ISO 9001:2015 ISO 27001:2013
ISO 20000-1:2018 ISO 22301:2019
Регламент (ЕС) 910/2014
Регламент (ЕС) 2016/679

# ПОЛИТИКА И ПРАКТИКА
# НА УСЛУГА ПО КВАЛИФИЦИРАНО ВАЛИДИРАНЕ НА
# КВАЛИФИЦИРАНИ ЕЛЕКТРОННИ ПОДПИСИ/ПЕЧАТИ

## СЪДЪРЖАНИЕ

# 1. ВЪВЕДЕНИЕ

Този документ определя правилата за квалифицирано валидиране на електронни подписи и печати и издаване на електронно подписани доклади чрез удостоверителната услуга за квалифицирано валидиране „Evrotrust Qualified Validation Service". Електронно подписаните доклади представляват автоматично генерирани електронно документи, съдържащи резултата от проверката на електронния подпис/печат, които доклади са електронно подписани от валидиращия орган на Евротръст.

Настоящият документ е разработен от „Евротръст Технолъджис" АД (Евротръст) в съответствие с изискванията, определени в Регламент (ЕС) № 910/2014[1] и в съответствие с ETSI TS 119 441.

## 1.1. ОБЩ ПРЕГЛЕД

Електронните подписи са основен крайъгълен камък за електронните транзакции, при условие че могат да бъдат валидирани по такъв начин, че потребителите и доверяващите се страни да имат пълно доверие във факта, че отговарят на своите (бизнес) нужди. В този смисъл потребителят и доверяващата се страна могат да се обърнат към Евротръст, който в качеството си на квалифициран доставчик на услуга за валидиране на подписи (QSVSP) ще извърши валидирането на цифровия подпис от тяхно име. Резултатът от тази услуга е доклад за валидиране. Участниците в електронните транзакции трябва да бъдат уверени, че Евротръст има установени процедури и защитни мерки, за да се сведе до минимум оперативните и финансовите заплахи, и рисковете, свързани с технологиите на електронните подписи.

Настоящият документ има заглавие „Политика и Практика на услуга по квалифицирано валидиране на квалифицирани електронни подписи/печати" (Политика и практика на услуга за валидиране на подпис/печат). Целта на Политиката и Практиката е да отговори на общите изисквания на международната общност за предоставяне на доверие в електронните

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

транзакции, включително и на общо приложимите изисквания на Регламент (ЕС) № 910/2014 г., които установяват правна рамка за електронния подпис и електронния печат, включително и за техното валидиране.

Евротръст предоставя услугата в съответствие с изискванията, определени в Регламент (ЕС) № 910/2014 г. и гарантира, че тази услуга:

- Използва оперативни процедури и процедури за управление на сигурността, които изключват всякакво възможност за манипулиране на данните и състоянието на валидираните удостоверения или;
- Проверява валидността на електронния подпис/печат в съответствие с изискванията на член 33 на Регламент (ЕС) № 910/2014 г.;
- Проверява състоянието на удостоверенията в съответствие с препоръка RFC 6960: X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP;
- Валидира квалифицирани удостоверения и електронни подписи/печати;
- Изпълнява техническите процедурите за валидиране на подписи съгласно изискванията на ETSI TS 319 102-1 и ETSI TS 119 172-4;
- Евротръст (QSVSP) може да предостави допълнителна информация за подписа или печата, напр. ако е усъвършенстван електронен подпис/печат въз основа на квалифицирано удостоверение;
- За да гарантира правилното функциониране на услугата за валидиране Евротръст тества всяка промяна във функционалността на услугата за валидиране, като тестовете се запазват във вътрешната документация на Евротръст. Тестовете подлежат на проверка и констатации;
- Докладът за валидиране носи електронния печат на Евротръст;
- Докладът за валидиране може да се предостави на доверяващата е страна по автоматизиран начин, в съответствие с ETSI TS 119 442 и ETSI TS 119 102-2;
- Докладът за валидиране може да се представи на потребителя чрез уеб страница, в рамките на TLS сесия, поддържана от удостоверение, издадено от сертифициращ орган в удобен за него вид;
- Докладът за валидиране съдържа квалифициран времеви печат, който е в съответствие с Регламент (ЕС) № 910/2014 г.;

- Евротръст проверява изчислението на хеша въз основа на който е подписан документа. Установяването на връзката между подписания документ и подписа е в съответствие с изискванията на Регламент (ЕС) № 910/2014 г.;
- Политиката за валидиране на подписа (OID) е в съответствие с ETSI TS 119 172-4 и недвусмислено посочва, че подписът е квалифициран съгласно Регламент (ЕС) № 910/2014 г.;
- Докладът за валидиране позволява на доверяващата се страна да се увери в сигурността на подписа/печата. Посочва се информация, че удостоверението е издадено от Доставчик на квалифицирани удостоверителни услуги и е било валидно към момента на подписването. Данните за валидиране на подписа съответстват на данните, предоставени от доверяващата страна. Ако към момента на подписване е бил използван псевдоним, то това е ясно указано на доверяващата се страна. Електронният печат е създаден от устройство за създаване на електронен печат. Целостта на подписаните данни не е застрашена.

### 1.1.1. ИДЕНТИФИКАЦИЯ НА ДОСТАВЧИКА

Доставчикът на услугата е Евротръст Технолъджис АД се идентифицира с регистриран идентификатор на обект (OID – Object Identifier) OID:1.3.6.1.4.1.47272.

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

### 1.1.2. ПОДДЪРЖАНИ ПОЛИТИКИ

Евротръст присвоява идентификатор на обект (OID – Object Identifier) на всяка от политиките, в съответствие с които се валидират издадените квалифицирани удостоверения от Евротръст.

Стойността на идентификатора на обект за политика, която Евротръст следва е:

| **Валидиращ орган (QESValidation/Q)** | **Идентификатор на обект (OID)** |
|---|---|
| **Evrotrust Qualified Validation Service**<br>Политика на валидиращия орган, обслужваща удостоверения за електронен подпис и печат по Регламент (ЕС) № 910/2014 г., | 1.3.6.1.4.1.47272.2.9 |

Той съответстват на ETSI TS 119 441 специфичен OID: itu-t(0) identified-organization(4) etsi(0) val-service-policies(19441) policy-identifiers(1) qualified (2).

Евротръст идентифицира политиките за обслужване, които поддържа съгласно ETSI EN 319 401. Услугата за валидиране на Евротръст вписва приложимия OID на използваната политика в отговорите, докладите и документите, които се предоставят на потребителите и доверяващите се страни.

Евротръст гарантира, че не променя обектния идентификатор на настоящия документ, както и обектните идентификатори на политиките, практиките и другите реферирaщи 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.въ

### 1.1.3. НОРМАТИВНИ ПОЗОВАВАНИЯ

**Regulation (EU) No 910/2014** of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC;

**ETSI TR 119 001** „Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures; Definitions and abbreviations“;

**ETSI TS 119 102-2** „"Elecrtonic Signatures and Infrastructures (ESI); Procedures for Creation and

Validation of AdES Digital Signatures; Part 2: Signature Validation Report";

**ETSI EN 319 122-1** „Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures";

**ETSI EN 319 122-2** „Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 2: Extended CAdES signatures";

**ETSI EN 319 132-1** „Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures";

**ETSI EN 319 132-2** „Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 2: Extended XAdES signatures";

**ETSI EN 319 142-1** „Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures";

**ETSI EN 319 142-2** "lectronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 2: Additional PAdES signatures profiles";

**ETSI TS 119 172-1** „Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 1: Building blocks and table of contents for human readable signature policy documents";

**ETSI TS 119 172-4** "lectronic Signatures and Infrastructures (ESI); Signature policies; Part 4: Signature validation policy for European qualified electronic signatures/seals using trusted Lists";

**ETSI TS 119 442** „Electronic Signatures and Infrastructures (ESI); Protocol profiles for trust service providers providing AdES digital signature validation services";

**ETSI EN 319 403** „Electronic Signatures and Infrastructures (ESI); Trust Service Provider

Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers";

**ETSI TS 119 312** „Electronic Signatures and Infrastructures (ESI); Cryptographic Suites";

**Regulation (EU) 2016/679** of the European Parliament and of the Council of 27 April 2016 on the
protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation);

**ETSI EN 319 411-1** „Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements";

**ETSI EN 319 411-2** „Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates";

**ETSI EN 319 412-4** „Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates";

**ETSI TS 119 172-2** „Electronic Signatures and Infrastructures (ESI); Signature Policies;
Part 2: XML format for signature policies";

**ETSI TS 119 172-3** „Electronic Signatures and Infrastructures (ESI); Signature Policies;
Part 3: ASN.1 format for signature policies";

**IETF RFC 3647** „Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework".

## 1.2. КОМПОНЕНТИ НА УСЛУГАТА ЗА ВАЛИДИРАНЕ НА ПОДПИСА

### 1.2.1. УЧАСТНИЦИ В УСЛУГАТА ЗА ВАЛИДИРАНЕ НА ПОДПИСИ (SVS)

Двата основни участника са Евротръст (QSVSP), който е квалифициран доставчик на удостоверителни услуги (QTSP) и клиент. QSVSP може да предложи една или повече услуги за валидиране на подписи въз основа на договорни отношения. Услугата за валидиране на електронен подпис/печат може да се комбинира с услуга за увеличаване надеждността на подписа, в съответствие с протоколът посочен в ETSI TS 119 442, който поддържа заявката за увеличаване надеждността на подписа с услугата за валидиране.

Клиентът може да бъде приложение или физическо лице (потребител), взаимодействащо с приложението за проверка на подписа.

Други участници в предоставянето на услуги за валидиране на подписа могат да бъдат:

- Подписващ - подписващият може да задава ограничения на подписа (например чрез политика за подписване и това може да повлияе върху валидирането на подписа;
- Свързаните с подписващите доставчици на удостоверителни услуги (TSP):
  - TSP, който е издал удостоверение на подписващия (CA);
  - Всеки TSP, който може да бъде включен в генерирането на подпис:
- Други TSP (TSAs; QSVSP и т.н.)
- Европейската комисия, която предоставя доверителен списък с квалифицирани доставчици.

### 1.2.2. ВАЛИДИРАЩ ОРГАН

Валидиращият орган, който обслужваща удостоверения за електронен подпис и печат, функционира в съответствия с изискванията на Регламент (ЕС) № 910/2014 г.

“Evrotrust Qualified Validation Service” и „Evrotrust Qualified Validation Service SU“ са квалифицирани удостоверение за квалифициран електронен печат на квалифицираната услуга за квалифицирано валидиране. Чрез тях квалифицирана услуга за квалифицирано валидиране електронно подписва докладите за квалифицирано валидиране на проверените електронно подписани документи, чрез използване на модул за подписване/signing unit (SU).

Квалифицираното удостоверение за електронен печат на „Evrotrust Qualified Validation Service“ е:

| | | |
|---|---|---|
| Version | V3 | |
| Serial number | 38 00 00 00 05 f0 08 5a 0a b9 a3 69 64 00 00 00 00 00 05 | |
| Signature Algorithm | SHA256RSA | |
| Issuer | CN= | Evrotrust RSA Root CA |
| | OU= | Evrotrust Qualified Root Authority |
| | O= | Evrotrust Technologies JSC |
| | organizationIdentifier | NTRBG-203397356 |
| | C= | BG |
| Valid from | 14 февруари 2018 г. 12:16:20 UTC | |
| Validit to | 14 февруари 2023 г. 12:26:20 UTC | |
| Subject | CN= | Evrotrust Qualified Validation Service |
| | O= | Evrotrust Technologies JSC |
| | organizationIdentifier (2.5.4.97)= (2.5.4.97) | NTRBG-203397356 |
| | C= | BG |
| Public Key Type/Length | RSA (2048 Bits) | |
| Subject Key Identifier | 5d 19 73 73 35 60 65 a1 62 e7 c2 0d d1 fe 63 e5 4f 90 c8 1a | |
| Certificate Policies | [1]Certificate Policy:<br>Policy Identifier=1.3.6.1.4.1.47272.2.9<br>[1,1]Policy Qualifier Info:<br>Policy Qualifier Id=CPS<br>Qualifier:<br>http://www.evrotrust.com/cps | |
| Authority Key Identifier | KeyID=74 5c a1 40 73 2e 1f e6 f9 3b bc ab a0 a4 a7 54 44 74 4f 70 | |
| CRL Distribution Points | [1]CRL Distribution Point<br>Distribution Point Name: | |

| | |
|---|---|
| | Full Name:<br>URL=http://ca.evrotrust.com/crl/EvrotrustRSARootCA.crl |
| Authority Information Access | [1]Authority Info Access<br>Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)<br>Alternative Name:<br>URL=http://ca.evrotrust.com/aia/EvrotrustRSARootCA.crt<br>[2]Authority Info Access<br>Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)<br>Alternative Name:<br>URL=http://ca.evrotrust.com/ocsp |
| Key Usage (critical) | Digital Signature, Non-Repudiation (c0) |
| Basic Constrains (critical) | Subject Type=End Entity<br>Path Length Constraint=None |

