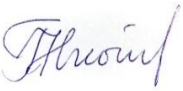
политика

ЗА КВАЛИФИЦИРАНО ВАЛИДИРАНЕ

Версия: 1.1

	Длъжност	Име, фамилия	Дата	Подпис
Утвърдил	Изпълнителен директор	Константин Безуханов	*13.02.2018 г.*	
Съгласувал	Представител на ръководството по СУСИ	Стефан Хаджистойчев	*13.02.2018 г.*	
Разработил	Системен одитор	Геновева Котова	*13.02.2018 г.*	

Дата на регистрация на документа:	*13.02.2018 г.*
Оригиналът се съхранява:	*при Представител на ръководството по СУСИ*

Вид на екземпляра и пореден №

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

Разпространение на документа:	**Абонат:**
Вътрешно:	
Външно:	

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

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

СЪДЪРЖАНИЕ

1. Въведение и обхват

Този документ определя правилата за квалифицирано валидиране на електронни подписи и печати (ЕП/ЕПечат) и издаване на електронно подписани доклади чрез удостоверителната услуга за квалифицирано валидиране „Evrotrust Qualified Validation Service“ (по-надолу за краткост „Услуга“). 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, Доставчик на квалифицирани удостоверителни услуги (по-надолу за краткост „ДКУУ ЕВРОТРЪСТ“) в съответствие с изискванията, определени в Регламент (ЕС) № 910/2014[1] (Регламента) и съгласно референтните европейски стандарти на ETSI (Technical Committee Electronic Signatures and Infrastructures).

ЕВРОТРЪСТ предоставя Услугата в съответствие с изискванията, определени в Регламента 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 ЕП/ЕПечат в съответствие с изискванията на Регламента;
- Проверява състоянието на удостоверенията в съответствие с препоръка RFC 6960: X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP;
- Валидира квалифицирани удостоверения (КУ) и ЕП/ЕПечати;
- Изпълнява техническите процедурите за валидност на подписи съгласно изискванията на ETSI TS 319 102-1.

Относно правния статус на ЕП/ЕПечат съгласно тази Политика, общия резултат от валидацията не се променя, независимо дали се отнася за усъвършенстван подпис/печат придружен от КУ или е ЕП/ЕПечат.

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

[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*

Стойностите на идентификаторите на обекти са:

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

1.1. Валидиращ орган

„Evrotrust Qualified Validation Service“ е валидиращ орган, който обслужваща удостоверения за електронен подпис и печат по Регламент (ЕС) № 910/2014. Валидиращият орган на Евротръст електронно подписва с Квалифицирано удостоверение за квалифициран електронен печат издадените от него доклади за валидация на проверените електронно подписани документи.

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 (2.5.4.97)=	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: Policy Identifier=1.3.6.1.4.1.47272.2.9 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: 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 Distribution Point Name: Full Name: URL=http://ca.evrotrust.com/crl/EvrotrustRSARootCA.crl
Authority Information Access	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://ca.evrotrust.com/aia/EvrotrustRSARootCA.crt [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ca.evrotrust.com/ocsp
Key Usage (critical)	Digital Signature, Non-Repudiation (c0)
Basic Constrains (critical)	Subject Type=End Entity Path Length Constraint=None

2. Съответствие

2.1. Съответствие с общоприети стандарти

[1] РЕШЕНИЕ ЗА ИЗПЪЛНЕНИЕ (ЕС) 2015/1506 НА КОМИСИЯТА от 8 септември 2015 (съгласно член 27, параграф 5 и член 37, параграф 5 от Регламент (ЕС) № 910/2014)

[2] EN 319 132-1 v1.1.1 XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures

[3] EN 319 132-2 v1.1.1 XAdES digital signatures; Part 2: Extended XAdES signatures

[4] ETSI TS 103 173 V2.2.1 (2013-04) Electronic Signatures and Infrastructures (ESI); CadES Base

Profile

[5] ETSI TS 103 172 V2.2.2 (2013-04) Electronic Signatures and Infrastructures (ESI); PadES Base Profile

[6] ETSI TS 103 174 V2.2.1 (2013-06) Electronic Signatures and Infrastructures (ESI); ASiC Baseline Profile

