политика

ЗА КВАЛИФИЦИРАНО ВАЛИДИРАНЕ

Версия: 1.0

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

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

Вид на екземпляра и пореден №

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

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

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

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

СЪДЪРЖАНИЕ

1. Въведение и обхват

Този документ определя правилата за валидиране на Квалифицирани и Усъвършенствани Електронни Подписи (КЕП/УсЕП), на Квалифицирани и Усъвършенствани Електронни Печати (КЕПечат/ УсЕПечат) и издаване на квалифицирани електронни атестати за статут на квалифицирани удостоверения (КУ) чрез удостоверителната услуга за квалифицирано валидиране „Evrotrust RSA QS Validation“ (по-надолу за краткост „Услуга“). Документът 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 на Европейския парламент и на Съвета от 23 юли 2014 г. за електронната идентификация и удостоверителни услуги при електронните транзакции на вътрешния пазар и съгласно референтните европейски стандарти на ETSI (Technical Committee Electronic Signatures and Infrastructures).

Посочените правила в документа рефлектират върху бизнес и правните отношения както и на политиката на сигурност в електронните транзакции.

Съгласно т. 6 от РЕШЕНИЕ ЗА ИЗПЪЛНЕНИЕ (ЕС) 2015/1506 НА КОМИСИЯТА от 8 септември 2015 година (съгласно член 27, параграф 5 и член 37, параграф 5 от Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета):

"Усъвършенстваните електронни подписи и усъвършенстваните електронни печати са сходни от техническа гледна точка. Поради това стандартите за формати на усъвършенстваните електронни подписи следва да се прилагат mutatis mutandis по отношение на форматите на усъвършенстваните електронни печати.“

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 КЕП/УсЕП и КЕПечат/УсЕПечат в съответствие с изискванията на Регламента;
- Проверява състоянието на удостоверенията в съответствие с препоръка RFC2560 Online Certificate Status Protocol (OCSP);
- Валидира квалифицирани удостоверения (КУ) и КЕП/УсЕП и КЕПечати/УсЕПечати;
- Изпълнява техническите процедурите за валидност на подписи съгласно изискванията на ETSI TS 119 102.

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

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

Валидиращ орган	Идентификатор на обект (OID)
Evrotrust RSA Validation Политика на валидиращия орган, обслужваща квалифицираните удостоверения на базовия удостоверяващ орган „**Evrotrust RSA Root CA**“	1.3.6.1.4.1.47272.1.1
Evrotrust RSA QS Validation Политика на валидиращия орган, обслужваща квалифицираните удостоверения на оперативния удостоверяващ орган „**Evrotrust RSA Operational CA**“	1.3.6.1.4.1.47272.2.1

2. Съответствие

Този документ е разработен съгласно действащото законодателство в Република България и паневропейските препоръки, спецификации и стандарти за предоставяне на квалифицирани удостоверителни услуги според Регламент (ЕС) № 910/2014.

[1] Регламент (ЕС) N°910/2014: “Относно електронната идентификация и удостоверителните услуги при електронни трансакции на вътрешния пазар и за отмяна на Директива 1999/93/ЕО“

[2] 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)

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

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

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

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

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

[8] [ETSI-119-102] ETSI TS 119 102-1 Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation

[9] [ETSI-119-101] ETSI TS 119 101 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for applications for signature creation and signature validation

[10] 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

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

[12] ETSI TS 119 412-2 V2.1.1 (2016-02) Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons

[13] ETSI TS 119 412-5 V2.1.1 (2016-02) Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements

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

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

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

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

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

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

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

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

[22] OASIS Digital Signature Service eXtended

[23] Adobe Systems Inc., PDF Reference – Fifth Edition – Adobe Portable Document Format Version 1.6. 004

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

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 КЕП/КЕПечат.

Услугата потвърждава валидността на КЕП/КЕПечат 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 квалифициран електронен подпис/печат;
- целостта на подписаните данни не е застрашена;
- изискванията за усъвършенстван електронен подпис (чл. 26 на Регламента) са били изпълнени към момента на подписването;
- предоставя на Доверяващата се страна правилния резултат от процеса на валидиране (статус-индикация и отчет) 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 подпис (или печат) на ДКУУ ЕВРОТРЪСТ.