Квалифицираното удостоверение за електронен печат на „Evrotrust Qualified Validation Service SU" е:

| | | |
|---|---|---|
| Version | V3 | |
| Serial number | 72 dc e5 b1 c8 ec e7 58 39 6f 7f 2e 1b e8 06 15 6e 7e b2 1b | |
| Signature Algorithm | SHA256RSA | |
| Issuer | CN= | Evrotrust Services CA |
| | organizationIdentifier | NTRBG-203397356 |
| | O= | Evrotrust Technologies JSC |
| | C= | BG |
| Valid from | 13 July 2019, 15:45:22 UTC | |
| Validit to | 11 July 2024, 15:45:22 UTC | |
| Subject | CN= | Evrotrust Qualified Validation Service SU |
| | organizationIdentifier | NTRBG-203397356 |
| | O= | Evrotrust Technologies JSC |
| | C= | BG |
| Public Key | RSA (2048 Bits) | |

<table>
<tr><td>Type/Length</td><td></td></tr>
<tr><td>Authority Key Identifier</td><td>KeyID=1b 3a 9e 6d 31 91 a1 5b 46 19 84 fe 9c 98 60 2c 09 d3 33 2e</td></tr>
<tr><td>Authority Information Access</td><td>[1]Authority Info Access<br>Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)<br>Alternative Name:<br>URL=http://services.evrotrust.com/EvrotrustServicesCA.crt<br>[2]Authority Info Access<br>Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)<br>Alternative Name:<br>URL=http://services.evrotrust.com/ocsp</td></tr>
<tr><td>Certificate Policies</td><td>[1]Certificate Policy:<br>Policy Identifier=1.3.6.1.4.1.47272.2.9<br>[1,1]Policy Qualifier Info:<br>Policy Qualifier Id=CPS<br>Qualifier:<br>http://www.evrotrust.com/cps</td></tr>
<tr><td>QCStatements</td><td>
<table>
<tr><td>id-qcs-pkixQCSyntax-v2 (oid=1.3.6.1.5.5.7.11.2)</td><td>id-etsi-qcs-SemanticsId-Legal (oid=0.4.0.194121.1.2)</td></tr>
<tr><td colspan="2">id-etsi-qcs-QcCompliance (oid=0.4.0.1862.1.1)</td></tr>
<tr><td 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:<br>PdsLocation=https://www.evrotrust.com/pds/pds_</td></tr>
</table>
</td></tr>
</table>

| | | |
|---|---|---|
| | | en.pdf<br>language=en |
| CRL Distribution Points | [1]CRL Distribution Point<br>Distribution Point Name:<br>Full Name:<br>URL=http://services.evrotrust.com/EvrotrustServicesCA.crl | |
| Subject Key Identifier | c5 da 13 76 8c ad fd fa 9e e3 2b 80 99 42 6e c7 3a f7 3c 1c | |
| Basic Constrains (critical) | Subject Type=End Entity<br>Path Length Constraint=None | |
| Key Usage (critical) | Digital Signature, Non-Repudiation (c0) | |

*Thumbprint (SHA1):* 9372295a5d83b7bd27dda84a9fb88f164363ca60

*Thumbprint (SHA256):*

43e0882978f98ceca29360083ab1ea5a277740714e9c6dbcc023b1618d3549a

*Filename: "Evrotrust Qualified Validation Service SU.pem.cer"*

### 1.2.3. АРХИТЕКТУРА НА УСЛУГАТА

Услугата за валидиране съдържа следните компоненти:

- Клиентът на услугата за валидиране на подписа е компонент или софтуер, който изпълнява валидирането на подписа по протокол по заявка от страна на потребителя. По-специално:
  - Изисква валидиране на подпис от сървъра за проверка на подписването (SVSServ);
  - Възможно е да се поиска валидиране на множество подписи, съобразно ETSI TS 119 442;
  - Изпълнява протокола за проверка на подписа (SVP) от страна на потребителя;
  - Когато е приложимо, се грижи за представянето на доклада за валидиране;

Клиентът може да включи:

- Потребителски интерфейс за ръчно въвеждане на заявката или

- Машинен интерфейс за автоматизирани заявки;
- Потребителски интерфейс за представяне на доклада. Проверката на приложимостта, т.е. окончателното решение за „приемане" на подписа въз основа на доклада от валидирането може да се извърши от потребителя (ръчно), или от клиента, или от сървъра (в зависимост от изпълнението на SVS). Това може да се направи съгласно правилата за приложимост на подписите, които са посочени в ETSI TS 119 172-1;

➢ Сървърът за валидиране на подпис (SVSServ), който в качеството си на компонент на услугата изпълнява протокол за валидиране от страна на QSVSP. По-специално:

- Изпълнява протокола за проверка на подпис и обработва валидирането на подписа;
- Изпълнява приложението за валидиране на подписа (SVA), както е определено в ETSI TS 119 102-1, което включва изпълнение на валидиращия алгоритъм, определен в ETSI TS 119 102-1. За тази цел Евротръст допуска услугата да призовава външни участници, напр. CA, който е издал удостоверението на подписващия, услуги за информация на статуса (OCSP), или списъци със спрени и прекратени удостоверения (CRL), CA на TSA, които са предоставили времеви печати, други QSVSP за допълнителни проверки, доверителни списъци на европейските държави-членки, доверителния списък на Европейската комисия и т.н.
- Създава доклада (ите) за валидиране на подписа;
- Създава отговор за валидиране на подписа. SVSServ изпълнява SVA, както е посочено в ETSI TS 119 102-1. Допустимо е в определени случаи приложението за управление (DA) да бъде изцяло от страната на клиента или да бъде споделено между клиент и сървър (сървърът за проверка на подпис може да изпълни част от DA, например извършване на проверка за приложимост). Настоящият документ не поставя изисквания към клиента. Изискванията са само към елементите на DA, внедрени на сървърната страна.

## 1.3. ОПРЕДЕЛЕНИЯ И СЪКРАЩЕНИЯ

### 1.3.1. ОПРЕДЕЛЕНИЯ

Прилагат се определенията посочени в ETSI EN 319 401 и ETSI TR 119 001, както и следните:

**Проверка на приложимостта (applicability checking) -** определяне дали подписът отговаря на правилата за приложимост. Проверката за приложимост допълва услугата за валидиране на подписа;

**Вид ангажираност на подписа (signature) commitment type)** – предназначение на подписа;

**Ограничение за създаване на подпис ((signature) creation constraint)** – критерии, използвани при създаването на подпис;

**Приложение за управление (driving application/DA)** - приложение, което използва система за създаване на подпис, за да създаде или валидира подпис. В процеса на валидиране на подписа приложението доставя AdES цифров подпис и други входни данни на приложението за валидиране на подпис (SVA);

**Услуга по квалифицирано валидиране на квалифицирани електронни подписи (qualified validation service for qualified electronic signatures)** – както е посочено в чл. 33 на Регламент (ЕС) № 910/2014 г.;

**Услуга по квалифицирано валидиране на квалифицирани електронни печати** (qualified validation service for qualified electronic seals) - както е посочено в чл. 40 на Регламент (ЕС) № 910/2014 г.;

**Доставчик на услуга по квалифицирано валидиране (qualified validation service provider/QSVSP)** – доставчик, който предоставя квалифицирана услуга за валидиране за квалифицирани електронни подписи/печати;

**Приемане на подпис (signature acceptance)** - технически процес, определен в ETSI TS 119 102-1 и представлява част от процеса по валидиране на подписа. Извършва се чрез подаване на заявление за валидиране на подписа;

**Правила за приложимост на подписа (signature applicability rules) -** набор от правила, приложими за един или повече цифрови подписи, които определят дали подписът е подходящ за определена бизнес или правна цел. Правилата включват политики за валидиране на подписа, съдържащи ограничения на проверката. За целите се прилага ETSI TS 119 172-1;

**Категории подписи (signature class)** - набор от подписи, постигащи определена функционалност (например времеви подпис, подпис за дългосрочно валидиране и др.)

**Устройство за създаване на подпис (signature creation device) -** конфигуриран софтуер или хардуер, който се използва за създаването на електронен подпис;

**Приложение за валидиране на подписа (signature validation application/SVA)** - приложение, което валидира подпис, в съответствие с установена политика за валидиране на подписа, и в резултат извежда индикация за състоянието на валидиране на подписа и доклад за проверка на подписа. Описание на приложението за валидиране на подписа е в ETSI TS 119 102-1;

**Валидиращ клиент на подписа (signature validation client)** - компонент или част от софтуер, който изпълнява протокола за проверка на подписа от страна на потребителя;

**Политика за валидиране на подписа (signature validation policy)** - набор от ограничения за валидиране на подписи, обработени или подлежащи на обработка от SVA. Политиката за валидиране на подписа е чисто техническа концепция. Политиката за валидиране на подписа определя правилата за приложимост на подписа;

**Доклад за валидиране на подписа (signature validation report)** - изчерпателен доклад за валидирането, предоставен от приложението за валидиране на подписа (DA) и разрешаване на приложението и всяка друга страна извън приложението, да проверят детайлите, снети по време на валидирането, и да проучат подробните причини за посочването на статуса,

предоставен на подписа. Докладът може да е в съответствие с ETSI TS 119 102-2, като минималните изисквания за съдържанието му са определени в клауза 5.1.3 на ETSI TS 119 102-1;

**Политика на услуга за валидиране на подпис (Signature Validation Service (SVS) policy)** – Представлява набор от правила, които определят качеството и приложимостта на услугата за валидиране на подпис. Документът определя приложимостта на услугата към дадена общност и/или категория с общи изисквания за сигурност. Политиката на SVS е приложима за удостоверителна услуга, както е определено в ETSI EN 319 401;

**Практика на услуга за валидиране на подпис (ignature validation service (SVS) practice statement)** - представлява практики и процедури, използвани за изпълнение на всички определени изисквания за предоставяне на услугата за валидиране на подпис. Практиката се отнася за удостоверителна услуга, която е част от документацията на QSVSP в съответствие с ETSI EN 319 401;

**Сървър за валидиране на подпис (signature validation service server)** - компонент, който изпълнява протокола за валидиране на подпис и обработва процеса по валидиране от страна на QSVSP;

**Статус на валидиране на подписа (signature validation status)** - едно от следните указания: TOTAL-PASSED, TOTAL-FAILED или неопределен;
**Валидиране на подписа (signature validation)** - процес на проверка и потвърждаване, че електронния подпис е технически валиден;

**Проверка на подписа (signature verification)** - процес на проверка на криптографската стойност на подписа, чрез използване на данни за проверка на подписа;

**Подписващ (signer)** - лице, което е създател на цифров подпис;

**Ограничение за валидиране на подписа (signature validation constraint)** - технически

критерии, спрямо които може да се валидира електронен подпис, както е посочено в ETSI TS 119 102-1;

**Потребител (user)** - приложение или физическо лице, взаимодействащо с приложението за проверка на подписа;

**Валидиране (validation)** - процеса на проверка и потвърждаване на валидността на електронен подпис или печат;

**Данни за валидиране (validation data)** - данни, които се използват за валидиране на електронен подпис или електронен печат;

**Валидиране на квалифициран електронен подпис (alidation of qualified electronic signature)** - както е посочено в член 32 на Регламент (ЕС) № 910/2014 г.;

**Валидиране на квалифицирани електронни печати (validation of qualified electronic seals)** - както е посочено в член 40 на Регламент (ЕС) № 910/2014 г.;

**Услуга за валидиране (validation service)** - система, достъпна чрез комуникационна мрежа, която валидира цифровия подпис;

**Верификатор (verifier)** - обект, който иска да провери или проверява цифровия подпис.

### 1.3.2. СЪКРАЩЕНИЯ

Прилагат се определенията посочени в ETSI EN 319 401 и ETSI TR 119 001, както и следните:

**DA** - Driving Application/Приложение за управление;

**OVR** – OveRall/Общи изисквания, приложими за повече от 1 (един) компонент;

**PoE** - Proof of Existence/Доказване за наличие;

**QES** - Qualified Electronic Signature or Qualified Electronic Seal/Квалифициран електронен подпис/печат;

**(Q)SCD** - (Qualified) Signature Creation Device/Устройство за създаване на (квалифициран) подпис;

**QSVSP** - Qualified Signature Validation Service Provider/Доставчик на квалифицирана услуга за валидиране на подпис;

**SD** - Signer's Document/Подписващ документ;

**SDO** - Signed Data Object/Подписан обект от данни;

**SDR** - Signed Document Representation/Представяне на подписан документ;

**SVA** - Signature Validation Application/Приложение за валидиране на подпис;

**SVP** - Signature Validation Protocol/Протокол за валидиране на подпис;

**SVR -** Signature Validation Report/Доклад за валидиране на подпис;

**SVS -** Signature Validation Service/Услуга за валидиране на подпис;

**QSVSP -** Signature Validation Service Provider/Доставчик на услуга за валидиране на подпис;

**SVSServ -** Signature Validation Service Server/Сървър на услуга за валидиране на подпис;

**TSA -** Time Stamping Authority/ Орган за удостоверяване на време;

**VPR -** signature Validation Process/Процес на валидиране на подписа.

## 1.4. ИЗИСКВАНИЯ КЪМ ПОЛИТИКАТА, ПРАКТИКАТА И ОБЩИТЕ УСЛОВИЯ

### 1.4.1. ОРГАНИЗАЦИЯ, УПРАВЛЯВАЩА ДОКУМЕНТАЦИЯТА НА ЕВРОТРЪСТ

Евротръст отговаря за управлението на публичната документация, в това число и настоящия документ. Всяка версия на всеки документ е в сила до момента на одобрение и публикуване на нова версия. Всяка нова версия се разработва от служители на Евротръст и след одобрение от Съвета на директорите на Евротръст се публикува.

