/TST)

Всеки токън за електронен времеви печат (TST), издаден от ЕВРОТРЪСТ, включва уникален идентификатор на политиката на Органа за удостоверяване на време.

Профилът на заявките/отговорите на „Evrotrust TSA“ системата е в съответствие с горепосочените технически спецификации и включва следните атрибути/параметри:

➢ Заявката за издаване на TST (TSQ) включва:

Поле	Атрибути	Значение/Стойност
Version	1	
Message Imprint	Hash Algorithm:	OID на хеш SHA-1, SHA-256
	Hash Value:	Хеш стойност на данните
Requested Policy		OID=1.3.6.1.4.1.47272.2.1 (съответства на политика с O.I.D.=0.4.0.2023.1.1)
Nonce		Опционално
Certificate Request		Ако е TRUE се включва Квалифицираното удостоверение на Evrotrust TSA
Extensions		не се използва

➢ TST отговора на заявката (TSR) включва:

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

7.3.2. СИНХРОНИЗАЦИЯ НА ЧАСОВНИКА С КООРДИНИРАНОТО УНИВИРСАЛНО ВРЕМЕ

„Evrotrust TSA“ 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 разкалибриране 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;
- 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 Органа за удостоверяване на време („Evrotrust TSA“) 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 на Органа за удостоверяване на време 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

Крипто-модулът (HSM) с удостоверено ниво на сигурност FIPS 140-2 Level 3 е оперативната среда за съхраняване на частния ключ на Органа за удостоверяване на време 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. КОМПРОМИТИРАНЕ НА ЧАСТНИЯ КЛЮЧ НА ОРГАНА ЗА УДОСТОВЕРЯВАНЕ НА ВРЕМЕ

Доставчикът ЕВРОТРЪСТ полага максимални грижи в рамките на възможностите и ресурсите си, да минимизира риска от компрометиране на частния ключ на Органа за удостоверяване на време („Evrotrust TSA“) 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 „Evrotrust TSA“;
- Базовият орган генерира нова двойка ключове и ново удостоверение;
- всички потребители и доверяващи се страни се информират за случилото се незабавно, с информация на страницата на Доставчика;
- 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

В случай на прекратяване на „Evrotrust TSA“ се изпълняват съответните процедури от 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 за удостоверяване на време“ 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.

7.4.12. ЗАПИС НА СЪБИТИЯ

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 Органа за удостоверяване на време 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 най-малко 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 TS 119 421.

„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
ул. „Николай Хайтов" 2, вх. Д, ет. 2
1113 София, България

Телефон за контакт:
+ 359 2 448 58 58
Уебсайт: http://www.evrotrust.com
Адрес на електронна поща: office@evrotrust.com

Регистриране на измененията																					
Страница																					
Валидно изменение																					