[7] ETSI EN 319 102-1 V1.1.1 (2016-05) Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation

[8] ETSI TS 119 101 V1.1.1 (2016-03) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for applications for signature creation and signature validation

[9] ETSI TS 119 172-1 V1.1.1 (2015-07) Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 1: Building blocks and table of contents for human readable signature policy documents

[10] ETSI TS 119 312 V1.1.1 (2014-11) Electronic Signatures and Infrastructures (ESI); Cryptographic Suites

[11] ETSI EN 319 412-2 V2.1.1 (2016-02) Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons

[12] ETSI EN 319 412-5 V2.1.1 (2016-02) Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements

[13] ETSI TS 101 733 V.1.7.4 (2008-07) Electronic Signature and Infrastructure (ESI) – CMS Advanced Electronic Signature (CAdES).

[14] ETSI TS 101 903 V.1.3.2 (2006-03) XML Advanced Electronic Signatures (XAdES).

[15] ETSI TS 102 778 (2009-07) Electronic Signature and Infrastructure (ESI) – PDF Advanced Electronic Signature (PAdES).

[16] R.Housley. Cryptographic Message Syntax (CMS). RFC5652. 2009.

[17] D.Eastlake, J.Reagle, D.Solo, (Extensible Markup Language) XML-Signature Syntax and Processing, RFC3275. 2002.

[18] ETSI TS 119 612 V2.1.1 (2015-07) Electronic Signatures and Infrastructures
(ESI); Trusted Lists

[19] S.Drees et al., Digital Signature Service Core Protocols and Elements OASIS. 2007.

[20] OASIS Digital Signature Service Signature Gateway Profile. 2007.

[21] OASIS Digital Signature Service eXtended

[22] Adobe Systems Inc., PDF Reference – Fifth Edition – Adobe Portable Document Format Version

1.6. 004

[23] M.Myers, R.Ankney, A.Malpani, S.Galperin, C.Adams. Internet X.509 Public Key Infrastructure Online Certificate Status Protocol – OCSP, RFC6960.

2.2. Съответствие с Регламент (ЕС) № 910/2014

Услугата се изпълнява е съответствие с изискванията за квалифицирано валидиране на квалифицирани електронни подписи (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: 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 ЕП/ЕПечат.
г) уникалният набор от данни, представляващи титуляря на електронния подпис в удостоверението, е надлежно предаден на доверяващата се страна;	Услугата автоматизирано създава доклад за валидация 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	Псевдонима се вписва в специален атрибут в

псевдоним, то това е ясно указано на доверяващата се страна;	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, 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 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: 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	Гарантира се чрез описаната в настоящата политика

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.	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 електронни печати.	Услугата покрива и валидирането на електронни печати по смисъла на чл.40

3. Съкращения

CA - Certificate Authority
CAdES - CMS Advanced Electronic Signatures
CRL - Certificate Revocation List
DSS - Digital Signature Standard
eIDAS - Regulation (EU) No 910/2014 of the European Parliament
ETSI - European Telecommunications Standards Institute
GUI - Graphical User Interface
OASIS - Organization for the Advancement of Structured Information Standards
OCSP - Online Certificate Status Protocol
PDF - Portable Document Format
PAdES - PDF Advanced Electronic Signatures
PoE - Proof of Evidence
SOAP - Simple Object Access Protocol
TLS - Transport Layer Security
TSA - Time Stamping Authority
TSL - Trust Status List
VA - Validation Authority
VS - Validation Service
XAdES - XML Advanced Electronic Signatures
XML - eXtended Markup Language
XML - DSIG XML Digital Signature