Потребителите са длъжни да се съобразяват само с валидната версия на Практиките и Политиките към момента на ползване на услугите на Евротръст.

Настоящият документ е неразривно свързан с документа „Практика при предоставяне на квалифицирани удостоверителни услуги".

### 1.4.2. ЛИЦЕ ЗА КОНТАКТ

Контактното лице за управление на документа „Политика и практика за

квалифицирано валидиране“ от „Евротръст Технолъджис“ АД е изпълнителния директор на Евротръст.

Допълнителна информация може да бъде получена на следния адрес:

гр. София, 1766

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

телефон, факс: + 359 2 448 58 58

електронна поща: office@evrotrust.com

### 1.4.3. ПРИЛОЖИМОСТ НА ПУБЛИЧНАТА ДОКУМЕНТАЦИЯ НА ЕВРОТРЪСТ

Публичната документация на Евротръст, която е свързана с предоставяне на услугата за квалифицирано валидиране е на разположение на всички заинтересовани страни и е публикувана на страницата на Евротръст в интернет: https://www.evrotrust.com/landing/en/a/tsp-documents. Наборът от свързаните документи с услугата за квалифицирано валидиране включват:

- „Политика и Практика на услуга по квалифицирано валидиране на квалифицирани електронни подписи/печати“ с OID: 1.3.6.1.4.1.47272.2.9;
- „Общи условия на договора за предоставяни удостоверителни, информационни, криптографски и консултантски услуги с OID: 1.3.6.1.4.1.47272.3.1.2;
- „Тарифа за предоставяни удостоверителни, информационни, криптографски и консултантски услуги“ с OID:1.3.6.1.4.1.47272.2.15;
- „Практика при предоставяне на квалифицирани удостоверителни услуги“ с OID: 1.3.6.1.4.1.47272.3.1.1;
- „Политика при предоставяне на квалифицирано удостоверение за квалифициран електронен подпис/печат“ с OID: 1.3.6.1.4.1.47272.2.2, 1.3.6.1.4.1.47272.2.3 и 1.3.6.1.4.1.47272.2.2.1;
- „Политика при предоставяне на квалифицирано удостоверение за усъвършенстван електронен подпис/печат“ с OID: 1.3.6.1.4.1.47272.2.7;
- Политика и Практика на услуга за предоставяне на квалифицирани електронни времеви печати, Version – 3.0/01.05.2019 с OID: 1.3.6.1.4.1.47272.1.2;
- „Договор за използване на услугите, достъпни чрез приложението на „Евротръст

Технолъджис" АД" с OID:1.3.6.1.4.1.47272.2.16.1;

- „Договор за квалифицирани удостоверителни услуги за клиенти на „Евротръст Технолъджис" АД – Част 1: Договор с клиент, физическо лице" с OID: 1.3.6.1.4.1.47272.2.16.2;
- „Договор за квалифицирани удостоверителни услуги за клиенти на „Евротръст Технолъджис" АД – Част 1: Договор с клиент, юридическо лице" с OID: 1.3.6.1.4.1.47272.2.16.3;
- „Договор за квалифицирани удостоверителни услуги за клиенти на „Евротръст Технолъджис" АД – Част 2: Договор с Титуляр/Създател" с OID: 1.3.6.1.4.1.47272.2.16.4.

### 1.4.4. ПОЛИТИКА НА УСЛУГАТА ЗА ВАЛИДИРАНЕ

Политиката на SVS е интегрирана в настоящия документ и съдържа информация относно приложимостта на услугата. Получателите на услугата могат да бъдат физически и юридически лица и доверяващи се страни. Политиката предоставя информация за нивото на услугата.

### 1.4.5. ПРАКТИКА НА УСЛУГАТА ЗА ВАЛИДИРАНЕ

Практика на услугата за валидиране на подпис QSVSP е интегрирана в настоящия документ и е разработена, прилага се, и се актуализира както е определено в ETSI EN 319 401. Практиката на SVS описва как Евротръст изпълнява услугата и е собственост на QSVSP. Достъп до практиката имат одиторите, потребителите и доверяващите се страни. Настоящият документ описва начина на изпълнение на изискванията, идентифицирани като необходими за поддържане на услуга за валидиране на подписи/печати на високо равнище. Документът е одобрен от Евротръст.

### 1.4.6. УПОТРЕБА И ПРИЛОЖИМОСТ НА УСЛУГАТА ЗА ВАЛИДИРАНЕ

Евротръст предоставя услуга по квалифицирано валидиране на електронни подписи и печати, която дава възможност на доверяващите се страни да получат доклад от процеса по проверка на валидността на подписите/печатите по автоматизиран и надежден начин.

Докладът е подписан с квалифициран електронен печат на Евротръст. Чрез услугата се гарантира, че подписите и печатите се създават и проверяват в съответствие с европейското законодателство (eIDAS).

## 2. УПРАВЛЕНИЕ И ДЕЙНОСТ НА УДОСТОВЕРИТЕЛНАТА УСЛУГА

Евротръст предоставя криптографски, информационни и консултантски услуги свързани с приложимостта на удостоверителните услуги, в това число:

- Издаване и управление на квалифицирани удостоверения за усъвършенствани и квалифицирани електронни подписи/печати;
- Издаване и управление на квалифицирани удостоверения за уебсайт;
- Издаване и управление на квалифициран електронен времеви печат;
- Валидиране на електронни подписи и печати и др.

Евротръст предоставя услугите, следвайки общоприетите препоръки, спецификации и стандарти. За тези услуги, Евротръст публикува отделно общи условия, които са неразривно свързани с договорни отношения. Политиките и практиките, свързани с предоставяните услуги се отнасят за всички участници в инфраструктурата на публичния ключ на Евротръст по целия свят, включително, удостоверяващи органи, регистриращи органи, търговски агенти, клиенти, крайни потребители и всички доверяващи се страни.

Удостоверителните услуги се предоставят в съответствие с Интегрираната система за управление, прилагана от Евротръст, която включва изискванията на ISO 9001, ISO 27001, ISO 22301, ISO 20000-1, Регламент (ЕС) № 910/2014 г., Регламент (ЕС) 2016/679 (GDPR), Директива (ЕС) 2015/2366 (PSD2) и приложимото законодателство в Република България.

### 2.1. ВЪТРЕШНА ОРГАНИЗАЦИЯ

Евротръст осъществява своята дейност чрез удостоверяващи и регистриращи органи в съответствие с приети политики и практики. Информация за контакт с удостоверяващите и регистриращи органи е на разположение на сайта на Евротръст.

За постигане на надеждност и сигурност в дейността по предоставяне на удостоверителни услуги Евротръст прилага изискванията, посочени в ETSI EN 319 401, в това

число:

- Евротръст гарантира висока сигурност и надеждност на своята дейност;
- Практиките на удостоверителните услуги, които Евротръст прилага, са недискриминационни;
- Услугите са достъпни за всички лица, чиито дейности попадат в декларираната сфера на дейност и които са съгласни да спазват задълженията си, както е посочено в общите условия на Евротръст;
- Евротръст сключва всяка година подходяща застраховка, в съответствие с приложимото право, за покриване на задължения, произтичащи от нейните дейности и в съответствие с член 13 от Регламент (ЕС) № 910/2014 г.;
- Евротръст има финансова стабилност и ресурси, необходими за работа в съответствие с настоящия документ;
- В документа „Практика при предоставяне на квалифицирани удостоверителни услуги" се съдържа процедура за разрешаване на жалби и спорове, получени от потребители или доверяващи се страни относно предоставянето на услугите или други свързани с тях въпроси;
- Евротръст има документирано споразумение и договорни отношения с трети лица, на които предоставя подизпълнение на услуги, аутсорсинг или други дейности.

### 2.1.1. НАДЕЖДНОСТ НА ОРГАНИЗАЦИЯТА

Задълженията и отговорността на потребителите и Евротръст се уреждат чрез договорни споразумения. Отношенията с доверяващи се страни се уреждат по реда на общото деликтно право.

Договорите за предоставяне на удостоверителна услуга следва да бъдат сключвани в писмена или електронна форма, при спазване на разпоредбите на Регламент (ЕС) № 910/2014, Регламент (ЕС) 2016/679 и приложимото законодателство в Република България. Конфликтните задължения и областите на отговорност се разделят, за да се намалят възможностите за неправомерно или непреднамерено изменение или злоупотреба с активите на TSP.

Квалифицираният орган за валидиране „Evrotrust Qualified Validation Service" на

Евротръст осъществява функциите си в съответствие с изисквания, определени в Регламент (ЕС) № 910/2014 г. Изискванията определят техническите и организационни условия в дейността на Евротръст, политиките за квалифицирано валидиране и техническите изисквания.

Когато Евротръст използва външни организации за поддържка на услуги или техни компоненти, те следват изискванията по настоящия документ.

Евротръст гарантира, че:

- използва оперативни процедури и такива за управление на сигурността, които изключват всякаква възможност за манипулиране на резултата/доклада от валидирането;
- проверява валидността на електронни подписи/печати, използвани в съответствие с изискванията на Регламент (ЕС) № 910/2014;
- „Evrotrust Qualified Validation Service" проверява валидността на подписите/печатите в съответствие с ETSI TS 119 441 Electronic Signatures and Infrastructures (ESI); Policy requirements for TSP providing signature validation services.

**Задълженията, отговорността и гаранциите на участниците в процеса по предоставяне на услуга за квалифицирано валидиране са описани в документа „Практика при предоставяне на квалифицирани удостоверителни услуги".*

### 2.1.2. РАЗДЕЛЯНЕ НА ЗАДЪЛЖЕНИЯТА

**Задълженията на Евротръст, потребителите и доверяващата се страна са описани в документа „Практика при предоставяне на квалифицирани удостоверителни услуги".*

## 2.2. ЧОВЕШКИ РЕСУРСИ

Евротръст прилага изискванията, посочени в точка 7.2 от ETSI EN 319 401.

- Евротръст гарантира, че служителите и изпълнителите спазват изискванията за надеждност на дейността;
- Евротръст наема служители и, ако е приложимо, подизпълнители, които притежават необходимите експертни знания, надеждност, опит и квалификация, и които са

преминали обучение относно сигурността и правилата за защита на личните данни, подходящи за дейността, която извършват;

- Служителите на Евротръст преминават периодично (поне на всеки 12 месеца) през обучение за повишаване на своите експертни знания, опит и квалификация, Обученията включват обучения по информационна сигурност, потенциални заплахи и добри практики за сигурност;
- На служителите, които нарушават политиките на Евротръст, се прилагат подходящи дисциплинарни санкции;
- Ролите и отговорностите по информационна сигурност са документирани в длъжностни характеристики;
- Евротръст определя надеждни роли, от които зависи сигурността на дейността по предоставяне на услуга за валидиране на подписи/печати;
- Ръководството но Евротръст определя отговорностите на доверените роли;
- Доверените роли се одобряват и приемат от ръководството;
- Служителите на Евротръст (както временен, така и постоянен) имат длъжностни характеристики, определени от гледна точка на ролите, които изпълняват с разделяне на задълженията и най-малко привилегии, с определяне на чувствителността на позицията въз основа на задълженията и нивата на достъп, квалификация и диплома;
- В длъжностните характеристики се включват изисквания за умения и опит и в тях се разграничават общите и специфични задължения;
- Служителите упражняват административни и управленски процедури и процеси, които са част от процедурите за управление на информационната сигурност на Евротръст;
- Ръководството притежава знания по отношение на предоставените удостоверителни услуги, познание на процедурите за сигурност, опит в областта на информационната сигурност и оценка на риска, достатъчни за изпълнение на управленски функции;
- Всички служители на Евротръст, които имат доверени роли са свободни от конфликт на интереси, който би могъл да засегне безпристрастност на дейността на Евротръст;
- Доверените роли включват следните отговорности:

а) Служители по сигурността - цялостна отговорност за администриране на прилагането на практиките за сигурност;

б) Системни администратори - инсталират, конфигурират и поддържат надеждните системи на Евротръст и управлението на услугите. Това включва възстановяване на системата;

в) Системни оператори - отговорни за ежедневната работа на надеждните системи на Евротръст. Упълномощени са да изпълняват системно архивиране;

г) Системни одитори - упълномощени са да преглеждат и одитират архивите и журналите на надеждните системи на Евротръст.

д) Допълнителни роли – в Евротръст има служители, които изпълняват доверени роли за конкретни услуги за доверие.

- Персоналът на Евротръст се назначава на доверени роли от висшето ръководство на принципа на „най-малка привилегия“ при достъп или при конфигуриране на привилегии за достъп;
- На персонала не се дава достъп до доверени функции, докато не бъдат извършени необходимите проверки. Евротръст изисква от свидетелство за съдимост.

