ПОЛИТИКА ЗА ПРЕДОСТАВЯНЕ НА УСЛУГА ЗА КВАЛИФИЦИРАНО ВАЛИДИРАНЕ НА КВАЛИФИЦИРАНИ ЕЛЕКТРОННИ ПОДПИСИ И КВАЛИФИЦИРАНИ ЕЛЕКТРОНИ ПЕЧАТИ

НА

КВАЛИФИЦИРАНИЯ ДОСТАВЧИК НА УДОСТОВЕРИТЕЛНИ УСЛУГИ

ИНФОНОТАРИ ЕАД

ВЕРСИЯ 1.0

В сила от 01.07.2021 г.

СЪДЪРЖАНИЕ

1. ВЪВЕДЕНИЕ

Основната цел на настоящия документ ПОЛИТИКА ЗА ПРЕДОСТАВЯНЕ НА УСЛУГА ЗА КВАЛИФИЦИРАНО ВАЛИДИРАНЕ НА КВАЛИФИЦИРАНИ ЕЛЕКТРОННИ ПОДПИСИ И КВАЛИФИЦИРАНИ ЕЛЕКТРОНИ ПЕЧАТИ (Политика) на Доставчика на удостоверителни услуги ИНФОНОТАРИ ЕАД (ИНФОНОТАРИ/Доставчик) е:

- да опише и направи публични правилата, условията и процедурите, които ИНФОНОТАРИ е въвело и изпълнява при предоставяне на квалифицираната услуга за валидиране на квалифицирани удостоверения, квалифициран електронен подпис, квалифициран/печат (Услуга/Услуга за валидиране);
- да предостави средства за установяване на съответствието на дейността на Доставчика, включително нейната надеждност и сигурност, с разпоредбите и изискванията на Регламент (ЕС) 910/2014 и изискванията на приложимото българско законодателство.
- да уточни основните формати на електронните подписи/печати, към които е приложима Услугата;
- да определи протоколите, интерфейсите и връзките с други квалифицирани услуги (например CRL, OCSP, TSA), предоставящи информация на Услугата за валидиране.

Политиката е публичен документ и може да бъде променяна при необходимост, като всяка промяна в нея е публично достъпна от всички заинтересувани лица на адрес: http://repository.infonotary.com и https://repository.infonotary.com

1.2. СЪОТВЕТСТВИЕ

Политиката е изготвена в съответствие с разпоредбите и изискванията на изброените по-долу европейски и национални нормативни документи и стандарти:

- Регламент 910/2014 на Европейския парламент и Съвет относно удостоверителните услуги и се позовава на информация, относно подготвяните в съответствие с този Регламент международни препоръки, спецификации и стандарти;
- Закон за електронния документ и електронните удостоверителни услуги;
- РЕШЕНИЕ ЗА ИЗПЪЛНЕНИЕ (ЕС) 2015/1506 НА КОМИСИЯТА за определяне на спецификации, отнасящи се до форматите на усъвършенствани електронни подписи и усъвършенствани печати, които трябва да бъдат признати от органите от публичния сектор съгласно член 27, параграф 5 и член 37, параграф 5 от Регламент (ЕС) № 910/2014;

- EN 319 401 v2.1.1 General Policy Requirements for Trust Service Providers;
- EN 319 411 Policy and security requirements for Trust Service Providers issuing certificates;
- 319 411-2 v2.1.1: Requirements for trust service providers issuing EU qualified certificates;
- EN 319 412 Certificate Profiles;
- ETSI TS 119 441 Policy Requirement for TSP providing signature validation services;
- ETSI TS 119 442: "Electronic Signatures and Infrastructures (ESI); Protocol for TSPs providing signature validation services";
- ETSI TS 119 101: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for applications for signature creation and signature validation";
- ETSI EN 319 102-1: Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures, Part1: Creation and Validation;
- ETSI TS 119 102-2: Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures, Part 2: Signature Validation Report;
- RFC 6960 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP.