Техническата валидност на КЕП/КЕПечат се проверява в съответствие на процеса описан в документа ETSI TS 119 102 и се потвърждава чрез издаване квалифицирани електронни атестати за статус.

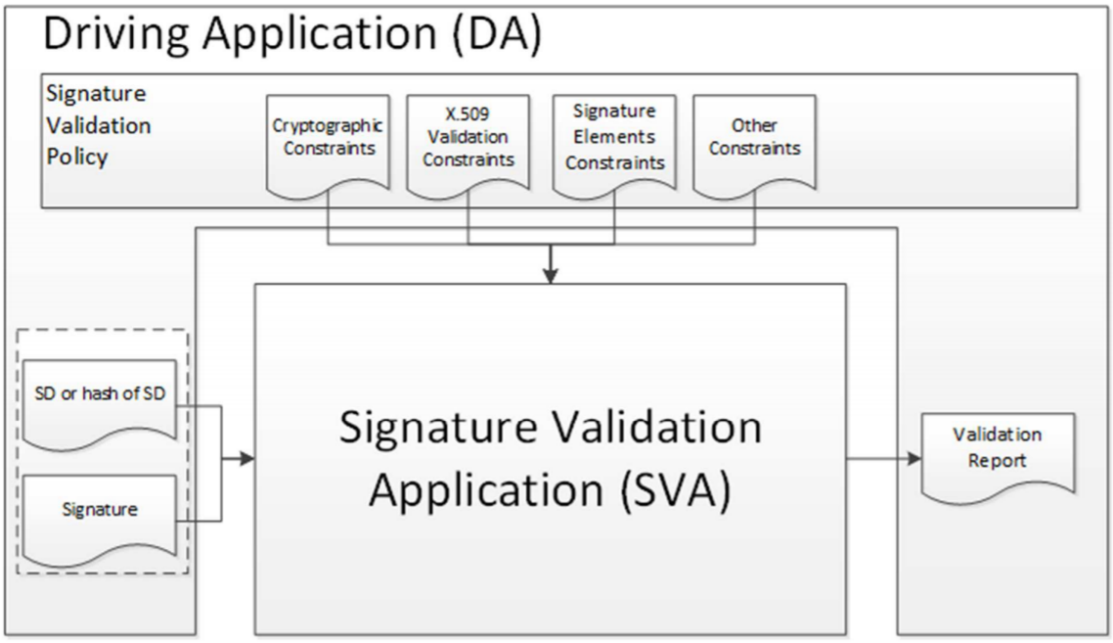
Следващите точки описват Услугата – концептуален модел, избор на процес на валидация и атестат (статус и отчет) на валидирано квалифицирано удостоверение на КЕП/КЕПечат.

Когато няма посочено специфично изискване относно Услугата в настоящия документ, приемат се изискванията в т. 5 от ETSI TS 119 102.

Когато има посочени специфични изисквания и правила в настоящия документ, те имат предимство пред съответните такива от ETSI TS 119 102-1.

В случай на несъответствие между изисквания и правила в този документ и ETSI TS 119 102, настоящите имат предимство.

4.2. Модел на Услугата



Съгласно концептуалният модел на процеса на валидация на усъвършенстван подпис/печат в ETSI TS 119 102-1 (фиг. 1), софтуерът с функции за валидация на КЕП/КЕПечат включва две компоненти:

- SVA/Signature Validation Application;
- 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 квалифициран атестат (статус и отчет).

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. Избор на процеса на валидация

В зависимост от класовете (формати) на КЕП, Услугата поддържа процеси на валидация на (т.е., валидира) Базови формати/Baseline formats на подпис/печат и на Разширени формати (с добавен електронен времеви печат (T) или данни за верификация във време (TL)) 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.

DA не може да определя процеса на валидация. Форматът на КЕП и нивото на сигурност (Level T/TL) на формата определят процеса на валидация.