## 2.3. УПРАВЛЕНИЕ НА АКТИВИТЕ

### 2.3.1. ОБЩИ ИЗИСКВАНИЯ

Евротръст прилага изискванията, посочени в т. 7.3 на ETSI EN 319 401. Евротръст осигурява високо ниво на защита на своите активи, включително и на информационните активи. Евротръст поддържа инвентаризация на всички информационни активи и ги класифицира в съответствие с оценката на риска.

Договорът за услугата, статусът за проверка на подписа и доклада за валидиране на подписа са свързани с практиките, политиките и договорености за съответствие на други доставчици на услуги, които не са под контрола на QSVSP. В този случай може да има забавяне на предоставяне на информация за статус на отмяна на удостоверение и да се наложи потребителят да изчака следващия CRL, за да се гарантира, че е било обработено всяко съответно искане за отмяна.

Общите условия са за политика с OID:1.3.6.1.4.1.47272.2.9.

Правата, задълженията и отговорностите на участниците в услугата са описани в документа „Общи условия на договора за предоставяни удостоверителни, информационни, криптографски и консултантски услуги", който е неразделна част от настоящия документ.

Евротръст предоставя приложимата политика при ниво на обслужване SLA: Услугата е достъпна през уеб сайта на Евротръст за лично ползване с нетърговска цел, без ангажимент от страна на Евротръст за нейното ниво на обслужване. За да се използва услугата със съответното ниво на обслужване или автоматизирано, е необходимо клиентът да се обърнете към Евротръст за уреждане на отношенията с договор, в който се уточняват предлаганото ниво на обслужване SLA.

Услугата поддържа следните опции:

а) Услугата позволява на потребителя да избере:

- обекта на подписаните данни (SDO) и документа на подписалия (SD).

б) Услугата може да позволи на потребителя да осигури допълнителни данни за процеса на валидиране:

- удостоверенията, които трябва да се използват за валидиране, напр. за случая, когато атрибутите на SDO не съдържат необходимите удостоверения;
- конкретният подпис, който трябва да бъде проверен в случай, че SDO съдържа множество подписи, и
- политиката за имплицитно или изрично валидиране на подписа, която да се използва сред наличните такива.

в) Евротръст поддържа формати на подпис, определени в ETSI EN 319 122-1 и ETSI EN 319 122-2 или в ETSI EN 319 132-1 и ETSI EN 319 132-2 или в ETSI EN 319 142-1 и ETSI EN 319 142-2.

Поддържани формати с базов профил на електронен подпис/печат:

- ETSI TS 103 171 Electronic Signatures and Infrastructures (ESI) - XadES Baseline Profile
- ETSI TS 103 173 Electronic Signatures and Infrastructures (ESI) - CadES Baseline Profile
- ETSI TS 103 172 Electronic Signatures and Infrastructures (ESI) – PadES Baseline Profile

- ETSI TS 103 174 Electronic Signatures and Infrastructures (ESI) – AsiC Baseline Profile

В допълнение Евротръст валидира горепосочените формати, но с разширен профил и нива:

- ETSI TS 103 171 Electronic Signatures and Infrastructures (ESI) – XadES-T/TL Level;
- ETSI TS 103 173 Electronic Signatures and Infrastructures (ESI) – CadES T/TL Level;
- ETSI TS 103 172 Electronic Signatures and Infrastructures (ESI) PadES T/TL Level;
- ETSI TS 103 174 Electronic Signatures and Infrastructures (ESI) AsiC T/TL Level.

Услугата за валидиране на Евротръст валидира следните типови формати за електронен подпис/печат:

- Обхващащ (Attached - Enveloped) – електронния подпис/печат обхваща подписания обект;
- Обхванат (Attached - Envelopeing) – подписания обект обхваща електронния подпис/печат;
- Отделен (Detached) – електронния подпис/печат е извън подписания обект – в отделен файл/обект;
- Един документ е електронно подписан с повече от един електронен подпис/печат.

Услугата успешно валидира електронни подписи/печати с изтекли или остарели елементи, като например удостоверения с изтекъл срок на валидност или времеви печати, като съобразява проверката с удостоверената дата и час на момента на полагане на електронния подпис/печат. Ако не е удостоверено такова време, проверката се прави към настоящия момент и ако валидността на елементите е изтекла, това прави подписа невалиден, което се отбелязва в доклада. Когато са използвани прекратени удостоверения, услугата проверява дали към момента на подписване те са били валидни и ако не, услугата отбелязва в доклада подписа като невалиден. Ако е бил използван алгоритъм извън приложимия му срок, услугата отбелязва в доклада като невалиден електронен подпис/печат по тази причина.

Евротръст използва криптографските алгоритми в съответствие с ETSI TS 119 312, като тази информация се дава чрез позоваване на съответния алгоритъм за валидиране (ETSI TS 119 102-1).

- SVS избира ограниченията за валидиране, когато клиентът предоставя конфликтна индикация, която противоречи практиката на QSVSP;
- QSVSP задава ограниченията за валидиране, когато политиката за проверка на подписа, предоставена от клиента не позволява;
- QSVSP посочва в своята практика как действа, когато не е възможно да се обработят ограниченията, подадени от клиента;
- QSVSP определя в своята практика при какви условия Политиката за проверка на подписа, може да бъде игнорирана и заменена с правила за валидиране на подписа, в съответствие с протокола, посочен в ETSI TS 119 442, който поддържа различни възможности;
- Политиката на SVS посочват какво се счита за (PoE) доказване за наличие на подпис.

### 2.3.2. РАБОТА С НОСИТЕЛИ

Всички носители се съхраняват сигурно в съответствие с изискванията на класификацията на информацията схема. Архивите, съдържащи чувствителни данни, се унищожават сигурно, когато вече не са необходими.

**Процедурата по архивиране е описана в документа „Практика при предоставяне на квалифицирани удостоверителни услуги"*

## 2.4. КОНТРОЛ НА ДОСТЪПА

Инфраструктурата на Евротръст е физически и логически обособена и не се използва при други дейности, които „Евротръст Технолъджис" АД осъществява. Мерките, предприети по отношение на физическата защита на Евротръст са елемент от разработената и внедрена в Евротръст Система за информационна сигурност, съответстваща на изискванията на

стандартите ISO/IEC 27001, ISO 9001, ISO 22301, и ISO/IEC 20000-1. Евротръст осигурява физическа защита и контрол на достъпа на помещенията, където има инсталирани критични компоненти в неговата инфраструктура.

За осъществяване на контрола на достъп Евротръст прилагат се изискванията, посочени в т. 7.4 на ETSI EN 319 401 и по-специално:

- Системата за достъп е ограничена до оторизирани лица;
- Контролите (например защитни стени) защитават вътрешните мрежови домейни на Евротръст от неоторизирани достъп, включително на достъп от потребители и трети страни;
- Защитните стени са конфигурирани така, че да не се изискват всички протоколи и достъп за функциониране на Евротръст;
- Евротръст администрира потребителския достъп от оператори, администратори и системни одитори;
- Администрацията включва управление на потребителски акаунти и своевременна промяна или премахване достъп;
- Достъпът до информация и дейностите на технологичната система е ограничен в съответствие с политика за контрол на достъпа;
- Системата на Евротръст осигурява достатъчен контрол на компютърната сигурност. За тази цел е извършено разделяне на функциите по администриране и управление на сигурността. Използването на каналите за комуникация на системите се ограничава и контролира;
- Персоналът на Евротръст се идентифицира и удостоверява преди използването на критични приложения, свързани с услугата;
- Персоналът на Евротръст носи отговорност за своите дейности. За тази цел се наблюдават и запазват регистрите на събитията;
- Чувствителните данни са защитени срещу разкриване чрез съхранение и ограничаване на достъпа до тях за неоторизирани потребители.

## 2.5. КРИПТОГРАФСКИ КОНТРОЛИ

Евротръст прилага изискванията за криптографски контроли, посочени в т. 7.5 на ETSI

EN 319 401. Освен тях Евротръст прилага и следните специфични изисквания:

- QSVSP подписва докладите за валидирани с удостоверение за подписване, издадено от удостоверяващия орган, в съответствие с ETSI EN 319 411-1 или ETSI EN 319 411-2;
- Частният ключ на QSVSP за подписване на докладите за валидиране се съхранява и използва в криптографски модул (хардуерна криптосистема/HSM/Hardware Security Module) с ниво на сигурност FIPS 140-2 Level 3 или по-високо, съответно CC EAL 4+ или по-високо.

## 2.6. ФИЗИЧЕСКАТА И ОРГАНИЗАЦИОННА СИГУРНОСТ

Евротръст прилага изискванията на т.7.6 от ETSI EN 319 401 относно физическата и организационна сигурност. В допълнение прилага за SVA следното специфично изискване на точка 5.2, GSM 1.4 от ETSI TS 119 101: Евротръст използва криптографски библиотеки, тествани спрямо съответния стандарт.

**Процедурите по изпълнение на общите изисквания по отношение на физическата и организационна сигурност са описани в документа „Практиката при предоставяне на квалифицирани удостоверителни услуги".*

## 2.7. СИГУРНОСТ НА ДЕЙНОСТТА

За сигурност на дейността си Евротръст прилага изискванията, посочени в точка 7.7 на ETSI EN 319 401. Евротръст използва надеждни системи и продукти, които са защитени срещу модификации и гарантират техническата сигурност и надеждност на поддържаните от тях процеси.

**Евротръст използва процедури за управление на информационната сигурност на цялата инфраструктура на Евротръст в съответствие с общоприети в международната практика стандарти, които са описани в документа „Практиката при предоставяне на квалифицирани удостоверителни услуги".*

- Евротръст извършва анализ на изискванията за сигурност при проектирането на нови системи и нови услуги, за да гарантира тяхната сигурност;
- Прилага процедурите за контрол на промените в софтуера и конфигурацията на технологичните системи;
- Процедурите за контрол на промените включват тяхното документиране;
- Целостта на системите и информацията на Евротръст е защитена срещу вируси, злонамерен и неоторизиран софтуер;
- Средствата, използвани в системите на Евротръст, са безопасно обработени, за да се предпазят архивите от повреда, кражба, неоторизиран достъп и остаряване;
- Процедурите за управление на архивите се предпазват от морално остаряване и влошаване на тяхното състояние в рамките на срока, в който се изисква съхраняването на записите;
- Процедурите се прилагат от всички доверителни и административни роли, които участват в предоставянето на услуги;
- Евротръст разработва и прилага процедури за гарантиране, че:

а) защитните „пачове“ се прилагат в рамките на разумен период от време, след което те стават достъпни;

б) защитните „пачове“ не се прилагат, ако има опасност да доведат до допълнителни уязвимости или нестабилности, които надвишават ползите от прилагането им;

в) документират се причините, поради които не се прилагат защитните „пачове“.

В допълнение се прилагат следните специфични изисквания за сигурност на дейността:

- Евротръст използва най-новата и актуална среда за приложения (управлявана софтуерна среда);
- Използват се положително тествани и преразгледани реализации на стандартизирани протоколи и библиотеки;
- SCA / SVA / SAA поддържа целостта и поверителността на цялата информация, предоставена от потребител и на всякакви данни, предавани между приложението и потребителя, дори в случай на приложение с публично достъпна среда.

### 2.7.1. ПОЛИТИКА ЗА ИНФОРМАЦИОННА СИГУРНОСТ

Евротръст има разработена и одобрена от ръководството Политика за информационна сигурност, съобразена с изискванията на точка 6.3 на ETSI EN 319 401:

- Политиката определя подхода на Евротръст за управление на дейността си по информационна сигурност;
- Промените в политиката за информационна сигурност се съобщават на трети страни (потребители, доверяващи се страни, надзорни и други регулаторни органи, органи за оценяване на съответствието), когато е приложимо;
- Политиката за информационна сигурност на Евротръст е документирана, внедрена и поддържана в актуално състояние;
- Всички служители на Евротръст са запознати с Политиката за информационна сигурност;
- Евротръст носи отговорност за спазването на процедурите в Политиката за информационна сигурност в случаи, когато е възложител на подизпълнители част от своите дейности. При наличие на подизпълнители, Евротръст определя тяхната отговорност и гарантира, че те прилагат стриктно всички контроли по информационна сигурност, изисквани от Евротръст;
- Политиката за информационна сигурност на Евротръст и инвентаризацията на активите за информационна сигурност се преразглеждат в планирани интервали от време или ако настъпят значителни промени, за да се гарантира тяхната пригодност, адекватност и ефективност;
- Всички промени, които могат да окажат влияние върху нивото на предоставената информационна сигурност, се одобряват от орган за управление на информационната сигурност;
- Конфигурацията на системите на Евротръст се проверяват редовно за промени, които могат да нарушат правилата за информационна сигурност. Максималният интервал между две проверки е съгласно вътрешните процедури на Евротръст.