1.3. ОСНОВНИ ПОЛОЖЕНИЯ

1.3.1. Доставчик на удостоверителни услуги

ИНФОНОТАРИ ЕАД е Доставчик на квалифицирани удостоверителни услуги съгласно Регламент (ЕС) № 910/2014 и е с предоставен квалифициран статут от националния Надзорен орган при предвидените в Регламент № (ЕС) 910/2014 условия и в съответствие със националното право.

ИНФОНОТАРИ ЕАД е търговско дружество, вписано в Търговския регистър при Агенция по вписванията с ЕИК 131276827. Дружеството е със седалище и адрес на управление в гр. София, ул. „Иван Вазов" №16, телефон за контакт: +359 2 9210857, интернет адрес: http://www.infonotary.com.

Дружеството използва в своята търговска дейност запазената търговска марка на InfoNotary.

Като квалифициран доставчик ИНФОНОТАРИ ЕАД извършва следните дейности и предоставя следните квалифицирани удостоверителни услуги:

- Услуги по издаване и управление на квалифицирани удостоверения за квалифициран и усъвършенстват електронен подпис и печат;

- Услуги по издаване и управление на квалифицирани удостоверения автентичност на уебсайт;
- Услуги по издаване и управление на квалифицирани електронни времеви печати;
- Услуги по издаване и управление на квалифицираното PSD2 удостоверения;
- Услуги за валидиране на квалифицирани удостоверения, квалифициран електронен подпис и квалифициран електронен печат:
  - предоставяне на услуги за проверка в реално време на статуса на издадено от ИНФОНОТАРИ квалифицирано удостоверение (OCSP);
  - предоставяне на услуги за проверка в реално време на статуса на квалифицирано удостоверение, квалифициран електронен подпис и квалифициран електронен печат (InfoNotary Qualified Validation Service - IQVS).

При осъществяване на дейностите по издаване и управление на квалифицирани удостоверения и Услугата за валидиране, ИНФОНОТАРИ ЕАД прилага внедрените в дружеството Система за управление, сертифицирана по стандарта ISO/IEC 9001:2008 и Система за управление сертифицирана по стандарта ISO/IEC 27001:2013.

1.4. ИМЕНУВАНЕ И ИДЕНТИФИКАЦИЯ НА ДОКУМЕНТА

Документа „Политика за предоставяне на услуга за квалифицирано валидиране на квалифицирани електронни подписи и квалифицирани електрони печати на ИНФОНОТАРИ ЕАД", се именува "InfoNotary CP QVS" и се идентифицира посредством следния идентификатор на обект:

Policy name	Identifier (OID)
InfoNotary Qualified Validation Service (IQVS)	1.3.6.1.4.1.22144.3.5.2 0.4.0.19172.1

1.5. УПРАВЛЕНИЕ НА УДОСТОВЕРИТЕЛНАТА ПОЛИТИКА НА ДОСТАВЧИКА

Удостоверителната политика на Доставчика се определят от Съвета на директорите на ИНФОНОТАРИ ЕАД.

Всички промени, редакции и допълнения на настоящата Политика се приемат от Съвета на директорите на ИНФОНОТАРИ ЕАД.

Новите версии на документа се публикуват след неговото одобрение в Документния регистър на Доставчика и е публично достъпен на адрес: http://repository.infonotary.com и https://repository.infonotary.com.

Всички коментари, запитвания за информация и разяснения по настоящата Политиката могат да бъдат отправяни на адрес:

„ИНФОНОТАРИ" ЕАД
1000 София, България ул. „Иван Вазов" №16
тел:+359 2 9210857
e-mail: legal@infonotary.com
URL: www.infonotary.com

1.6. УЧАСТНИЦИ В УСЛУГАТА ЗА ВАЛИДИРАНЕ

Страните, участващи в процеса на валидиране са:

- Удостоверяващ орган и Оперативен удостоверяващ орган за валидиране;
- Потребители/Абонати и Доверяващи се страни;
- Външни източници за процеса на валидиране:
  - Страни, които са подписали/подпечатели документ(и);
  - Вътрешни услуги на Доставчика (удостоверяващи органи – CA, TSA, CRL/OCSP);
  - Национален Доверителен списъци (Trusted Lists);
  - Европейски доверителен списък (EU Trusted Lists).