Когато валидира подпис/печат, Услугата изпълнява последователно следните действия:

1. Извършва процес по валидиране на КЕП/КЕПечат с Разширен формат.
2. Извършва процес на валидиране на Базовия формат на КЕП/КЕПечат.
3. Ако избрания процес на валидиране завърши със статус-индикация „Успешен“ (PASSED), SVA предоставя на DA статус-индикация „Напълно Успешен“ (TOTAL-PASSED).
4. Ако избрания процес на валидиране завърши със статус-индикация „Грешка“ (FAILED), SVA предоставя на DA статус-индикация „Напълни Грешен“ (TOTAL-FAILED).
5. В противен случай, SVA предоставя към DA статус-индикация „Неопределен“(INDETERMINATE).

4.4. Статус-индикация на процеса на валидиране и отчет на валидация

Услугата предоставя подробен отчет на валидацията на подписа/печата, позволявайки на DA да провери в детайли решенията, взети по време на валидирането и подробно да установи/разследва причините за предоставения статус-индикация.

Уеб клиентът, който се предоставя заедно с Услугата когато тя се ползва от лице, представя отчета на валидация в PDF-формат.

Резултатът от процеса на валидация включва:

- статус-индикация на резултатите от процеса на валидиране на КЕП/КЕПечат;

- означение на политиката, по която е валидиран КЕП/КЕПечат;
- дата и време на статута на валидиране, включително данните, които се използват за валидиране;
- използваният процес на валидация ;
- допълнителни отчетни данни за валидиране, съгласно таблиците по-долу;
- атрибут, който показва причината за създаване на КЕП/КЕПечат, ако такъв има към предоставените данни за подпис/печат.

4.5. Статус-индикация на процеса на валидиране на КЕП/КЕПечат

Статус-индикация	Семантика	Данни към отчета на валидация
TOTAL-PASSED	Процесът на валидиране на КЕП/КЕПечат е с резултат TOTAL-PASSED поради: • успешни криптографски проверки на КЕП/КЕПечат (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 КЕП/КЕПечат спрямо валидиращи ограничения и по тази причина се приема спрямо тези ограничения.	Процесът на валидиране извежда валидираната удостоверителна верига, включително удостоверението за КЕП/КЕПечат, използвани в процеса на валидиране, заедно с конкретен подписан/подпечатан атрибут (ако присъства), който се разглежда като доказателства за валидиране.
TOTAL-FAILED	Процесът на валидиране на КЕП/КЕПечат е с резултат TOTAL-FAILED защото криптографските проверките на КЕП/КЕПечат са неуспешни(включително проверките на хешовете на отделните обекти на данни, подписани/подпечатани косвено) или е доказано, че	Процесът на валидиране извежда допълнителна информация, поясняваща статус-индикацията TOTAL-FAILED за всяко от ограниченията за валидиране, взети под внимание и за които са настъпили отрицателни резултати.

	генерирането на подписа/печата е след отмяна/прекратяване на КУ.	
INDETERMINATE	Наличната информация е недостатъчна за процеса на валидация, за да установи статуса-индикация TOTAL-PASSED или TOTAL-FAILED на КЕП/КЕПечат.	Процесът на валидиране извежда допълнителна информация, за да обясни неопределената индикация и да помогне на проверяващите да определят липсващите данни, за да завърши процеса на валидиране.

Отчетът на валидацията, съответстващ на статус-индикации TOTAL-FAILEQ и INDETERMINATED при валидация на КЕП 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 Отчета от валидация