4. Услуга

4.1. Общи принципи

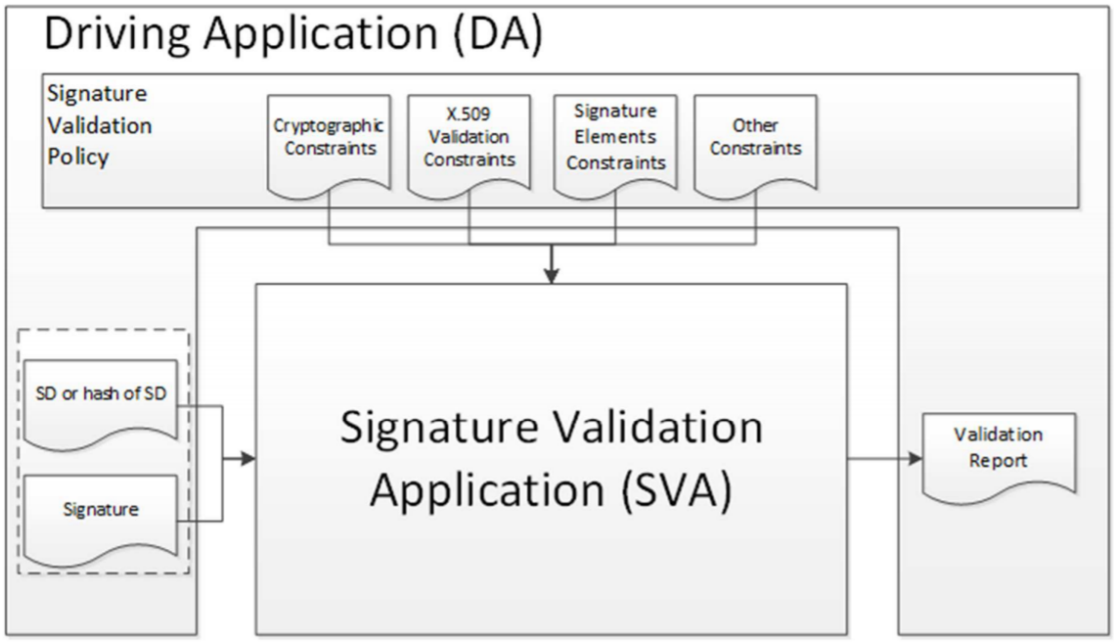
Услугата „валидиране“ означава процеса на проверка и потвърждаване на валидността на ЕП/ЕПечат. Услугата потвърждава валидността на ЕП/ЕПечат при условие, че:

- удостоверението в подкрепа на подписа/печата към момента на подписването е било квалифицирано (КУ) съгласно Приложение I на Регламента;
- КУ 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;
- уникалният набор от данни, представляващи Титуляря на електронния подпис в удостоверението, е надлежно предаден на Доверяващата се страна;
- ако към момента на подписване е бил използван псевдоним, то това е ясно указано на Доверяващата се страна;
- електронният подпис/печат е създаден от устройство за създаване на електронен подпис/печат;
- целостта на подписаните данни не е застрашена;
- изискванията за усъвършенстван електронен подпис са били изпълнени към момента на подписването;
- предоставя на Доверяващата се страна доклад от процеса на валидиране и позволява тя да открие евентуални проблеми, свързани със сигурността;
- услугата дава възможност на Доверяващите се страни да получат резултата от процеса на валидиране по автоматизиран начин, който е надежден и ефикасен и носи квалифициран печат на Валидиращия орган на Евротръст.

Техническата валидност на ЕП/ЕПечат се проверява в съответствие с процеса, описан в документа ETSI TS 319 102-1 и се потвърждава, чрез издаване електронни доклади подписани от валидиращия орган на Евротръст.

Когато няма посочено специфично изискване относно Услугата по подразбиране се приемат изискванията в т. 5 от ETSI TS 319 102-1, а когато има посочени такива специфични изисквания, те се ползват с предимство.

4.2. Модел на Услугата



Съгласно общоприетия модел на процеса на валидация на усъвършенствани подпис/печат, описан в ETSI TS 319 102-1, софтуерът с функции за валидация на ЕП/ЕПечат включва компонентите SVA/Signature Validation Application и DA/Driving Application.

Услугата на ДКУУ ЕВРОТРЪСТ се позиционира като компонентата Signature Validation Application(SVA) от модела. SVA се активира чрез компонентата Driving Application (DA), която трябва да получи резултата от процеса на валидиране под формата на доклад.

Driving Application (DA) на ДКУУ ЕВРОТРЪСТ може да бъде:

- Уеб-клиент с графичен интерфейс (GUI);
- Приложение-клиент (или софтуерна библиотека), ползващо OASIS-DSS спецификации.

Тези две форми на DA се реализират съгласно принципите, описани в настоящия документ.