1.6.1. Удостоверяващ орган

InfoNotary е Удостоверяващият орган на Доставчика на удостоверителни услуги, извършващ следните дейности: издаване на удостоверения за електронен подпис и електронен печат, управление на удостоверенията, включващо спиране, възобновяване и прекратяване действието на удостоверения, валидиране на удостоверения, водене на регистър за издадените удостоверения и осигуряващ достъпа и средствата за ограничение на достъпа до удостоверения.

Удостоверяващият орган (root CA) контролира удостоверителните политики на Доставчика, определящи съдържащата се в различните типове удостоверения за крайни потребители индивидуализираща Титуляря информация, ограничения в приложението и отговорности.

Удостоверяващият орган издава различни типове удостоверения, съобразно удостоверителните политики, посредством диференцирани свои **Оперативни удостоверяващи органи** (operational CAs).

1.6.2. Оперативен удостоверяващ орган за валидиране (InfoNotary Qualified Validated Service)

InfoNotary Qualified Validated Service е оперативен валидиращ орган, който обслужва процеса на проверка на квалифицирани удостоверения, квалифициран електронен подпис, квалифициран електронен печат и усъвършенстват основан на квалифицирано удостоверение. Също така той издава и подписва квалифицираното удостоверение за усъвършенстван електронен печат, с което се подписват докладите (резултатите) от извършените проверки за статуса на проверените удостоверения, подписи и печати.

Удостоверението за публичния ключ на Оперативния Удостоверяващ Орган за предоставяне на услуги по валидиране (**InfoNotary Qualified Validation**

Services CA), **OID: 1.3.6.1.4.1.22144.3.5**, се подписва с частния ключ на базовия удостоверяващ орган **InfoNotary TSP Root**, **OID: 1.3.6.1.4.1.22144.3**.

Удостоверението на Оперативния удостоверяващ орган **InfoNotary Qualified Validated Service** съдържа следната основна информация:

InfoNotary Qualified Validation Services CA			
Основни x509 атрибути:			
Атрибут			Стойност
Версия			3 (0x02)
Сериен номер			Уникален за регистъра на Доставчика; 16-байтово число
Начало на периода на валидност			Дата и час на подписване
Край на периода на валидност			Дата и час на подписване + 19 години
Алгоритъм на електронния подпис			SHA256/RSA
Атрибути на Издателя:			
Атрибут			Стойност
Common Name	Име	CN	InfoNotary TSP Root
Domain Component	Домейн компонент	DC	qualified-root-ca
Country Name	Държава	C	BG
Locality Name	Град	L	Sofia
Organization Name	Организация	O	InfoNotary PLC
Organizational Unit Name	Организационно звено	OU	Qualified TSP
Organization Identifier	Идентификатор на организацията (ЕИК)	2.5.4.97	NTRBG-131276827
Атрибути на Титуляря (x509 Subject DN):			
Атрибут			Стойност
Common Name	Име	CN	InfoNotary Qualified Validation Services CA
Domain Component	Домейн компонент	DC	qualified-validation-ca

Country Name	Държава	C	BG
Locality Name	Град	L	Sofia
Organization Name	Организация	O	InfoNotary PLC
Organizational Unit Name	Организационно звено	OU	Qualified TSP
Organization Identifier	Идентификатор на организацията (ЕИК)	2.5.4.97	NTRBG-131276827

Допълнителни атрибути на x509 разширения (x509v3 extensions):	
Атрибут	Стойност
Basic Constraints (Critical)	Subject Type=CA
Key Usage (Critical)	Certificate Signing, CRL Signing
Public Key	RSA 3072 bits
Authority information Access	[1] Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.infonotary.com/qualified
CRL Distribution Point (Non Critical)	[1] CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.infonotary.com/crl/qualified-root-ca.crl
Certificate Policies (Non Critical)	[1] Certificate Policy: Policy Identifier=1.3.6.1.4.1.22144.3.5 [1.1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://repository.infonotary.com/cps/qualified-tsp.html Unotice: InfoNotary Qualified Validation Services CA
Subject Key Identifier	subjectKeyIdentifier
Authority Key Identifier	authorityKeyIdentifier=keyid,issuer

1.6.3. Доверяващи се страни - Потребители/Абонати

„Доверяващи се страни", като цяло са физически или юридически лица, които се доверяват на удостоверителните услуги, предоставяни от Доставчици на удостоверителни услуги.