Основен код/статус-индикация	Помощен код	Семантика	Данни, към отчета на валидация
TOTAL-FAILED	HASH_FAILURE	Процесът на валидиране на КЕП/КЕПечат води до TOTAL-FAILED, защото най-малко един хеш на обект, участващ в процеса на подписване не съответства на съответния хеш в КЕП/КЕПечат.	Процесът на валидиране предоставя идентификатор, който еднозначно идентифицира елемент в обект за подпис/печат, предизвикващ грешката, под формата на удостоверението за КЕП/КЕПечат.
	FORMAT_FAILURE	КЕП/КЕПечат не е съвместим с поддържаните стандарти, посочени в този документ, до степен не позволяваща криптографската блокова проверка да го обработи.	Процесът на валидиране предоставя всяка налична информация за неуспешната обработка на КЕП/КЕПечат.
	SIG_CRYPTO_FAILURE	Процесът на валидиране на КЕП/КЕПечат води до TOTAL-FAILED, защото цифровата	Процесът на валидиране предоставя удостоверението за КЕП/КЕПечат, използвано в

		стойност на подписа не може да бъде проверена с помощта на публичния ключ от удостоверението за КЕП/КЕПечат.	процеса на валидиране.
	REVOKED	Процесът на валидиране на КЕП/КЕПечат води до TOTAL-FAILED, защото: . удостоверението на КЕП/КЕПечат е отменено; и · има доказателство (PoE), че времето на подписа/печата е след времето на отмяната на удостоверението.	Процесът на валидиране предоставя: ·Удостоверителната верига, използвана в процеса на валидиране. · Времето и причината, ако има такава, за отмяна/прекратяване на удостоверението на КЕП/КЕПечат. · CRL, ако има такъв, в който е установена отмяната / прекратяването. · електронен времеви печат към подписа/печата, ако има такъв, който показват най-ранното известно време на съществуване на КЕП/КЕПечат.
INDETERMINATE	SIG_CONSTRAINTS_FAILURE	Процесът на валидиране на КЕП/КЕПечат води до INDETERMINATE, защото един или повече атрибути на КЕП/КЕПечат не съответстват на ограниченията при валидиране.	Процесът на валидиране предоставя: •Удостоверителната верига, използвана в процеса на валидиране. •Допълнителна информация относно причината.
	CHAIN_CONSTRAINTS_FAILURE	Процесът на валидиране на КЕП/КЕПечат води до INDETERMINATE, защото удостоверителната верига, използвана в процеса на валидиране не съответства на ограниченията свързани с	Процесът на валидиране предоставя: •Удостоверителната верига, използвана в процеса на валидиране. •Допълнителна информация относно причината

		удостоверението при валидирането	
	CERTIFICATE_CHAIN_GENERAL_FAILURE	Процесът на валидиране на КЕП/КЕПечат води до INDETERMINATE, защото проверката на удостоверителната верига извежда грешка поради неустановена причина	Процесът на валидиране предоставя: Допълнителна информация относно причината.
	CRYPTO_CONSTRAINTS_FAILURE	Процесът на валидиране на КЕП/КЕПечат води до INDETERMINATE, защото поне един от използваните алгоритми (за КЕП/КЕПечат или съответстващи удостоверения), които участват във валидирането на КЕП/КЕПечат или размерът на ключовете, които използват тези алгоритми, е под необходимото ниво за криптографска сигурност, както и: • КЕП/КЕПечат и/или съответстващи удостоверения са генерирани след момент, до който тези алгоритми/ключове се считат сигурни (ако такова време е известно); и • КЕП/КЕПечат 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).	Процесът на валидиране предоставя: Идентификация/означение на КЕП/КЕПечат или на удостоверение, които са генерирани с алгоритъм или размер на ключа, под необходимото ниво за криптографска сигурност
	NOT_YET_VALID	Процесът на валидиране на КЕП/КЕПечат води до	

		INDETERMINATE, защото времето на подписа/печата е преди срока на годност (notBefore) на удостоверението.	
	EXPIRED	Процесът на валидиране на КЕП/КЕПечат води до INDETERMINATE, защото времето на подписа е след изтичане срока на годност (notAfter) на удостоверението.	Процесът на валидиране предоставя: Валидираната удостоверителна верига
	NO_SIGNING_CERTIFICATE_FOUND	Процесът на валидиране на КЕП/КЕПечат води до INDETERMINATE, защото удостоверението за КЕП/КЕПечат не може да бъде идентифицирано	
	NO_CERTIFICATE_CHAIN_FOUND	Процесът на валидиране на КЕП/КЕПечат води до INDETERMINATE, защото не е намерена удостоверителна верига за идентификация на удостоверението за КЕП/КЕПечат.	
	REVOKED_NO_POE	Процесът на валидиране на КЕП/КЕПечат 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	Процесът на валидиране предоставя: •Удостоверителната верига, която се използва в процеса на валидиране. • Времето и причината за отмяната/прекратяване на на удостоверението на КЕП/КЕПечат.
	OUT_OF_BOUNDS_NO_P	Процесът на валидиране на КЕП/КЕПечат води до	