4.3. Процес на валидация

В зависимост от използвания формат на ЕП/ЕПечат, Услугата поддържа процеси на валидация 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 валидация на базов формат на подпис/печат (Validation Process for Basic Signatures) - Baseline;
- Процес на валидация на подпис/печат с време (Validation Process for Signatures with Time) – Baseline + T;
- Процес на валидация на подпис/печат с данни за верификация във времето (Validation Process for Signatures with Long-Term validation data) – Baseline + LT.

Услугата изпълнява последователност от действия по квалифицирано валидиране:

1. Извършва процес по квалифицирано валидиране на електронни подписи и печати с разширен формат.
2. Извършва процес квалифицирано валидиране на електронни подписи и печати с базовия формат.
3. Ако избрания процес на валидиране завърши със статус „Успешен“ (PASSED), статуса е „Напълно Успешен“ (TOTAL-PASSED).
4. Ако избрания процес на валидиране завърши със статус „Грешка“ (FAILED), статуса е „Напълни Грешен“ (TOTAL-FAILED).
5. В противен случай статусът остава „Неопределен“(INDETERMINATE).

4.4. Процес по изготвяне на доклад

В следствие на извършената автоматизирана обработка, Услугата изготвя подробен отчет в PDF формат за валидацията на подписа/печата, в който подробно са описани причините за предоставените статуси.

Резултатът от процеса на валидация включва статус на резултатите от процеса на квалифицирано валидиране на електронни подписи и печати. Допълнително се включва и дата и време на статута на валидиране, както и допълнителни данни.

4.5. Статус на процеса на квалифицирано валидиране на електронни подписи и печати

Вписана в отчета за валидация информация		Семантика
Статус	**Данни в Отчета за валидация**	
TOTAL-PASSED	Процесът на валидиране извежда валидираната удостоверителна верига, включително удостоверението за ЕП/ЕПечат, използвани в процеса на валидиране.	Процесът на квалифицирано валидиране на електронни подписи и печати е с резултат TOTAL-PASSED поради: • успешни криптографски проверки на ЕП/ЕПечат (включително проверки на хешове на отделните обекти от данни, подписани косвено); • положително валидирани ограничения, относно удостоверяване на идентичност на подписващия (напр., подписващото удостоверение е валидно); и • успешно валидиран ЕП/ЕПечат 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 ЕП/ЕПечат са неуспешни(включително проверките на хешовете на отделните обекти на данни, подписани косвено) или е доказано, че генерирането на подписа/печата е след отмяна/прекратяване на КУ.
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 валидация, за да установи статуса-индикация TOTAL-PASSED или TOTAL-FAILED на ЕП/ЕПечат.

Докладът на валидацията, съответстващ на статус-индикации TOTAL-FAILEQ и INDETERMINATED при валидация на ЕП/ЕПечат има структура, която е представена в таблицата по-долу и включва основни и помощни кодове, които процеса на валидация връща/предоставя.

Структура и семантика на доклада (отчета от валидация)

Вписана в отчета за валидация информация			Семантика
Основен статус	**Помощен статус**	**Данни към отчета на валидация**	
TOTAL-FAILED	FORMAT_FAILURE	Процесът на валидиране предоставя отделниоте факти, довели до налична информация за неуспешната обработка на ЕП/ЕПечат.	ЕП/ЕПечат не е съвместим с поддържаните стандарти, посочени в този документ, до степен не позволяваща криптографската блокова проверка да го обработи.
	HASH_FAILURE	Процесът на валидиране предоставя идентификатор, който еднозначно идентифицира елемент в обект за подпис/печат, предизвикващ грешката, под формата на удостоверението за ЕП/ЕПечат.	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 ЕП/ЕПечат.
	SIG_CRYPTO_FAILURE	Процесът на валидиране предоставя удостоверението за ЕП/ЕПечат, 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 ЕП/ЕПечат.
	REVOKED	Процесът на валидиране предоставя: ·Удостоверителната верига, използвана в процеса на	Процесът квалифицирано валидиране на електронни подписи и печати води до TOTAL-FAILED, защото:

		валидиране. · Времето и причината, ако има такава, за отмяна/прекратяване на удостоверението на ЕП/ЕПечат. · CRL, ако има такъв, в който е установена отмяната / прекратяването.	. удостоверението на ЕП/ЕПечат е отменено; и · има доказателство (PoE), че времето на подписа/печата е след времето на отмяната на удостоверението.
INDETERMINATE	SIG_CONSTRAINTS_FAILURE	Процесът на валидиране предоставя множество от причини, довели до неуспешна валидация.	Процесът квалифицирано валидиране на електронни подписи и печати води до INDETERMINATE, защото един или повече атрибути на ЕП/ЕПечат не съответстват на ограниченията при валидиране.
	CHAIN_CONSTRAINTS_FAILURE	Процесът на валидиране предоставя: •Удостоверителната верига, използвана в процеса на валидиране. •Допълнителна информация относно причината	Процесът квалифицирано валидиране на електронни подписи и печати води до 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.	Процесът квалифицирано валидиране на електронни подписи и печати води до INDETERMINATE, защото проверката на удостоверителната верига извежда грешка поради неустановена причина
	CRYPTO_CONSTRAINTS_FAILURE	Процесът на валидиране предоставя: Идентификация/означение на ЕП/ЕПечат или на удостоверение,	Процесът квалифицирано валидиране на електронни подписи и печати води до INDETERMINATE, защото поне

		които са генерирани с алгоритъм или размер на ключа, под необходимото ниво за криптографска сигурност	един от използваните алгоритми (за ЕП/ЕПечат 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: • ЕП/ЕПечат и/или съответстващи удостоверения са генерирани след момент, до който тези алгоритми/ключове се считат сигурни (ако такова време е известно); и • ЕП/ЕПечат 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: Валидираната удостоверителна верига.	Процесът квалифицирано валидиране на електронни подписи и печати води до INDETERMINATE, защото времето на подписа е след изтичане срока на годност (notAfter) на удостоверението.
	NOT_YET_VALID	-	Процесът квалифицирано валидиране на електронни подписи и печати води до INDETERMINATE, защото времето на подписа/печата е преди срока на годност (notBefore) на удостоверението.

	POLICY_PROCESSING_ERROR	Процесът по валидиране предоставя допълнителна информация за причината.	Процесът квалифицирано валидиране на електронни подписи и печати води до 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 квалифицирано валидиране на електронни подписи и печати води до 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 квалифицирано валидиране на електронни подписи и печати води до INDETERMINATE, защото предоставения списък с удостоверения за време и/или електронно подписани обекти не отговарят на исканата подредбата.
	NO_SIGNING_CERTIFICATE_FOUND	-	Процесът квалифицирано валидиране на електронни подписи и печати води до INDETERMINATE, защото удостоверението за ЕП/ЕПечат не може да бъде идентифицирано
	NO_CERTIFICATE_CHAIN_FOUND	-	Процесът квалифицирано валидиране на електронни подписи и печати води до INDETERMINATE, защото не е намерена удостоверителна верига

			за идентификация на удостоверението за ЕП/ЕПечат.
	REVOKED_ NO_POE	Процесът на валидиране предоставя: •Удостоверителната верига, която се използва в процеса на валидиране. • Времето и причината за отмяната/прекратяване на удостоверението на ЕП/ЕПечат.	Процесът квалифицирано валидиране на електронни подписи и печати води до INDETERMINATE, защото съответстващото удостоверение е отменено/прекратено по време на валидацията. 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: •Удостоверителната верига, която включва в себе си прекратения Удостоверяващ орган; • Времето и причината за отмяната/прекратяване на удостоверението.	Процесът квалифицирано валидиране на електронни подписи и печати води до INDETERMINATE, защото е открита поне една удостоверителна верига, но използваният Удостоверяващ орган е прекратен.
	OUT_OF_BO UNDS_NO_P OE	-	Процесът квалифицирано валидиране на електронни подписи и печати води до 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_CO NSTRAINTS_ FAILURE_N O_POE	Процесът на валидиране предоставя: Идентификация на ЕП/ЕПечат или на съответстващото	Процесът квалифицирано валидиране на електронни подписи и печати води до INDETERMINATE, защото най-

		удостоверение, генерирани с недопустима дължина на ключа или с алгоритъм, не отговарящи на криптографските изисквания за ниво на сигурност	малко един от алгоритмите, които са били използвани в ЕП/ЕПечат 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 квалифицирано валидиране на електронни подписи и печати води до 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 квалифицирано валидиране на електронни подписи и печати води до INDETERMINATE, защото не всички ограничения могат да бъдат изпълнени с при 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 квалифицирано валидиране на електронни подписи и печати води до 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 квалифицирано валидиране на електронни подписи и печати води до INDETERMINATE, поради други причини.