В конкретния случай на Услугата за валидиране доверяващите се страни могат да бъдат:

„Потребител" и физическо или юридическо лице, което използва Услугата за валидиране достъпна през уеб базиран потребителски интерфейс на адрес: https://www.infonotary.com/in-validator.

„Абонат" е физическо или юридическо лице, което има сключен писмен договор с Доставчика за предоставяне на Услугата за валидиране, която е реализирана като уеб услуга (web service) за автоматично валидиране.

Доверяващите се страни следва да имат умения да ползват Услугата за валидиране, да вземат под внимание и да съобразяват действията си с всички ограничения на ползването на Услугата посочени в тази Политика, както и да се доверяват на издаваните от Доставчика резултати (докладите) от извършените проверки на квалифицирани удостоверенията, квалифициран електронен подпис и електронен печат.

1.6.4. Ползване и достъпност на услугите

Когато е практически осъществимо и в зависимост от удостоверителната услуга, която е заявена или предоставена на Абонат, както и продукти, свързани с нейното получаване, Доставчика осигурява възможност за ползване от хора с увреждания. Достъпността до услугите и продуктите се осигурява без това да накърнява или изключва спазване на изискванията за сигурност, приложимост и съответствие с разпоредбите на Регламент (ЕС) №910/2014, националното законодателство и вътрешните политики и процедури на Доставчика.

1.6.5. Ограничения на удостоверителното действие

Изрично е забранено на трети страни да използват услугите за валидиране на "ИНФОНОТАРИ" ЕАД, за да предоставят услуги за валидиране на други трети страни. Доставчикът не носи отговорност за вреди, настъпили вследствие на ползването на Услугата за валидиране, извън разрешената употреба и съобразно ограниченията на приложение по отношение на нейното предназначение и ще доведе до анулиране на гаранциите, които "ИНФОНОТАРИ" ЕАД дава на потребителите и на Доверяващите се страни.

1.7. ТЕРМИНИ И СЪКРАЩЕНИЯ

Валидиране	Процес на проверка и потвърждаване на валидността на квалифицирано удостоверение, квалифициран електронен подпис или квалифициран електронен печат
Квалифицирано валидиране	Услугата по валидиране се предоставя от доставчик на квалифицирани удостоверителни услуги, в съответствие с Регламент 910/2014 (чл. 32, 33 и 40)
Данни за валидиране	Данни, които се използват за валидиране на електронен подпис или електронен печат.
Ограничение за валидиране	Технически критерии, спрямо които може да бъде валидиран електронен подпис/печат
Доклад за валидиране	Доклад от процеса на валидиране на подписа/печата, който се представя на потребителя
Статус на валидиране на електронен подпис/печат	Един от следните статус-индикатори, съдържащи се в доклада – ВАЛИДАН (TOTAL-PASSED), НЕВАЛИДЕН (TOTAL-FAILLED) или НЕОПРЕДЕЛЕН (INDETERMINATE)
Електронен печат	Данни в електронна форма, които се добавят към други данни в електронна форма или са логически свързани с тях, за да се гарантират произходът и целостта на последните.
Електронен подпис	Данни в електронна форма, които се добавят към други данни в електронна форма или са логически свързани с тях, и които титулярят на електронния подпис използва, за да се подписва.
Квалифициран електронен времеви печат	Електронен времеви печат, който отговаря на следните изисквания: а) обвързва датата и часа с данните по начин, който до голяма степен изключва възможността за незабелязана промяна на данните; б) основава се на източник на точно време, свързан с координираното универсално време; и в) подписан е с усъвършенстван електронен подпис или е подпечатан с усъвършенстван електронен печат на доставчик на квалифицирани удостоверителни услуги или с друг равностоен метод.