	OE	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 на КЕП/КЕПечат води до INDETERMINATE, защото най-малко един от алгоритмите, които са били използвани в КЕП/КЕПечат 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.	Процесът на валидиране предоставя: Идентификация на КЕП/КЕПечат или на съответстващото удостоверение, генерирани с недопустима дължина на ключа или с алгоритъм, не отговарящи на криптографските изисквания за ниво на сигурност
	NO_POE	Процесът на валидиране на КЕП/КЕПечат води до INDETERMINATE, защото липсва доказателство (PoE), чрез което доказва, че подписът/печатът е бил генериран преди станало известно компрометиращо събитие (напр. разбит алгоритъм).	Процесът на валидиране идентифицира само подписи/печати, за които липсват доказателства (POEs). Процесът на валидиране трябва да предостави допълнителна информация по проблема.

	TRY_LATER	Процесът на валидиране на КЕП/КЕПечат 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 на КЕП/КЕПечат води до INDETERMINATE, защото данните за подпис/печат не могат да бъдат получени	Процесът на валидиране предоставя: Идентификаторът (например URI) на данните за подпис/печат, които са причинили грешката.
	GENERIC	Процесът на валидиране на КЕП/КЕПечат води до INDETERMINATE, поради други причини.	Процесът на валидиране предоставя: Допълнителна информация, която показва защо статуса от валидиране е INDETERMINATE.

5. Политика

ДКУУ ЕВРОТЪСТ оперира Услугата в рамките на настоящата Политика. Тази Политика е в сила по подразбиране за всички Доверяващи се страни, които използват Услугата. Въвеждане на специфични ограничения за Доверяваща се страна са недопустими.

5.1. Ограничения при валидация

Процесът на валидация/Услугата се управлява чрез набор от ограничения за валидиране. Тези ограничения при работа с Услугата са изрично дефинирани чрез система от специфични данни за управление, както и от самото приложение.

Всички ограничения за валидация, които не са част от Услугата, следват директно от самото съдържание на КЕП/КЕПечат (включени в подписаните атрибути) или косвено от него, т.е. чрез позоваване на външен документ, предназначен за машинна (автоматизирана) обработка. Допълнителни ограничения могат да бъдат предоставени от DA на SVA чрез параметри, избрани от приложението или от потребителя.

Всяко допълнително ограничение се предоставя след взаимно споразумение между ДКУУ ЕВРОТРЪСТ и Доверяващата се страна.

Поддържат се следните специфични ограничения:

- Ограничения относно валидиране на удостоверения (веригата удостоверения);
- Криптографски ограничения;
- Ограничения относно елементи на подписа.

5.1.1. Общи ограничения

Услугата на ДКУУ ЕВРОТРЪСТ поддържа следните общи ограничения за валидация:

Ограничения	Стойност на ограничението при валидиране на КЕП/КЕПечат (SVA или DA)
TSA услуга, използвана за удостоверяване на време (квалифициран електронен времеви печат)	Evrotrust TSA
Максимален размер на файл	10MB

5.1.2. Ограничения при валидация на удостоверения

Услугата на ДКУУ ЕВРОТРЪСТ поддържа следните ограничения при валидация на X.509 удостоверения в процеса на валидация на удостоверителна верига съгласно ETSI TS 119 172-1, клауза A.4.2.1., Таблица A.2. ред (m).