В допълнение се прилагат следните специфични изисквания:

Политиката за сигурност документира контролите за сигурност и

неприкосновеността на личните данни. Личните данни, предоставени на Евротръст се съхраняват и обработват в съответствие със Закона за защита на личните данни и РЕГЛАМЕНТ (ЕС) 2016/679 General Data Protection Regulation (GDPR). Евротръст събира количество информация пропорционално на нейното предназначение и употреба. Всеки потребител дава съгласие за обработването на личните му данни. Това съгласие се заявява с подписването на Договор за удостоверителни услуги. Личните данни се използват само във връзка с предоставянето на конкретната удостоверителна услуга. Личните данни са защитени в съответствие с правилата за поверителност, съдържащи се в политиката за сигурност на Евротръст.

## 2.8. МРЕЖОВА СИГУРНОСТ

Евротръст прилагат изискванията, определени в точка 7.8 на ETSI EN 319 401.

**Евротръст гарантира мрежовата сигурност на системите срещу външни интервенции и заплахи като използва процедури описани в документа „Практиката при предоставяне на квалифицирани удостоверителни услуги“.*

В допълнение Евротръст прилага следните специфични изисквания:

- В случай, че е позволен отдалечен достъп до системи, съхраняващи или обработващи поверителни данни, се следва политика да бъдат документирани контролите за сигурност и поверителност, реализирани с цел защита на личните данни.
- В случай, че е позволен отдалечен достъп до системи, съхраняващи или обработващи поверителни данни са предприети мерки за защита срещу рисковете от отдалечен достъп. ЗАБЕЛЕЖКА: Тази поверителна информация може да бъде информация, свързана с клиента (като предпочитания), или подписани данни, които биха могли да се съхранява в очакване на по-нататъшна обработка (напр. ако данните за състоянието на анулирането не са налице).

## 2.9. УПРАВЛЕНИЕ НА ИНЦИДЕНТИ

### 2.9.1. 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.

Евротръст прилага изискванията, посочени в точка 5 на ETSI EN 319 401 за оценка на риска:

- Евротръст извършва оценка на риска, за да идентифицира, анализира и оцени рисковете, свързани с бизнеса и технически проблеми с предоставяната удостоверителна услуга;
- Евротръст избира подходящи мерки за третиране на риска, като взема предвид резултатите от оценката на риска. Мерките за третиране на риска гарантират, че нивото на сигурност е съизмеримо със степента на риска;
- Евротръст определя всички изисквания за сигурност и оперативни процедури, които са необходими да изпълнят избраните мерки за третиране на риска, както е документирано в политиката за информационна сигурност и в практиката;
- Оценката на риска се преразглежда периодично;
- Ръководството на Евротръст одобрява оценката на риска и приема установения остатъчен риск.

### 2.9.2. УПРАВЛЕНИЕ НА ИНЦИДЕНТИ

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.

**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.*

За управление на инциденти Евротръст прилага процедури, които изпълняват изискванията, посочени в точка 7.9 на ETSI EN 319 401:

- Евротръст наблюдава всички дейности, свързани с достъпа до и използване на информационните системи и до заявките за услуги;
- В следствие на мониторинга се отчита и анализира чувствителността на всяка събрана информация;
- Анормални системни дейности, които показват потенциално нарушение на сигурността, включително проникване в системата и мрежата на Евротръст, се откриват и докладват като аларми;
- Евротръст наблюдава следните събития:

  а) включване и изключване на функциите за логове; и

  б) наличност и използване на необходимите услуги в мрежата на Евротръст.
- Евротръст действа своевременно и координирано, за да реагира бързо на инциденти

и да ограничи въздействието на нарушенията на сигурността;
- Евротръст назначава доверени служители, които да следят за сигнали с потенциално критични събития и да се гарантира, че съответните инциденти се докладват в съответствие с установените вътрешни процедури;
- Евротръст е установил процедури за уведомяване на съответните компетентни органи в съответствие с приложимите регулаторни правила за всяко нарушение на сигурността или загуба на интегритет, което има значително въздействие върху удостоверителната услуга и личните данни, в рамките на 24 часа от идентифицирането на нарушението;
- Когато нарушаването на сигурността или загубата на интегритет може да повлияе неблагоприятно на физическо или юридическо лице, на което е предоставена удостоверителна услуга, Евротръст уведомява същото физическо или юридическо лице за нарушение на сигурността или за загуба на интегритет без излишно забавяне;
- Системите на Евротръст се наблюдават регулярно за идентифициране на доказателства за злонамерена дейност, като се прилагат автоматични механизми за обработка на регистрационните журнали, а служителите се предупреждават за възможни

критични събития, свързани със сигурността;

- Евротръст обявява всяка критична уязвимост, която преди това не е била обявявана от него, в рамките на период от 48 часа след откриването ѝ;
- За всяка уязвимост, предвид потенциалното ѝ въздействие, Евротръст:
  - създава и прилага план за смекчаване на уязвимостта; или
  - документира с доказателства, че уязвимостта не изисква смекчаване, например ако разходите за потенциалното ѝ въздействие не оправдават разходите за нейното смекчаване;
- Процедурите за докладване и реагиране на инциденти се използват по такъв начин, че вредите от инцидентите със сигурността и неизправностите в системите са сведени до минимум.

## 2.10. СЪБИРАНЕ НА ДОКАЗАТЕЛСТВА

При събиране на доказателства, Евротръст прилага изискванията, посочени в точка 7.10 на ETSI EN 319 401:

- Евротръст записва и поддържа достъпа за подходящ период от време, включително за след преустановяване на дейността си, до цялата информация относно данните, издадени и получени по време на дейността си, с цел предоставяне на доказателства в съдебни производства и с цел осигуряване на непрекъснатост на услугата;
- Запазва поверителността и целостта на текущите и архивирани записи относно работата на услугите;
- Документи, касаещи функционирането на услугите, се архивират изцяло и поверително в съответствие с добрите бизнес практики;
- Документи, отнасящи се до експлоатацията на услугите, се предоставят, ако се изискват с цел предоставяне на доказателства за правилното функциониране на услугите за целите на съдебното производство;
- Записва се точното време на значимите за управление на дейността събития, като управление на ключовете и синхронизация на часовник;
- Времето, използвано за записване на събития, както се изисква в дневника на одита, се синхронизира с UTC на поне веднъж на ден;

- Записите, отнасящи се до услугите, се съхраняват за определен период от време, който е подходящ за предоставяне необходимите правни доказателства и както е записано в Общите условия и договор;
- Събитията се регистрират по начин, който не може лесно да бъде изтрит или унищожен, освен ако са надеждно прехвърлени към дългосрочни архиви в рамките на срока, в който те трябва да бъдат държани.

В допълнение Евротръст прилага следните специфични изисквания:

- QSVSP трябва да въведе регистри на събитията, за да съхрани информацията, необходима за по-късни доказателства;
- Всяко валидиране на подписа се регистрира, евентуално заедно с идентификацията на потребителя, когато тази информация е известна. Стандартно, Евротръст не регистрира самоличността на потребителя;
- Протоколите от събития се маркират с времеви печат;
- Архивираните данни (на хартия и в електронен вид) се съхраняват за период от минимум 10 години. След изтичане на този период на съхранение, архивираните данни се унищожават;
- Дневникът за събития включва типа на събитието, успеха или неуспеха на събитието и идентификатор на лице и / или компонент в началото на такова събитие.

**Допълнителна информация относно архивните данни и събиране на доказателства има описана в документа „Практика при предоставяне на квалифицирани услуги".*

## 2.11. УПРАВЛЕНИЕ НА НЕПРЕКЪСНАТОСТТА НА БИЗНЕСА

При управление на непрекъснатостта на бизнеса Евротръст прилага изискванията, посочени в точка 7.11 на ETSI EN 319 401:

- Евротръст е създал и поддържа план за непрекъснатост, който да се прилага в случай на бедствие;
- В случай на бедствие, отказ на критични компоненти на технологичната система, включително хардуер и софтуер, компрометиране на частен ключ за подписване или компрометиране  други ключове операциите се възстановяват в рамките на

закъснението, установено в плана за непрекъснатост, след като се обърне внимание на причината за бедствието, за да се избегне нейното повтаряне.

За да се осигури непрекъснатост на бизнеса се прилагат допълнителни специфични за услугата изисквания:

- В плана за непрекъснатост на бизнеса, плана за възстановяване след бедствие и т.н. се описват процедури, посредством които се полагат всички разумни усилия за поддържане на услугата в съответствие с нивото на обслужване (SLA), както и необходимите технически и организационни предпазни мерки, за да се гарантира това привеждане в съответствие.
- Следва да се прилагат мерки, за да се избегне прекъсване от трети страни или неумишлено прекъсване от страна на потребителя.
- Когато докладите за валидиране са цифрово подписани и се очаква те да бъдат валидирани в дългосрочен план, QSVSP подписва с удостоверение за електронен печат, издадено от удостоверяващ орган, който предоставя гаранции за наличието на информация за статуса на неговите удостоверения, както и че има план за прекратяване на дейността си;
- Когато докладите за валидиране са цифрово подписани и се очаква да бъдат валидирани в дългосрочен план QSVSP избира надежден източник за доказване на съществуването си. В случая Евротръст използва квалифициран орган за времеви печат.

**Подробно описание на възможните причини за възникване на аварии и прилагане на план за непрекъснатост се намира в документа „Практика при предоставяне на квалифицирани удостоверителни услуги“*

## 2.12. ПЛАНОВЕ ЗА ПРЕКРАТЯВАНЕ НА ДЕЙНОСТТА НА ЕВРОТРЪСТ

Задълженията, описани по-долу, са разработени, за да минимизират прекъсванията в дейността на потребителите и доверяващите се страни, произтичащи от решението на Евротръст да преустанови дейността си. В плановете за прекратяване на дейността Евротръст прилага описание на процедурата по изпълнение на изискванията, посочени в точка 7.12 на ETSI EN 319 401:

- В резултат на прекратяване на услугите на Евротръст потенциалните смущения

на потребителите и доверяващите се страни се свеждат до минимум, и по-специално продължаване на поддържането на информацията, необходима за проверка на валидността на удостоверителните услуги;

➢ Евротръст актуализира периодично плана за прекратяване. Преди Евротръст да прекрати услугите си, се прилагат най-малко следните процедури:

- Евротръст информира за прекратяване на дейността си всички потребители и други заинтересовани лица, с които има споразумения или друга форма на взаимоотношения, в това число доверяващите се страни, съответните компетентни органи, като например надзорните органи;
- Преди да прекрати услугите си, Евротръст прекратява разрешението на всички подизпълнители да действат от негово име при изпълнението на всякакви функции, свързани с процеса на издаване на удостоверения/токени и/или доклади на удостоверителни услуги;
- Преди да прекрати услугите си, Евротръст прехвърля задълженията си на надеждна страна за поддържане на цялата информация, необходима за предоставяне на доказателства за функционирането на услугите за разумен срок, освен ако може да се докаже, че Евротръст не разполага с такава информация;
- Преди да прекрати услугите си, частните ключове на Евротръст, включително резервните копия, се унищожават или изтеглят от употреба по такъв начин, че личните ключове да не могат да бъдат извлечени;
- Преди да прекрати услугите си, когато е възможно, Евротръст прехвърля предоставянето на удостоверителните услуги на своите съществуващи клиенти на друг квалифициран доставчик на удостоверителни услуги;

➢ Евротръст има договореност за покриване на разходите за изпълнение на минималните изисквания в случай, че настъпи банкрут или поради други причини не е в състояние да покрие разходите сам, доколкото е възможно в рамките на приложимото законодателство;

➢ Евротръст поддържа или прехвърля на надеждна страна задълженията си за предоставяне на ключовете или токените за удостоверителната услуга на доверяващите се страни за разумен период от време.

**Плановете и процедурите за прекратяване на дейността на Евротръст са описани в документа „Практика при предоставяне на квалифицирани удостоверителни услуги".*

## 2.13. СЪОТВЕТСТВИЕ

За съответствие със законовите изисквания Евротръст прилага изискванията, посочени в точка 7.13 на ETSI EN 319 401:

- Евротръст гарантира, че функционира по законен и надежден начин;
- Предоставя доказателства за това как отговаря на приложимите законови изисквания;
- Удостоверителните услуги и продуктите за крайните потребители, използвани при предоставянето на тези услуги, са достъпни за хората с увреждания, когато е възможно;
- Взима в предвид в своята дейност приложими стандарти, като ETSI EN 301 549 Accessibility requirements suitable for public procurement of ICT products and services in Europe;
- Предприема подходящи технически и организационни мерки срещу неоторизирана или неправомерна обработка на лични данни и срещу случайна загуба, унищожаване или повреждане на лични данни. Евротръст гарантира, че личните данни се обработват в съответствие с Регламент (ЕС) 2016/679. В това отношение, за да предостави достъп до услуга онлайн обработва само тези идентификационни данни, които са адекватни, релевантни, а не прекомерно.