Квалифициран електронен печат	Усъвършенстван електронен печат, който е създаден от устройство за създаване на квалифициран електронен печат и се основава на квалифицирано удостоверение за електронен печат.
Квалифициран електронен подпис	Усъвършенстван електронен подпис, който е създаден от устройство за създаване на квалифициран електронен подпис и се основава на квалифицирано удостоверение за електронни подписи
Квалифицирано удостоверение за електронен подпис	Удостоверение за електронен подпис, което се издава от доставчик на квалифицирани удостоверителни услуги и отговаря на изискванията, предвидени в нормативната уредба.
Квалифицирано удостоверение за автентичност на уебсайт	Удостоверение за автентичност на уебсайт, което се издава от доставчик на квалифицирани удостоверителни услуги и отговаря на изискванията, предвидени в приложение IV на Регламент (ЕС) 910/2014.
Квалифицирано удостоверение за електронен печат	Удостоверение за електронен печат, което се издава от доставчик на квалифицирани удостоверителни услуги и отговаря на изискванията, предвидени в приложение III на Регламент (ЕС) 910/2014.
Удостоверение за електронен печат	Електронен атестат, който свързва данните за валидиране на електронен печат с юридическо лице и потвърждава името на това лице.
Удостоверение за електронен подпис	Електронен атестат, който свързва данните за валидиране на електронен подпис с физическо лице и потвърждава най-малко името или псевдонима на това лице
Удостоверителна услуга	Електронна услуга, обикновено предоставяна срещу възнаграждение, която се състои в: - създаването, проверката и валидирането на електронни подписи, електронни печати или електронни времеви печати, услуги за електронна препоръчана поща, както и удостоверения, свързани с тези услуги; или - създаването, проверката и валидирането на удостоверения за автентичност на уебсайт; или - съхраняването на електронни подписи, печати или удостоверения, свързани с тези услуги.

КРС	Комисия за регулиране на съобщенията
ПИН	Персонален Идентификационен Номер
Практика	Практика при предоставяне на квалифицирани удостоверителни услуги **InfoNotary Qualified CPS**
Политика	Политика за предоставяне на услуга за квалифицирано валидиране на квалифицирани електронни подписи и квалифицирани електрони печати
Регламент	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.
Регламент GDPR	Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните)

СЪКРАЩЕНИЯ

ASN.1	Abstract Syntax Notation One – Абстрактен език за описание на обекти в удостоверенията
CA	Certification Authority – Удостоверяващ орган
CC	Common Criteria – Общи критерии
CEN	European Committee for Standardization - Европейски стандартизационен комитет
CENELEC	European Committee for Electronic Standardization - Европейски комитет за електротехническа стандартизация
CP	Certificate Policy – Политика за предоставяне на удостоверителни услуги
CPS	Certification Practice Statement – Практика при предоставяне на удостоверителни услуги
CRL	Certificate Revocation List – Списък на спрените и прекратени удостоверения
DN	Distinguished Name – Уникално име
ETSI	European Telecommunications Standards Institute - Европейски институт за телекомуникационни стандарти
EU	European Union - Европейски съюз
FIPS	Federal Information Processing Standard – Федерален стандарт за обработка на информация
IEC	International Electrotechnical Commission - Международна електротехническа комисия
ISO	International Standardization Organization - Международна организация за стандартизация
LDAP	Lightweight Directory Access Protocol – Протокол за опростен достъп до регистър
OID	Object Identifier – Идентификатор на обект
OCSP	On-line Certificate Status Protocol – Протокол за проверка на статуса на удостоверения в реално време

PKCS	Public Key Cryptography Standards – Криптографски стандарт за пренос на публичен ключ
PKI	Public Key Infrastructure – Инфраструктура на публичния ключ
RA	Registration Authority – Регистриращ орган
RSA	Rivest-Shamir-Adelman – Криптографски алгоритъм за създаване на подпис
SHA	Secure Hash Algorithm – Хеш-алгоритъм за извличане на хеш-идентификатор
SSL	Secure Socket Layer – Сигурен канал за предаване на данни
URL	Uniform Resource Locator – Единен ресурсен локатор