5. Политика

ДКУУ ЕВРОТЪСТ оперира Услугата в рамките на Политиката, описана в този документ. Тази Политика е в сила по подразбиране за всички, които използват Услугата.

5.1. Ограничения при валидация на електронно подписан документ

Процесът на валидация/Услугата се управлява чрез набор от ограничения за валидиране. Тези ограничения при работа с Услугата могат да се задават при управлението на услугата. В допълнение може да се появят ограничения, свързани с използваните удостоверения за ЕП/ЕПечат.

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 ЕП/ЕПечат, 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 Услугата се

използва и квалифицираната услуга за удостоверяване на време на Евротръст, която има собствена политика за използване.

5.1.1. Ограничения при валидация на удостоверения за ЕП/ЕПечат

Услугата поддържа следните ограничения при валидация на удостоверенията за ЕП/ЕПечат (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: (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 ЕП/ЕПечат, използван при валидиране на подписа. Ограничението може да включва пътя или да указва необходимостта от включване на пътят, предоставен чрез ЕП/ЕПечата, ако има такъв.	
➢ (m) 1.3. *user-initial-policy-set:* Съгласно IETF RFC 5280 клауза 6.1.1 (c)	**Няма**
➢ (m) 1.4. *initial-policy-mapping-inhibit*: Съгласно IETF RFC 5280 клауза 6.1.1 (e)	**Няма**
➢ (m) 1.5. *initial-explicit-policy*: Съгласно IETF RFC 5280 клауза 6.1.1 (f)	**Няма**
➢ (m) 1.6. *initial-any-policy-inhibit*: Съгласно IETF RFC 5280 клауза 6.1.1 (g)	**Няма**
➢ (m) 1.7. *initial-permitted-subtrees*: Съгласно IETF RFC 5280 клауза 6.1.1 (h)	**Няма**
➢ (m) 1.8. *initial-excluded-subtrees*: Съгласно IETF RFC 5280 клауза 6.1.1 (i)	**Няма**
➢ (m) 1.9. *path-length-constraints*: Това ограничение е относно броя на удостоверенията на УО (CA) в удостоверителната верига.	**Няма**
➢ (m) 1.10. *policy-constraints*: Това ограничение е относно политиката (те) в удостоверението за ЕП/ЕПечат.	**Няма**

(m) 2. **RevocationConstraints:** Този набор от ограничения е относно проверката на статуса на удостоверенията на ЕП/ЕПечат по време на процеса на валидиране. Тези ограничения могат да бъдат различни за различните видове удостоверения за ЕП/ЕПечат. Семантиката на възможен/допустим набор от изискуеми стойности, която се ползва да представи тези изисквания, се определя по следния начин:	
(m) 2.1. *RevocationCheckingConstraints:* Това ограничение е относно изискванията за проверка на удостоверението за ЕП/ЕПечат 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: - ClrCheck: Проверките се извършват срещу текущия CRL; - OcspCheck: Статусът за отмяна/прекратяване се проверява чрез OCSP IETF RFC 6960; - BothCheck: Извършват се и двете проверки чрез OCSP и CRL; - EitherCheck: Извършват се проверки или чрез OCSP или чрез CRL; - 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 ЕП/ЕПечат и времето на валидиране, или да изисква SVA да приема само информация за отмяна/прекратяване, издадена в определено време след създаването/генерирането на ЕП/ЕПечат.	**Няма**
(m) 2.3. *RevocationInfoOnExpiredCerts*: Това ограничение налага удостоверението за ЕП/ЕПечат, използвано при валидиране му да бъде издадено от УО (CA), който поддържа обновяванията на	**Няма**