Ограничения	Стойност на ограничението при валидиране на КЕП/КЕПечат (SVA или DA)

(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.	ЕС (TSL)
(m) 1.2 *CertificationPath*: Това ограничение показва пътя на удостоверяване, който се използва от SVA за валидиране на КЕП/КЕПечат. Пътят на удостоверяване е с дължина "n" от началото/Органа на доверие (TA) в посока към удостоверените на КЕП/КЕПечат, използван при валидиране на подписа. Ограничението може да включва пътя или да указва необходимостта от включване на пътят, предоставен чрез КЕП/КЕПечата, ако има такъв.	
(m) 1.3. *user-initial-policy-set:* Съгласно IETF RFC 5280 клауза 6.1.1 (c) (m) 1.4. *initial-policy-mapping-inhibit*: Съгласно IETF RFC 5280 клауза 6.1.1 (e) (m) 1.5. *initial-explicit-policy*: Съгласно IETF RFC 5280 клауза 6.1.1 (f) (m) 1.6. *initial-any-policy-inhibit*: Съгласно IETF RFC 5280 клауза 6.1.1 (g) (m) 1.7. *initial-permitted-subtrees*: Съгласно IETF RFC 5280 клауза 6.1.1 (h) (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. (m) 1.10. *policy-constraints*: Това ограничение е относно политиката (те) в удостоверението за КЕП/КЕПечат.	
(m) 2. **RevocationConstraints:** Този набор от ограничения е относно проверката на статуса на удостоверенията на КЕП/КЕПечат по време на процеса на валидиране. Тези ограничения могат да бъдат различни за различните видове удостоверения за КЕП/КЕПечат. 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 КЕП/КЕПечат 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 КЕП/КЕПечат и времето на валидиране, или да изисква SVA да приема само информация за	Няма

отмяна/прекратяване, издадена в определено време след създаването/генерирането на КЕП/КЕПечат.	
(m) 2.3. *RevocationInfoOnExpiredCerts*: Това ограничение налага удостоверението за КЕП, 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 КЕП/КЕПечат, за да бъдат потвърдени по време на процеса на валидиране по пътя на удостоверенията,.	Няма
EUQualifiedCertificateRequired	Да
EUQualifiedCertificateSigRequired	Да
EUQualifiedCertificateSealRequired 1	Да

5.1.3. Криптографски ограничения

Услугата на ДКУУ ЕВРОТРЪСТ поддържа следната криптографски ограничения, които посочват изисквания за алгоритмите и параметрите, използвани при създаването на КЕП/КЕПечат или използвани при валидиране на подписан обект, както е посочено в ETSI TS 119 172-1, клауза A.4.2.1, Таблица A2, ред (p).

Ограничения	Стойност на ограничението при валидиране на КЕП/КЕПечат
(p)1. **CryptographicSuitesConstraints**: Това ограничение указва изисквания за алгоритмите и параметрите, използвани при създаването на КЕП/КЕПечат или използвани при валидирането на подписи/печати на обекти, включени в процеса на валидация (напр. КЕП/КЕПечат, удостоверения, CRLs, OCSP-отговори, времеви печати/TSTs).	Съгласно документа ETSI TS 119 312

5.1.4. Ограничения за елементите на подписа

Услугата на ДКУУ ЕВРОТРЪСТ поддържа следната ограничения относно елементите на КЕП/КЕПечат, които указват изисквания към DTBS (Data To Be Signed), съгласно ETSI TS 119 172-1, клауза A.4.2.1., таблица A.2, ред (b).

Ограничения	Стойност на ограничението при валидиране на КЕП/КЕПечат
(b) 1. **ConstraintOnDTBS:** Това ограничение указва изискванията за вида на данните, които се подписват/подпечатват от подписващия/подпечатващия.	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 КЕП/КЕПечат. Наборът включва: (b) 2.1 *MandatedSignedQProperties-DataObjectFormat* изисква специфичен формат за съдържанието, което ще бъде подписано/подпечатано от подписващия/подпечатващия. (b) 2.2 *MandatedSignedQProperties-content-hints* изисква конкретна информация, която описва най-вътрешното подписано/подпечатано 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
(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;	Няма

• 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/подпечатани.	