В допълнение се прилагат следните специфични изисквания:

- Когато личните данни се обработват от трета страна, Евротръст сключва подходящо споразумение за обработващ лични данни, за да гарантира, че той отговаря на изискванията, посочени в практиката на QSVSP и условията, включително по отношение на прилагането на технически, организационни и правни мерки за защита на личните данни (както подписаните данни, така и подписа могат да съдържат лични данни);
- QSVSP не съхранява подписания документ (SD/Signer's Document) след обработка, когато не е необходимо. Ако услугата за валидиране работи в комбинация с услуга за дългосрочно съхраняване, може да е необходимо да се съхраняват такива данни;

- QSVSP носи цялата отговорност за изпълнението на посочените по-горе изисквания, когато някои или всички негови функционалности се изпълняват от подизпълнители.

Услугата се изпълнява е съответствие с изискванията за квалифицирано валидиране на квалифицирани електронни подписи на Регламент (ЕС) № 910/2014 (eIDAS: чл. 32 и 33) и печати (eIDAS: чл. 40)

| **Изисквания в чл. 32, 33 и 40 от Регламент (ЕС) № 910/2014** | **Изпълнение от услугата** |
|---|---|
| ***Чл. 32 Изисквания към валидирането на квалифицирани електронни подписи*** | |
| 1. В процеса на валидиране на квалифициран електронен подпис се потвърждава валидността на квалифицирания електронен подпис, при условие че:<br>а) удостоверението в подкрепа на подписа към момента на подписването е било квалифицирано удостоверение за електронен подпис, отговарящо на приложение I; | Процесът по квалифицирано валидиране на електронни подписи изпълнява изискванията на ЕС за доставчик на квалифицирани удостоверителни услуги, който издава квалифицирани удостоверения за електронен подпис и електронен печат. |
| б) квалифицираното удостоверение е издадено от доставчик на квалифицирани удостоверителни услуги и е било валидно към момента на подписването; | Процесът по квалифицирано валидиране на електронни подписи изпълнява изискванията на ЕС за доставчик на квалифицирани удостоверителни услуги, който издава квалифицирани удостоверения за електронен подпис и електронен печат. |
| в) данните за валидиране на подписа съответстват на данните, предоставени от доверяващата се страна; | Гарантира се чрез поддържаните формати за електронен подпис/печат. |

| | |
|---|---|
| г) уникалният набор от данни, представляващи титуляря на електронния подпис в удостоверението, е надлежно предаден на доверяващата се страна; | Услугата автоматизирано създава доклад за валидиране в който са вписани данните от използваните за подписване на документа удостоверения за електронен подпис/печат, които тя е надлежно валидирала. |
| д) ако към момента на подписването е бил използван псевдоним, то това е ясно указано на доверяващата се страна; | Псевдонима се вписва в специален атрибут в полето Subject и така се гарантира, че има ясно указано на доверяващата се страна за този факт. |
| е) електронният подпис е създаден от устройство за създаване на квалифициран електронен подпис; | Прави се специална проверка дали електронният подпис е създаден от устройство за създаване на квалифициран електронен подпис (SSCD за QSign/QSeal). |
| ж) целостта на подписаните данни не е застрашена; | Гарантира се чрез описаната в настоящата политика методика на проверка и валидиране на електронно подписните документи. |
| з) изискванията по член 26 са били изпълнени към момента на подписването. | Услугата извършва проверки, че положения усъвършенстван електронен подпис отговаря на изискванията за свързаност по уникален начин с титуляря на подписа,<br>идентифицира титуляря на подписа, създаден е чрез данни за създаване на електронен подпис, които титулярят на електронния подпис може да използва с висока степен на доверие и единствено под свой контрол и е свързан с данните, които са подписани с него, по начин, позволяващ |

| | |
|---|---|
| | да бъде открита всяка последваща промяна в тях. Тези проверки се извършват за всички, поддържани от услугата формати. |
| 2. Използваната за валидиране на квалифицирания електронен подпис система предоставя на доверяващата се страна правилния резултат от процеса на валидиране и ѝ позволява да открие евентуални проблеми, свързани със сигурността. | Гарантира се чрез описаната в настоящата политика и практика методика на проверка и валидиране на електронно подписните документи. |
| ***Член 33 Услуга по квалифицирано валидиране на квалифицирани електронни подписи*** | |
| 1. Услугата по квалифицирано валидиране на квалифицирани електронни подписи може да се предоставя единствено от доставчик на квалифицирани удостоверителни услуги, който:<br>а) извършва валидиране в съответствие с член 32, параграф 1; и | В предходната точка е описано как Услугата изпълнява изискванията на чл.32 |
| б) дава възможност на доверяващите се страни да получат резултата от процеса на валидиране по автоматизиран начин, който е надежден и ефикасен и носи усъвършенстван електронен подпис или усъвършенстван електронен печат на доставчика на услугата по квалифицирано валидиране. | Гарантира се чрез описаната в настоящата политика методика на проверка и валидиране на електронно подписните документи, както и на процеса на получаване на електронно подписания доклад за валидиране. |
| ***Член 40 Валидиране и съхраняване на квалифицирани електронни печати*** | |
| Членове 32, 33 и 34 се прилагат mutatis mutandis към валидирането и съхраняването на квалифицирани | Услугата покрива и валидирането на електронни печати по смисъла на чл.40 |

| | |
|---|---|
| електронни печати. | |

# 3. ДИЗАЙН НА УСЛУГАТА ЗА ВАЛИДИРАНЕ НА ПОДПИСА

## 3.1. ИЗИСКВАНИЯ КЪМ ПРОЦЕСА НА ВАЛИДИРАНЕ

Процесът на валидиране съответства на ETSI TS 119 102-1. QSVSP прилага алгоритъма, посочен в ETSI TS 119 102-1, като позволява алтернативни изпълнения, при условие че те произвеждат същата индикация за основно състояние и дават същия набор от входна информация.

По-специално Евротръст изпълнява следните изисквания:

- Политиката за валидиране на подписа не се ограничава до минималния набор от ограничения, изисквани от точка 5.1.4.1 от ETSI TS 119 102-1;
- Процесът на валидиране извежда за всеки един подпис индикация за статуса на валидиране на подписа и доклад за валидиране на подписа;
- Съгласно алгоритъма, посочен в ETSI TS 119 102-1, статусът на валидиране на подписа може да бъде:

| **Информация вписана в доклада** | | **Семантика** |
|---|---|---|
| **Статус** | **Данни в доклада** | |
| **TOTAL-PASSED** | Процесът на валидиране извежда валидираната удостоверителна верига, включително удостоверението за електронен подпис/печат, използвани в процеса на валидиране. | Процесът на квалифицирано валидиране на електронни подписи и печати е с резултат TOTAL-PASSED поради:<br>• успешни криптографски проверки на електронен подпис/печат (включително проверки на хеш на отделните обекти от данни, подписани косвено);<br>• положително валидирани ограничения, относно удостоверяване на идентичност на подписващия (напр., подписващото удостоверение е валидно); и<br>• успешно валидиран електронен |

| | | |
|---|---|---|
| | | подпис/печат спрямо валидиращи ограничения и по тази причина се приема спрямо тези ограничения. |
| **TOTAL-FAILED** | Процесът на валидиране извежда допълнителна информация, поясняваща статусът TOTAL-FAILED за всяко от ограниченията за валидиране, взети под внимание и за които са настъпили отрицателни резултати. | Процесът на квалифицирано валидиране на електронни подписи и печати е с резултат TOTAL-FAILED защото криптографските проверките на електронен подпис/печат са неуспешни(включително проверките на хеш на отделните обекти на данни, подписани косвено) или е доказано, че генерирането на подписа/печата е след отмяната/прекратяването му. |
| **INDETERMINATE** | Процесът на валидиране извежда допълнителна информация, за да обясни INDETERMINATE индикацията и да помогне на проверяващите да определят липсващите данни, за да завърши процеса на валидиране. | Наличната информация е недостатъчна за процеса на валидиране, за да установи статуса TOTAL-PASSED или TOTAL-FAILED на електронен подпис/печат. |

Освен основния статус, доклада за валидиране на подписа включва и помощен статус със следната семантика:

| **Информация вписана в доклада** | | | **Семантика** |
|---|---|---|---|
| **Основен статус** | **Помощен статус** | **Данни към доклада** | |
| **TOTAL-FAILED** | FORMAT_FAILURE | Процесът на валидиране предоставя отделните факти, довели до налична информация за неуспешната обработка на | Електронният подпис/печат не е съвместим с поддържаните стандарти, посочени в този документ, до степен която не |

| | | | |
|---|---|---|---|
| | | електронен подпис/печат. | позволяваща криптографската проверка да го обработи. |
| | HASH_FAILURE | Процесът на валидиране предоставя идентификатор, който еднозначно идентифицира елемент в обект за подпис/печат, предизвикващ грешката, във формата на удостоверението за електронен подпис/печат. | Процесът на квалифицирано валидиране на електронни подписи и печати води до TOTAL-FAILED, защото най-малко един хеш на обект, участващ в процеса на подписване не съответства на съответния хеш в електронния подпис/печат. |
| | SIG_CRYPTO_FAILURE | Процесът на валидиране предоставя удостоверението за електронен подпис/печат, използвано в процеса на валидиране. | Процесът на квалифицирано валидиране на електронни подписи и печати води до TOTAL- FAILED, защото цифровата стойност на подписа не може да бъде проверена с помощта на публичния ключ от удостоверението за електронен подпис/печат. |
| | REVOKED | Процесът на валидиране предоставя:<br>• Удостоверителната верига, използвана в процеса на валидиране;<br>• Времето и причината, ако има такава, за отмяна/прекратяване на удостоверението на електронен подпис/печат.<br>• CRL, ако има такъв, в който е | Процесът на квалифицирано валидиране на електронни подписи и печати е TOTAL-FAILED, защото:<br>• удостоверението на електронен подпис/печат е отменено; и<br>• има доказателство (PoE), че времето на подписа/печата е след времето на отмяната на удостоверението. |

| | | | |
|---|---|---|---|
| | | установена отмяната / прекратяването. | |
| **INDETERMINATE** | SIG_CONSTRAINTS_FAILURE | Процесът на валидиране предоставя множество причини, довели до неуспешно валидиране. | Процесът на квалифицирано валидиране на електронни подписи и печати е INDETERMINATE, защото един или повече атрибути на електронен подпис/печат не съответстват на ограниченията при валидиране. |
| | CHAIN_CONSTRAINTS_FAILURE | Процесът на валидиране предоставя:<br>• Удостоверителната верига, използвана в процеса на валидиране.<br>• Допълнителна информация относно причината, довела до този резултат. | Процесът на квалифицирано валидиране на електронни подписи и печати е INDETERMINATE, защото удостоверителната верига, използвана в процеса на валидиране не съответства на ограниченията свързани с удостоверението при валидирането. |
| | CERTIFICATE_CHAIN_GENERAL_FAILURE | Процесът на валидиране предоставя допълнителна информация относно причината, довела до този резултат. | Процесът на квалифицирано валидиране на електронни подписи и печати е INDETERMINATE, защото проверката на удостоверителната верига извежда грешка поради неустановена причина |
| | CRYPTO_CONSTRAINTS_FAILURE | Процесът на валидиране предоставя идентификация на електронен подпис/печат или | Процесът на квалифицирано валидиране на електронни подписи и печати е |

| | | | |
|---|---|---|---|
| | | на удостоверение, които са генерирани с алгоритъм или размер на ключа, под необходимото ниво за криптографска сигурност | INDETERMINATE, защото поне един от използваните алгоритми (за електронен подпис/печат или съответстващи удостоверения), които участват във квалифицирано валидиране на електронни подписи и печати или размерът на ключовете, които използват тези алгоритми, е под необходимото ниво за криптографска сигурност, както и:<br>• електронен подпис/печат и/или съответстващи удостоверения са генерирани след момент, до който тези алгоритми/ключове се считат сигурни (ако такова време е известно); и<br>• електронен подпис/печат не е защитен с достатъчно надежден времеви печат, приложен преди времето, до което се смята че алгоритъма/ ключа, са сигурни (ако такова време е известно). |
| | EXPIRED | Процесът на валидиране предоставя данни за валидираната удостоверителна верига. | Процесът на квалифицирано валидиране на електронни подписи и печати е INDETERMINATE, защото |

| | | | |
|---|---|---|---|
| | | | времето на полагане на електронния подпис/печат е след изтичане срока на валидност (notAfter) на удостоверението. |
| | NOT_YET_VALID | - | Процесът на квалифицирано валидиране на електронни подписи и печати е INDETERMINATE, защото времето на полагане на електронния подпис/печат е преди срока на валидност (notBefore) на удостоверението. |
| | POLICY_PROCESSING_ ERROR | Процесът по валидиране предоставя допълнителна информация за причината. | Процесът на квалифицирано валидиране на електронни подписи и печати е INDETERMINATE, защото посоченият формален файл на политиката не може да бъде обработен по някаква причина (не е достъпен, не подлежи на обработка, с грешна контролна сума е, др.). |
| | SIGNATURE_POLICY_NOT_AVAILABLE | - | Процесът на квалифицирано валидиране на електронни подписи и печати е INDETERMINATE, защото не е достъпен документа, описващ използваната политика. |