1.8. УПОТРЕБА НА УДОСТОВЕРЕНИЯТА НА УСЛУГАТА ЗА ВАЛИДИРАНЕ

Услугата за валидиране използва следните служебни удостоверения:

- Удостоверение на Оперативния Удостоверяващ Орган за предоставяне на услуги по валидиране (**InfoNotary Qualified Validation Services CA);**
- Квалифицирано удостоверение за усъвършенстван електронен печат;
- Удостоверение за автентичност на уеб сайт.

С удостоверението на Оперативния Удостоверяващ Орган**/InfoNotary Qualified Validation Services CA** се подписва квалифицираното удостоверение за усъвършенстван електронен печат.

С квалифицираното удостоверение за електронен печат се подписват докладите (резултатите) от извършените проверки за статуса на проверените удостоверения, подписи и печати.

Удостоверението за автентичност на уеб сайт извършва онлайн автентикация на Услугата за валидиране пред Потребителя и осигурява защитен комуникационен канал/защитена сесия с Потребителя при ползване на Услугата.

Квалифицираното удостоверение за усъвършенстван електронен печат, има следния профил:

InfoNotary Qualified Validation Stamp			
Основни x509 атрибути:			
Атрибут			Стойност
Версия			3 (0x02)
Сериен номер			Уникален за регистъра на Доставчика; 16- байтово число
Начало на периода на валидност			Дата и час на подписване
Край на периода на валидност			Дата и час на подписване + 5 год.
Алгоритъм на електронния подпис			SHA256/RSA
Атрибути на Издателя:			
Атрибут			Стойност
Domain Component	Домейн компонент	DC	qualified-validation-ca

Common Name	Име	CN	InfoNotary Qualified Validation Services
Country Name	Държава	C	BG
Locality Name	Град	L	Sofia
Organization Name	Организация	O	InfoNotary PLC
Organizational Unit Name	Организационно звено	OU	Qualified TSP
Organization Identifier	Идентификатор на организацията (ЕИК)	2.5.4.97	NTRBG-131276827
Атрибути на Титуляря (x509 Subject DN):			
Атрибут			Стойност
Domain Component	Домейн компонент	DC	qualified-validation-ca
Common Name	Име	CN	InfoNotary Qualified Validation Stamp
Country Name	Държава	C	BG
Locality Name	Град	L	Sofia
Organization Name	Организация	O	InfoNotary PLC
Organizational Unit Name	Организационно звено	OU	InfoNotary Qualified Validation Services
Organization Identifier	Идентификатор на организацията (ЕИК)	2.5.4.97	NTRBG-131276827
Допълнителни атрибути на x509 разширения (x509v3 extensions):			
Атрибут			Стойност
Basic Constraints (Critical)	End entity		
Key Usage (Critical)	Digital Signature, Non-Repudiation		
Public Key	RSA 2048 bits		
Authority Key Identifier	AuthorityKeyIdentifier		
Subject Key Identifier	SubjectKeyIdentifier		
Authority information Access	[1] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)		

	Alternative Name: URL= https://repository.infonotary.com/qualified-validation-ca.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://ocsp.infonotary.com/qualified
CRL Distribution Point (Non Critical)	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.infonotary.com/crl/ qualified-validation-ca.crl
	[1]Certificate Policy: Policy dentifier=0.4.0.194112.1.1 [2]Certificate Policy: Policy Identifier=1.3.6.1.4.1.22144.3.5.2 [2.1] Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://repository.infonotary.com/cps/qualified-tsp.html Unotice: InfoNotary Qualified Validation Service [3] Certificate Policy: Policy dentifier=0.4.0.19172.1
Qualified Certificate Statement (Non Critical)	id-etsi-qcs-semanticsId-Legal (oid=0.4.0.194121.1.2) id-etsi-qcs-QcCompliance (oid=0.4.0.1862.1.1) id-etsi-qct-eseal (oid=0.4.0.1862.1.6.2) (oid=0.4.0.1862.1.2) id-etsi-qcs-QcPDS (oid=0.4.0.1862.1.5) PDSLocation=https://repository.infonotary.com/pds/pds_bg.pdf Language=bg PDSLocation=https://repository.infonotary.com/pds/pds_en.pdf Language=en
Extended Key Usage (Non Critical)	