5.2. Поддържани формати и нива на сигурност за КЕП/КЕПечат

Услугата на ЕВРОТРЪСТ поддържа/валидира следната формати и нива на КЕП/КЕПечат 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 КЕП/КЕПечат:

- 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 КЕП/КЕПечат:

- 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.

5.2.1. Ограничения на поддържаните КЕП/КЕПечат

Разположение на подписа/печата и подписания даннов обект	Стойност
Обхващащ КЕП/КЕПечат – подпис/печат обхваща данновия обект	да
Обхванат (тип „писмо“) КЕП/КЕПечат – подписания даннов обект обхваща подписа/печата	да
Отделен КЕП/КЕПечат – подпис/печат и даннов обект са разделени (самостоятелни)	да
Едновременно многократно сравнявани позиции	да
Един документ е с повече от един КЕП/КЕПечат	да

6. Обхват на Органите за удостоверяване

Съгласно Регламента за eIDAS, непосредствена и приоритетна задача е създаване на обща европейска система от доверителни списъци (TSL), която покрива квалифицираните удостоверяващи органи в страните-членки.

7. Интерфейси на Услугата за потребители и Доверяващи се страни

Услугата на ДКУУ ЕВРОТРЪСТ се предлага като уеб услуги (Web Services), които се достъпват и ползват чрез:

- OASIS DSS Интерфейс;
- GUI интерфейс

И при двата интерфейса Услугата се автентифицира (чрез удостоверение за сървър/удостоверение за автентичност на Уеб-сайт) пред приложението или клиента/браузъра.

Услугата не изисква автентификация на потребителя (приложение или клиент/браузър).

8. OASIS DSS Интерфейс

Услугата на ДКУУ ЕВРОТРЪСТ се достъпва и ползва чрез OASIS DSS интерфейс. Интерфейсът дефинира XML-команди Запитване/Отговор (Request/Response) за двата протокола:

- Протокол за подписване/подпечатване на документи с КЕП/КЕПечат;
- Протокол за валидация на подписан/подпечатени документи (валидация на КЕП/КЕПечат).

И двата протокола на OASIS DSS интерфейса използват транспортен протокол SOAP за обмен на XML-командите при подписване/подпечатване и при валидация на подписа/печата.

Спецификациите на DSS-интерфейса се регулират и поддържат от OASIS-консорциума.

8.1. Графичен интерфейс на потребител (GUI)

Услугата на ДКУУ ЕВРОТРЪСТ се достъпва и ползва чрез GUI (графичен потребителски интерфейс). При този интерфейс XML-командите на DSS-интерфейса използват HTTP POST за обмен/транспорт.

Използвайки GUI, клиент достъпва Услугата и може да посочи и зареди (upload) подписан документ с КЕП/КЕПечат, да избере параметрите на заявката и параметрите на отговор, след което да изпрати формираната XML-заявка/Request на Услугата чрез HTTP POST протокола.

9. Съответствие с Регламент (ЕС) N 910/2014

9.1. Валидиране на квалифицирани електронни подписи според eIDAS: чл. 26, 28 и 32

Изисквания в чл.26, 28 и 32 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 валидиране на удостоверенията изпълнява изискванията описани в ЕС 2015/1505 и ETSI 119 412-5 Приложение A.1 за ДКУУ, който издава квалифицирани удостоверения за електронен подпис.
Б) квалифицираното удостоверение е издадено от доставчик на квалифицирани удостоверителни услуги и е било валидно към момента на подписването	Процесът по валидиране на удостоверенията изпълнява изискванията описани в ЕС 2015/1505 и ETSI 119 412-5 Приложение A.1 за ДКУУ, който издава квалифицирани удостоверения за електронен подпис.
В) данните за валидиране на подписа съответстват на данните, предоставени от доверяващата се страна	Гарантира се чрез поддържаните формати за КЕП/КЕПечат.
Г) уникалният набор от данни, представляващи титуляря на електронния подпис в удостоверението, е надлежно предаден на доверяващата се страна	Подписващото удостоверение за КЕ/КЕПечат е включено в отговора от валидиранията за всеки поддържан протокол, съгласно този документ.
Д) ако към момента на подписването е бил използван псевдоним, то това е ясно указано на доверяващата се страна	Тъй като индикацията на псевдоним в полето Subject се използва само по изрично желание на клиента и предварителна договорка между него и ДКУУ, се спазват изискванията на ETSI 119 412-2 съгласно този документ.
Е) електронният подпис е създаден от устройство за създаване на квалифициран електронен подпис	Процесът по валидиране на удостоверенията изпълнява изискванията описани в ЕС 2015/1505 за ДКУУ, издаващи квалифицирани удостоверения. Прави се проверка за