| | | | |
|---|---|---|---|
| | TIMESTAMP_ORDER_FAILURE | Процесът по валидиране предоставя списък с удостоверения за време, които не отговарят на исканата подредба. | Процесът на квалифицирано валидиране на електронни подписи и печати е INDETERMINATE, защото предоставения списък с удостоверения за време и/или електронно подписани обекти не отговарят на исканата подредбата. |
| | NO_SIGNING_CERTIFICATE_FOUND | - | Процесът на квалифицирано валидиране на електронни подписи и печати е INDETERMINATE, защото удостоверението за електронен подпис/печат не може да бъде идентифицирано. |
| | NO_CERTIFICATE_CHAIN_FOUND | - | Процесът на квалифицирано валидиране на електронни подписи и печати е INDETERMINATE, защото не е намерена удостоверителна верига за идентификация на удостоверението за електронен подпис/печат. |
| | REVOKED_NO_POE | Процесът на валидиране предоставя:<br>•Удостоверителната верига, която се използва в процеса на валидиране.<br>• Времето и причината за отмяната/прекратяване на | Процесът на квалифицирано валидиране на електронни подписи и печати е INDETERMINATE, защото съответстващото удостоверение е отменено/прекратено по |

| | | | |
|---|---|---|---|
| | | удостоверението на електронен подпис/печат. | време на валидирането. Обаче, SVA не може да установи, дали времето на подписа се намира преди или след времето на отмяна/прекратяване |
| | REVOKED_CA_NO_POE | Процесът на валидиране предоставя:<br>•Удостоверителната верига, която включва в себе си прекратения удостоверяващ орган;<br>• Времето и причината за отмяната/прекратяване на удостоверението. | Процесът на квалифицирано валидиране на електронни подписи и печати е INDETERMINATE, защото е открита поне една удостоверителна верига, но използваният удостоверяващ орган е прекратен. |
| | OUT_OF_BOUNDS_NO_POE | - | Процесът на квалифицирано валидиране на електронни подписи и печати е INDETERMINATE, защото удостоверението е с изтекъл срок или все още не е валидно към дата/час на валидиране и SVA не може да определи дали времето на подписа е в интервала на валидност на удостоверението. |
| | CRYPTO_CONSTRAINTS_FAILURE_NO_POE | Процесът на валидиране предоставя:<br>Идентификация на електронен подпис/печат или на съответстващото удостоверение, генерирани с | Процесът на квалифицирано валидиране на електронни подписи и печати е INDETERMINATE, защото най-малко един от алгоритмите, които са били използвани в |

| | | | |
|---|---|---|---|
| | | недопустима дължина на ключа или с алгоритъм, не отговарящи на криптографските изисквания за ниво на сигурност | електронен подпис/печат или в съответстващите удостоверения, участващи при валидиране им или размера на ключа, който се използва с такъв алгоритъм, е под необходимото ниво на криптографска сигурност, както и няма доказателства, че подписа/печата или тези удостоверения са генерирани преди времето, до което този алгоритъм/ключ се е считал за сигурен. |
| | NO_POE | Процесът на валидиране идентифицира само подписи/печати, за които липсват доказателства (POEs). Процесът на валидиране трябва да предостави допълнителна информация по проблема. | Процесът на квалифицирано валидиране на електронни подписи и печати е INDETERMINATE, защото липсва доказателство (PoE), чрез което доказва, че подписът/печатът е бил генериран преди станало известно компрометиращо събитие (напр. разбит алгоритъм). |
| | TRY_LATER | | Процесът на квалифицирано валидиране на електронни подписи и печати е INDETERMINATE, защото не всички ограничения могат да бъдат изпълнени с наличната |

| | | | |
|---|---|---|---|
| | | | информация. Въпреки това, процесът е възможен ако валидирането използва допълнителна информация за отмяната/прекратяването, която ще бъде на разположение на по-късен етап от време. |
| | SIGNED_DATA_NOT_FOUND | Процесът на валидиране предоставя: Идентификаторът (например URI) на данните за подпис/печат, които са причинили грешката. | Процесът на квалифицирано валидиране на електронни подписи и печати е INDETERMINATE, защото данните за подпис/печат не могат да бъдат получени. |
| | GENERIC | Процесът на валидиране предоставя допълнителна информация, която показва защо статуса от валидиране е INDETERMINATE. | Процесът на квалифицирано валидиране на електронни подписи и печати е INDETERMINATE, поради други причини. |

- Евротръст поддържа поне една политика за валидиране на подписи като вход за приложението за валидиране (SVA);
- Услугата за валидиране (SVS) не приема няколко източника на политика за валидиране;
- Политиката за проверка на подписа, не може да бъде игнорирана и заменена с правила за валидиране на подписа, в съответствие с протокола, посочен в ETSI TS 119 442, който поддържа различни възможности;
- Приложението за валидиране (SVA) отговаря на изискванията в точка 7.4 на ETSI TS 119 101 (SIA 1 към SIA 4);
- Процесът на валидиране гарантира, че използваната Политика за валидиране съответства на стратегия, определена в политиката на SVS и/или на Общите условия за

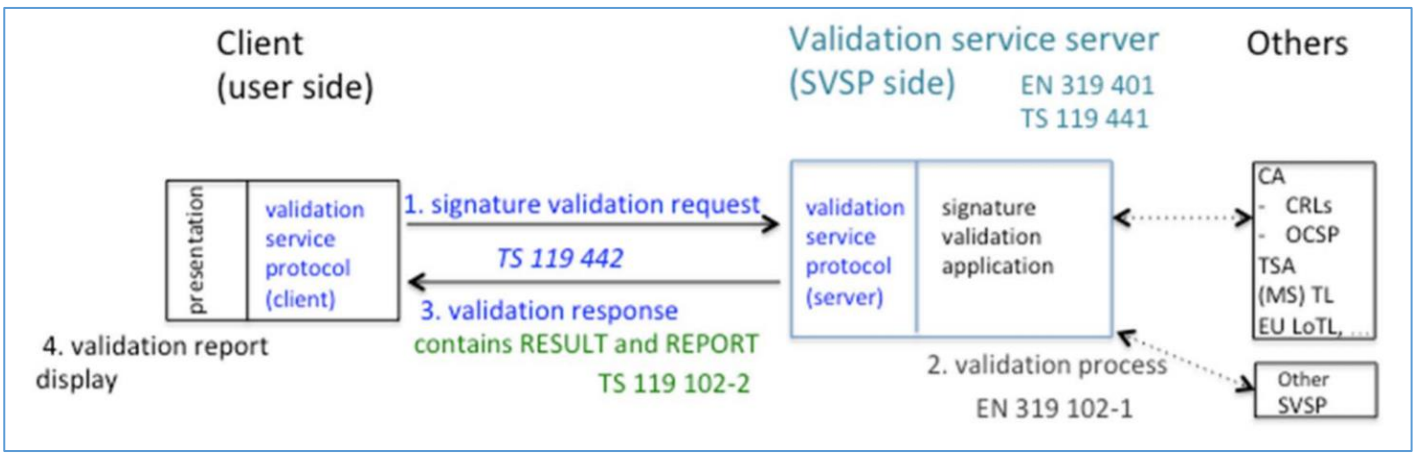
използване на SVS;

- Стратегията, определена в политиката на услугата за валидиране (SVS) и/или на Общите условия за използване на SVS, следва най-малко следните принципи:
- За един и същ вход услугата за валидиране на подписа трябва да има същия изход, като се има предвид, че политиката за валидиране на подписа е част от входа.
- SVS може да приема различни елементи като доказателство за съществуването на подпис.

### 3.1.1. ПРОЦЕС НА ВАЛИДИРАНЕ

В зависимост от използвания формат на електронен подпис/печат, услугата поддържа процеси на валидиране на базови формати/Baseline formats на подпис/печат и на разширени формати (с добавен електронен времеви печат или данни за верификация във време), както следва:

- Процес на валидиране на базов формат на подпис/печат (Validation Process for Basic Signatures) - Baseline;
- Процес на валидиране на подпис/печат с време (Validation Process for Signatures with Time) – Baseline + T;
- Процес на валидиране на подпис/печат с данни за верификация във времето (Validation Process for Signatures with Long-Term validation data) – Baseline + LT.




Процесът преминава през следните стъпки:

**Стъпка 1.** Клиентът генерира и подава заявка за валидиране на подписа. Евротръст може да използва протоколи, които са описани в ETSI TS 119 442. Заявката включва подписания документ (и) (SD) и подписът (ите) (SDO), с които ги подписват.

Ограничения за валидиране са определени в ETSI TS 119 102-1 и според настоящата политика, Евротръст ограничава валидирането само до описаните в нея параметри.

QSVSP не поддържа политики за валидиране на подписи, предоставени от потребител.

**Стъпка 2.** SVSServ изпълнява процеса на валидиране в съответствие с в ETSI TS 119 102-1.

Валидирането се извършва от QSVSP в съответствие с ограничения, които са поставени от самата услуга. SVS прилага политика за проверка на подпис "стойност по подразбиране".

**Стъпка 3.** SVSServ подготвя и изпраща отговор за проверка. Евротръст може да използва протоколи, които са описани в ETSI TS 119 442. Отговорът за потвърждаване на валидирането се вгражда доклада за проверка. Той носи OID на политиката за услугата и може да вгради OID на използваната политика за проверка на подписа. Докладът за валидиране включва:

- Докладът е подписан с квалифицирано удостоверение за квалифициран електронен печат.
- Доклади за всяко ограничение на валидирането:
  - когато ограничението е било обработено, със съответния резултат,
  - когато ограничението не е било обработено с указание, че ограничението е игнорирано или заменено когато е уместно.

**Стъпка 4.** Представяне на доклада за валидиране.

### 3.1.2. ОГРАНИЧЕНИЯ ПРИ ВАЛИДИРАНЕ НА ЕЛЕКТРОННО ПОДПИСАН ДОКУМЕНТ

Услугата по квалифицирано валидиране се управлява чрез набор от ограничения за валидиране. Тези ограничения при работа се задават при управлението на услугата. В

допълнение може да се появят ограничения, свързани с използваните удостоверения за електронен подпис/печат. Също така е възможно да се подаде и специализирана политика, описана във формален документ, която да бъде приложена в момента на валидиране. Възможно е да бъдат договорени и специфични за дадена доверена страна ограничения и/или разширения на валидирането на предоставените към нея доклади. Услугата поддържа специфични ограничения, свързани с елементи на положения подпис/печат, използвани допустими криптографски комбинации и алгоритми, както и в самото квалифицирано валидиране на електронни подписи и печати. При използването на услугата има ограничения в размера на приетия за подписване електронно подписан файл, който е не повече от 10 мегабайта. В процеса на валидиране освен се използва и квалифицираната услуга за удостоверяване на време на Евротръст, която има собствена политика за използване.

### 3.1.3. ОГРАНИЧЕНИЯ ПРИ ВАЛИДИРАНЕ НА УДОСТОВЕРЕНИЯ ЗА ЕЛЕКТРОНЕН ПОДПИС/ПЕЧАТ

Услугата за валидиране поддържа следните ограничения при валидиране на удостоверенията за електронен подпис/печат (ETSI TS 119 172-1, клауза A.4.2.1, BSP (m), LoA on signer authentication):

| **Ограничение(я)** | **Стойност на ограничението при квалифицирано валидиране на електронни подписи и печати** |
|---|---|

| | |
|---|---|
| (m) 1. **X509 CertificateValidationConstraints**: Този набор от ограничения е относно изискванията в процеса на валидиране на удостоверителната верига съгласно IETF RFC 5280. Ограниченията могат да бъдат различни за различни видове удостоверения (например, удостоверения за подписи, за Удостоверяващи Органи, за OCSP-отговори, за CRL-списъци, електронни времеви печати/TST). Семантиката на възможен набор от изискуеми стойности, която се ползва да представи тези изисквания, се определя по следния начин:<br>(m) 1.1 *SetOfTrustAnchors*: Това ограничение посочва набор от допустими доверени Органи за удостоверяване (TAs) с цел да се ограничи процеса на валидиране. | **European Union Trusted List of Trust Service Providers** https://webgate.ec.europa.eu/tl-browser |
| (m) 1.2 *CertificationPath*: Това ограничение показва пътя на удостоверяване, който се използва от SVA за квалифицирано валидиране на електронни подписи и печати. Пътят на удостоверяване е с дължина "n" от началото/Органа на доверие (TA) в посока към удостоверените на електронен подпис/печат, използван при валидиране на подписа. Ограничението може да включва пътя или да указва необходимостта от включване на пътят, предоставен чрез електронен подпис/печата, ако има такъв.<br>➢ (m) 1.3. *user-initial-policy-set:* Съгласно IETF RFC 5280 клауза 6.1.1 (c)<br>➢ (m) 1.4. *initial-policy-mapping-inhibit*: Съгласно IETF RFC 5280 клауза 6.1.1 (e)<br>➢ (m) 1.5. *initial-explicit-policy*: Съгласно IETF RFC 5280 клауза 6.1.1 (f)<br>➢ (m) 1.6. *initial-any-policy-inhibit*: Съгласно IETF RFC 5280 клауза 6.1.1 (g)<br>➢ (m) 1.7. *initial-permitted-subtrees*: Съгласно IETF RFC 5280 клауза 6.1.1 (h)<br>➢ (m) 1.8. *initial-excluded-subtrees*: Съгласно IETF RFC 5280 клауза 6.1.1 (i)<br>➢ (m) 1.9. *path-length-constraints*: Това ограничение е относно броя на удостоверенията на УО (CA) в удостоверителната верига.<br>➢ (m) 1.10. *policy-constraints*: Това ограничение е относно политиката (те) в удостоверението за електронен подпис/печат. | **Няма**<br>**Няма**<br>**Няма**<br>**Няма**<br>**Няма**<br>**Няма**<br>**Няма**<br>**Няма** |