2. ОПИСАНИЕ НА УСЛУГИТЕ ЗА ВАЛИДИРАНЕ

Квалифицираната услуга за валидиране на ИНФОНОТАРИ позволява да се потвърди валидността на квалифицирано удостоверение, квалифициран електронен подпис и квалифициран електронен печат при условие че:

- удостоверението, за създаване на подписа/печата към момента на подписване/подпечатване, е квалифицирано в съответствие с приложение I към Регламента 910/2014;
- квалифицираното удостоверение е издадено от квалифициран доставчик на удостоверителни услуги и е било валидно към момента на подписване;
- данните за валидиране на подписа съответстват на данните, предоставени от доверяващата се страна;
- уникалният набор от данни, представляващи Титуляря на електронен подпис/Създателя на печат в удостоверението, е надлежно предаден на доверяващата се страна;
- ако към момента на подписването 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 нарушена;
- към момента на подписване са спазени изискванията за усъвършенстван електронен подпис (чл. 26 от Регламента).

Квалифицираната услуга за валидиране на ИНФОНОТАРИ осигурява възможност на Потребителите и Доверяващите се страни да получат резултата от процеса на валидиране (доклада) по автоматизиран начин с индикатор на състоянието, който е надежден и точен и е подпечатан с квалифицирано удостоверение за електронен печат на Доставчика.

Квалифицираната услуга за валидиране на ИНФОНОТАРИ проверява само техническата валидност на квалифицираното удостоверение, квалифицирания подпис и печат.

Техническата валидност на квалифицираното удостоверение, квалифицирания подпис и печат се проверява в съответствие с процеса, описан в документа ETSI TS 319 102 и ETSI TS 119 172-4 и се потвърждава чрез подписване на резултата (доклада) с квалифицирано удостоверение за усъвършенстван електронен печат на Доставчика.

Квалифицираната услуга за валидиране позволява проверка на следните формати и профили подписи:

Формат/Профил	**BASELINE_B**	**BASELINE_T**	**BASELINE_LT**	**BASELINE_LTA**
CAdES	√	√	√	√
XAdES	√	√	√	√
PAdES	√	√	√	√
ASiCS/ ASiCE	√	√	√	√

Всички удостоверения и свързаните с тях вериги се валидират спрямо Европейският доверителен списък (EU MS TSL- https://esignature.ec.europa.eu/efda/tl-browser/#/screen/home).

2.1. КОМПОНЕНТИ НА УСЛУГАТА ЗА ВАЛИДИРАНЕ

Квалифицираната услуга за валидиране на ИНФОНОТАРИ (**InfoNotary Qualified Validation Service - IQVS**) включва следните софтуерни компоненти, съгласно ETSI TS 319 102:

- Приложение/клиент за валидиране на подписа/печата – софтуерен агент от страна на Потребителя. Може да бъде софтуерен или уеб клиент, който работи през браузър и има следната функционалност:
  - Създава заявки за валидиране;
  - Изпълнява протокола за валидиране от страна на потребителя;
  - Представя доклада за валидиране.
- Сървър за валидиране – изпълнява следната функционалности от страна на Доставчика:
  - Получава електронните подписи/печати и други входящи данни от клиента за валидиране;
  - Извършва процеса на валидиране съобразно приложимата Политика и ограничения, като използва процеси, алгоритми и протоколи за валидиране, съгласно ETSI EN 319 102-1 и ETSI TS 119 442;
  - Комуникира с вътрешни и външни източници на Услугата – CRL/OCSP на Удостоверяващ Орган, TSA, EU Trusted List;
  - Генерира доклад и индикатор на статуса на валидиране на подписа/печата.