	изисквания тип на SSCD (QSCD).
Ж) целостта на подписаните данни не е застрашена	Гарантира се чрез поддържания модел за валидиране, посочен в този документ.
З) изискванията по член 26 са били изпълнени към момента на подписването.	Виж по-долу (за чл. 26)
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	Процесът по валидиране на КЕП/КЕПечат и статус-индикацията след проверката са описани в този документ.
Член 28 *Квалифицирани удостоверения за електронни подписи*	
1. Квалифицираните удостоверения за електронни подписи отговарят на изискванията, предвидени в Приложение I.	Съответства на изискванията от ETSI 119 412-5, Приложение A.1
2. Квалифицираните удостоверения за електронни подписи не подлежат на каквото и да било задължително изискване, което надхвърля изискванията, предвидени в приложение I.	Процесът по валидиране на удостоверенията изпълнява изискванията описани в ЕС 2015/1505 за доверителни списъци. Не се изискват допълнителни проверки, освен тези посочени в Приложение I на Регламента.
3. Квалифицираните удостоверения за електронни подписи могат да включват допълнителни незадължителни специфични данни. Тези данни не засягат оперативната съвместимост и признаването на квалифицираните електронни подписи.	Не се изискват допълнителни проверки, освен тези посочени в Приложение I на Регламента.
4. Ако квалифицирано удостоверение за електронни подписи бъде отменено след първоначалното активиране, то губи валидността си от момента на отмяната и неговият статут не може да бъде възстановен при никакви обстоятелства.	Съобразно Политиката и Практиката за квалифицирани удостоверителни услуги за КЕП/КЕПечат.
5. Държавите членки могат да определят	Според ETSI TS 110 102-1 ако по пътя на валидиране на

национални правила относно временното спиране на валидността на квалифицирано удостоверение за електронен подпис при спазване на следните условия:	удостоверение, се получи резултат/отговор за грешна валидация, защото удостоверение за КЕП/КЕПечат е спряно, Услугата ще прекрати процеса на валидиране. Статус-индикацията е INDETERMINATE и допълнителен код TRY_LATER с времето на спиране и, ако има такова, полето nextUpdate на CRL или OCSP -отговор се използва за определяне на последващото валидиране.
А) ако квалифицирано удостоверение за електронен подпис бъде временно спряно, то губи валидността си за срока на спирането	
Б) срокът на спирането се отбелязва ясно в базата данни за удостоверенията, а статутът на спряното удостоверение е видим за срока на спирането в рамките на услугата, предоставяща информация за статута на удостоверението	
Член 26 **Изисквания към усъвършенстваните електронни подписи**	
Усъвършенстваният електронен подпис отговаря на следните изисквания:	Гарантира се чрез поддържаните формати за КЕП/КЕПечат.
А) свързан е по уникален начин с титуляря на подписа	Гарантира се чрез поддържаните формати за КЕП/КЕПечат.
Б) може да идентифицира титуляря на подписа	Гарантира се чрез поддържаните формати за КЕП/КЕПечат.
В) 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	Гарантира се чрез поддържаните формати за КЕП/КЕПечат.
Г) свързан е с данните, които са подписани с него, по начин, позволяващ да бъде открита всяка последваща промяна в тях	Гарантира се чрез поддържаните формати за КЕП/КЕПечат.

Регистриране на измененията																					
Страница																					
Валидно изменение																					