отмененти/прекратени удостоверения дори и след като са изтекли, за период по-дълъг дадена долна граница.	
(m) 3. LoAOnTSPPractices: Това ограничение указва нивото на споразумение (LoA) относно практиките на TSP (s), които издават удостоверение на ЕП/ЕПечат, за да бъдат потвърдени по време на процеса на валидиране по пътя на удостоверенията: • EUQualifiedCertificateRequired • EUQualifiedCertificateSigRequired • EUQualifiedCertificateSealRequired 1	**Няма** Да Да Да

5.1.2. Ограничения, свързани с криптографията

Услугата 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 ЕП/ЕПечат или използвани при валидирането на подписи/печати на обекти, включени в процеса на валидация (напр. ЕП/ЕПечат, удостоверения, CRLs, OCSP-отговори, времеви печати/TSTs).“

5.1.3. Ограничения за елементите на подписа и печата

Услугата 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 ЕП/ЕПечат. Наборът включва: (b) 2.1 *MandatedSignedQProperties-DataObjectFormat* изисква специфичен формат за съдържанието, което ще бъде подписано от подписващия. (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. (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. (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** **Няма** **Няма** **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 изисквани стойности, използвана да укаже на тези изисквания се определя, както следва: • Whole: всички данни трябва да бъде подписани; • 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.	**Няма**

5.2. Поддържани формати и нива на сигурност за ЕП/ЕПечат

Услугата на ЕВРОТРЪСТ поддържа/валидира следната формати и нива на ЕП/ЕПечат в съответствие с РЕШЕНИЕ ЗА ИЗПЪЛНЕНИЕ (ЕС) 2015/1506 НА КОМИСИЯТА за определяне на спецификации, отнасящи се до формата на усъвършенствани електронни подписи и печати:

Формати с базов профил на ЕП/ЕПечат:

- ETSI TS 103 171 V2.1.1 Electronic Signatures and Infrastructures (ESI) - XadES Baseline Profile
- ETSI TS 103 173 V2.2.1 Electronic Signatures and Infrastructures (ESI) - CadES Baseline Profile
- ETSI TS 103 172 V2.2.2 Electronic Signatures and Infrastructures (ESI) – PadES Baseline Profile
- ETSI TS 103 174 V2.2.1 Electronic Signatures and Infrastructures (ESI) – AsiC Baseline Profile

В допълнение, Услугата валидира горепосочените формати, но с разширен профил, съобразно нивото на сигурност на ЕП/ЕПечат:

- ETSI TS 103 171 V2.1.1 Electronic Signatures and Infrastructures (ESI) – XadES-T/TL Level;
- ETSI TS 103 173 V2.2.1 Electronic Signatures and Infrastructures (ESI) – CadES T/TL Level;
- ETSI TS 103 172 V2.2.2 Electronic Signatures and Infrastructures (ESI) PadES T/TL Level;
- ETSI TS 103 174 V2.2.1 Electronic Signatures and Infrastructures (ESI) AsiC T/TL Level.

Услугата на ЕВРОТРЪСТ поддържа/валидира следните типови формати на ЕП/ЕПечат:

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

6. Обхват на Органа за валидиране

Услугата се изпълнява в съответствие с изискванията на Регламента. Тя се включва в общия доверителен списък на Европейската комисия (European Union Trusted List of Trust Service Providers), съставен от националните доверителни списъци на страните-членки на Европейския съюз (Trusted List).

7. Интерфейси на Услугата за потребители и Доверяващи се страни

Услугата се предлага като уеб услуга (Web Services), която се достъпва и ползва през Уеб интерфейс или през OASIS DSS Интерфейс. Услугата използва HTTPS автентификация, чрез удостоверение за сървър/удостоверение за автентичност на Уеб-сайт пред приложение или клиент/браузър, без да се изисква автентификация от страна на потребителя.

OASIS DSS интерфейсът дефинира интерфейс за подписване на един или няколко документи с ЕП/ЕПечат, както и за валидация на подписани с ЕП/ЕПечат документи. И двата протокола на OASIS DSS интерфейса използват транспортен протокол SOAP за обмен на XML-командите при подписване и при валидация 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 ЕП/ЕПечат, да избере параметрите на заявката, след което да изпрати формираната XML-заявка/Request на Услугата чрез HTTP POST протокол.

Регистриране на измененията																					
Страница																					
Валидно изменение																					