| | |
|---|---|
| (m) 2. **RevocationConstraints:** Този набор от ограничения е относно проверката на статуса на удостоверенията на електронен подпис/печат по време на процеса на валидиране. Тези ограничения могат да бъдат различни за различните видове удостоверения за електронен подпис/печат. Семантиката на възможен/допустим набор от изискуеми стойности, която се ползва да представи тези изисквания, се определя по следния начин:<br>(m) 2.1. *RevocationCheckingConstraints:* Това ограничение е относно изискванията за проверка на удостоверението за електронен подпис/печат за отмяна/прекратяване. Такива ограничения специфицират, дали проверката за отмяна/прекратяване е необходима или не и дали следва да се използват OCSP-отговори или издадени CRL. Семантиката на възможен набор от изискуеми стойности, която се ползва да представи тези изисквания, се определя по следния начин:<br>- ClrCheck: Проверките се извършват срещу текущия CRL;<br>- OcspCheck: Статусът за отмяна/прекратяване се проверява чрез OCSP IETF RFC 6960;<br>- BothCheck: Извършват се и двете проверки чрез OCSP и CRL;<br>- EitherCheck: Извършват се проверки или чрез OCSP или чрез CRL;<br>- NoCheck: Без проверки | **EitherCheck** |
| (m) 2.2. *RevocationFreshnessConstraints*: Това ограничение посочва времевите изисквания на информацията за отмяна/прекратяване. Ограниченията могат да посочат максималната допустима разликата между датата на издаване на информация за състоянието на отмяна/прекратяване на удостоверението за електронен подпис/печат и времето на валидиране, или да изисква SVA да приема само информация за отмяна/прекратяване, издадена в определено време след създаването/генерирането на електронен подпис/печат. | **Няма** |
| (m) 2.3. *RevocationInfoOnExpiredCerts*: Това ограничение налага удостоверението за електронен подпис/печат, използвано при валидиране му да бъде издадено от УО (CA), който поддържа обновяванията на отменени/прекратени удостоверения дори и след като са изтекли, за период по-дълъг дадена долна граница. | **Няма** |

| | |
|---|---|
| (m) 3. LoAOnTSPPractices: Това ограничение указва нивото на споразумение (LoA) относно практиките на TSP (s), които издават удостоверение на електронен подпис/печат, за да бъдат потвърдени по време на процеса на валидиране по пътя на удостоверенията: | **Няма** |
| • EUQualifiedCertificateRequired | Да |
| • EUQualifiedCertificateSigRequired | Да |
| • EUQualifiedCertificateSealRequired 1 | Да |

### 3.1.4. ОГРАНИЧЕНИЯ, СВЪРЗАНИ С КРИПТОГРАФИЯТА

Услугата за валидиране поддържа криптографски ограничения, свързани с изискваните алгоритми и параметри. Те са съгласно документа ETSI TS 119 312 и покриват изискванията на ETSI TS 119 172-1 „(p)1. **CryptographicSuitesConstraints**: Това ограничение указва изисквания за алгоритмите и параметрите, използвани при създаването на електронни подписи/печати или използвани при валидирането на подписи/печати на обекти, включени в процеса на валидиране (напр. електронни подписи/печати, удостоверения, CRLs, OCSP-отговори, времеви печати/TSTs).“

### 3.1.5. ОГРАНИЧЕНИЯ ЗА ЕЛЕМЕНТИТЕ НА ПОДПИСА И ПЕЧАТА

Услугата за валидиране поддържа ограничения относно елементите на квалифицирано валидиране на електронни подписи и печати. В съответствие с изискванията на ETSI TS 119 172-1 те са:

| **Ограничения** | **Стойност на ограничението при квалифицирано валидиране на електронни подписи и печати** |
|---|---|

| | |
|---|---|
| (b) 1. **ConstraintOnDTBS:** Това ограничение указва изискванията за вида на данните, които се подписват от подписващия. | **Няма** |
| (b) 2. **ContentRelatedConstraintsAsPartOfSignatureElements:** Този набор от ограничения показва необходимите информационни елементи свързани със съдържанието, под формата на подписани или неподписани квалифицирани реквизити, които присъстват в електронните подписи/печати. Наборът включва:<br>(b) 2.1 *MandatedSignedQProperties-DataObjectFormat* изисква специфичен формат за съдържанието, което ще бъде подписано от подписващия.<br>(b) 2.2 *MandatedSignedQProperties-content-hints* изисква конкретна информация, която описва най-вътрешното подписано съдържание на многослойно съобщения, в което едно съдържание е капсулирано в друго, за да бъде подписано цялото съдържание от подписващия.<br>(b) 2.3 *MandatedSignedQProperties-content-reference* изисква включването на информация за начина, по който да се свърже заявка и отговор на съобщението в обмен между двете страни, или начина по който трябва да се направи връзката, и т.н.<br>(b) 2.4 *MandatedSignedQProperties-content-identifier* изисква присъствие и евентуално конкретна стойност на идентификатор, който да се използва по-късно в подписания атрибут, квалифициращ "съдържание-препратка". | **Няма**<br><br>**Няма**<br><br>**Няма**<br><br>**Няма** |
| (b)3. **DOTBSAsAWholeOrInParts:** Това ограничение показва дали данните или само определена/и част/и от тях трябва да бъдат подписани. Семантиката за възможен набор от | **Няма** |

| | |
|---|---|
| изисквани стойности, използвана да укаже на тези изисквания се определя, както следва:<br>• Whole: всички данни трябва да бъде подписани;<br>• Parts: само определена/и част/и на данните трябва да бъде подписана. В този случай се използва допълнителна информация, за да укаже кои части трябва да бъдат подписани. | |

## 3.2. ИЗИСКВАНИЯ КЪМ ПРОТОКОЛА ЗА ВАЛИДИРАНЕ НА ПОДПИСА

Протоколът за валидиране на подпис, използван от QSVSP, може да съответства на ETSI TS 119 442. Отговорът за валидиране на подписа съдържа OID на политиката на SVS.

Комуникационният канал между клиента и валидационната услуга транспортира заявката за валидиране на електронния подписа в едната посока и връща обратно отговорът. Той може да бъде синхронен или асинхронен. Той обхваща удостоверяването на QSVSP, за да се избегне фалшивост в доклада и може да поддържа удостоверяването на клиента. Комуникационният канал между QSVSP и други TSP е извън обхвата на настоящия документ.

## 3.3. ИНТЕРФЕЙСИ

Комуникационният канал между клиента и QSVSP е обезпечен чрез използване на надеждно защитен канал по протокол HTTPS и използване на TLS 1.2 и по-висок. QSVSP гарантира, че може да установи сигурен канал с клиента и да запази поверителността на данните.

Услугата използва HTTPS автентификация, чрез удостоверение за сървър/удостоверение за автентичност на уебсайт пред приложение или клиент/браузър, без да се изисква автентификация от страна на потребителя. OASIS DSS интерфейсът дефинира интерфейс за валидиране на един или няколко на подписани с електронен подпис/печат документи. И двата протокола на OASIS DSS интерфейса използват транспортен протокол SOAP за обмен на XML командите при валидиране на

подписа/печата. Спецификациите на DSS интерфейса се регулират и поддържат от OASIS консорциума.

Услугата се достъпва и ползва и през уеб интерфейс. При този интерфейс XML командите на DSS интерфейса използват HTTP POST за обмен/транспорт. Клиентът достъпва услугата и може да посочи и зареди подписан документ с електронен подпис/печат, да избере параметрите на заявката, след което да изпрати формираната Request на услугата чрез HTTP POST протокол.

### 3.3.1. КОМУНИКАЦИОНЕН КАНАЛ

QSVSP предлага сигурен комуникационен канал и гарантира поверителността на процеса по автентификация и личните данни на потребителите. QSVSP допуска сигурно удостоверяване на автентичността на потребителите.

### 3.3.2. QSVSP - ДРУГИ ДОСТАВЧИЦИ НА УДОСТОВЕРИТЕЛНИ УСЛУГИ

Статусът за проверка на подписа и докладът за валидиране на подписа могат да бъдат засегнати от практиките, политики и договорености за съответствието на други доставчици на услуги, които не са под контрола на SVSP. Други доставчици на удостоверителни услуги, които контактуват с Евротръст (QSVSP) в качеството му на доставчик на услуга за квалифицирано валидиране могат да бъдат Органи за удостоверяване на време (TSAs), други доставчици на услуга за валидиране (SVSP), други доставчици на CRL, други доставчици на валидиране на статус на удостоверения (OCSP) на които Евротръст може да препредава заявка и т.н. Комуникационният канал между SVSP и други TSP е извън обхвата на настоящия документ.

## 3.4. ДОКЛАД ЗА ВАЛИДИРАНЕ НА ПОДПИС

В следствие на извършената автоматизирана обработка, услугата изготвя подробен отчет в PDF формат за валидирането на подписа/печата, в който подробно са описани причините за предоставените статуси. Резултатът от процеса на валидиране включва статус

на резултатите от процеса на квалифицирано валидиране на електронни подписи и печати. Допълнително разширеният доклад включва и дата и време на статуса на валидиране, както и допълнителни данни.

Услугата за валидиране на подпис (SVS) извежда индикация за състоянието и доклад за валидиране, предоставящ подробности за техническата проверка на всяко от приложимите ограничения, описани в ETSI TS 119 102-1. Процесът на валидиране се контролира от набор от ограничения за валидиране. Всяко ограничение на валидирането, може да произхожда от различни източници:

- от самото съдържание на подписа, директно (включено в атрибутите на подписа) или непряко, т.е. чрез позоваване на външен документ, предоставен или в четлива за човека и/или машинно обработваема форма; или
- от местен източник от верификатора (напр. конфигурационен файл, политика за проверка на подпис от машина).

Допълнителни ограничения могат да бъдат осигурени от DA към SVA чрез зададени параметри. Тези ограничения влияят на процеса на валидиране и на резултата от валидирането, независимо от това къде са дефинирани. Някои от ограниченията могат да са свързани с елементи на процеса на валидиране на подписа, които са широко разпространени в приложения и вече са стандартизирани другаде, напр. в IETF RFC 5280.

Поддържат се следните ограничения:

- Ограничения на веригата, както е определено в точка 5.1.4.2 на ETSI TS 119 102-1;
- Криптографски ограничения, както са определени в точка 5.1.4.3 на ETSI TS 119 102-1;
- Ограничения на елементите на подписа, определени в точка 5.1.4.4 на ETSI TS 119 102-1.

Докладът за валидиране на подпис може да съответства на изискванията в ETSI TS 119 102-2, както следва:

- посочва едно от трите състояния, определени в ETSI TS 119 102-1: TOTAL-PASSED, TOTAL-FAILED или INDERTERMINATE;
- дава информация за под-индикации, както е посочено в ETSI TS 119 102-1;

- може да отчита за всяко от валидираните ограниченията, които се обработват, включително всички ограничения за валидиране, които са приложени безусловно от изпълнението;
- съдържа идентификатора на политиката за валидиране на подписа. Този идентификатор присъства и в отговора на валидирането, когато протоколът съответства на ETSI TS 119 442 и присъства в доклада за валидиране, когато съответства на ETSI TS 119 102-2;
- съдържа информация за процеса на валидиране на подписа, като може да следва определеното в ETSI TS 119 102-2 с идентификатор, указващ процеса на валидиране, определен в т. 5.3, 5.5 и 5.6.3 на ETSI TS 119 102-1, който се използвани при валидирането;
- когато политиката за валидиране на подписа не е напълно обработена от SVS, докладът може да дава информация за ограниченията, които са били игнорирани или подтиснати;
- когато не е възможно да се обработят ограниченията, подадени от клиента, докладът, който се генерира може да дава информация за ограниченията, които са били игнорирани или подтиснати;
- докладът за валидиране на подписа носи самоличността на Евротръст;
- докладът за валидиране на подписа трябва да отчита самоличността на подписващия;
- докладва за всички подписани атрибути. В случай на некритичен атрибут на подписа, който не може да бъде декодиран, може да се постави информация за това, че атрибутът съществува;
- съдържа квалифициран времеви печат;
- може ясно да посочва дали SVS не е извършила изчислението на хеша, а е разчитала на такова изчисление, направено от потребителя;
- може ясно да посочва произхода на всеки PoE (от подпис, от потребител, от сървър);
- съдържа електронен печат на Евротръст;
- подписаните доклади за валидиране имат формат и подпис, които могат да отговарят на изискванията на ETSI TS 119 102-2;

- когато се представя чрез уеб страница на Евротръст, валидирането се прави в TLS сесия.

За доказателство (PoE) за доказване за наличие на подпис се счита доклада, описан в настоящата точка.

*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.*