2.2. ИНТЕРФЕЙС И ПРЕДОСТАВЯНЕ НА УСЛУГАТА ВАЛИДИРАНЕ

Услугата за валидиране е достъпна на адрес - https://www.infonotary.com/validate.

Квалифицираната услуга за валидиране на ИНФОНОТАРИ се предоставя чрез:

- Уеб базиран потребителски интерфейс с графичен интерфейс (Signature Validation Application - SVA), и който използва защитен комуникационен канал/защитена сесия (HTTPS протокол/удостоверение за автентичност на уеб сайт) за връзка със сървъра за валидиране. След като достъпи Услугата, Потребителят (Доверяващата се страна) зарежда (upload) електронно подписан/подпечатан файл или удостоверение, което желае на провери, избира параметри на заявката и изпраща заявката към сървъра за валидиране.
- Уеб услуга (web service) и се предоставя посредством приложен програмен интерфейс за автоматично валидиране, като условията се уреждат в договор между Доставчика и Доверяваща се страна.

2.3. ПРОЦЕС НА ВАЛИДИРАНЕ

Процесът на валидиране преминава през следните стъпки съгласно ETSI TS 319 172-1:

Заявките за валидиране на електронен подпис/печат и отговорите на тези заявки ползват комуникацията клиент-сървър. Протоколът за валидиране е в съответствие с ETSI EN 119 442.

Стъпка 1: SVA/уеб клиентът генерира и изпраща заявка за валидиране, която съдържа подписания/подпечатания документ или изпраща документ и подпис;

Стъпка 2: Сървърът за валидиране извършва валидиране на електронния подпис/печат, като използва вътрешни услуги на Доставчика (CRL, OCSP, TSA) или външни услуги на други доставчици или на външни източници на удостоверения (Европейски доверителен списък).

Стъпка 3: Сървърът за валидиране генерира и изпраща доклад от валидирането. Докладът е подпечатан с квалифицирано удостоверение за електронен печат на Инфонотари.

Стъпка 4: Web-клиентът визуализира доклада от валидиране в pdf-формат и той може да бъде запазен, локално на компютър на потребителя, или да бъде разпечатен.

Услугата за валидиране поддържа следните процеси на валидиране на квалифицирани електронни подписи и печати в различни формати:

- Процес на валидиране на подпис/печат с базов формат/профил BASELINE;
- Процес на валидиране на времеви печат;
- Процес на валидиране на подпис/печат с профил BASELINE_T и BASELINE_LT;
- Процес на валидиране на подпис/печат с профил BASELINE_LTA.

За всеки формат на квалифициран електронен подпис/печати, Услугата за валидиране изпълнява последователно следните действия:

- Извършва процес на валидиране на електронни подпис/печат с разширен формат - BASELINE_T, BASELINE_LT и BASELINE_LTA;
- Извършва процес на валидиране на електронни подпис/печат с базов

формат – BASELINE;

- Ако статусът на валидиране от избрания процес на валидиране е ВАЛИДЕН (PASSED), се връща статус-индикатор ВАЛИДЕН (TOTAL-PASSED) и доклад от валидиране;
- Ако статусът на валидиране от избрания процес на валидиране е НЕВАЛИДЕН (FAILED) се връща статус-индикатор НЕВАЛИДЕН (TOTAL-FAILED) и доклад от валидиране;
- Ако статусът на валидиране от избрания процес на валидиране не е ВАЛИДЕН или НЕВАЛИДЕН се връща статус-индикатор НЕОПРЕДЕЛЕН (INDETERMINATE) и доклад от валидиране.

2.4. СТАТУС ИНДИКАТОРИ И ДОКЛАД

2.4.1. Статус индикатори

Статусът на валидиране на квалифицираният подпис/печат може да бъде:

Информация вписана в доклада		**Значение**
Статус-индикатори	**Данни свързани с информацията в доклада**	
TOTAL-PASSED ВАЛИДЕН	Процесът на валидиране извежда валидираната удостоверителна верига, включително удостоверението за електронен подпис/печат, използвани в процеса на валидиране. Освен това процесът на валидиране може да предостави резултата от валидирането за всяко от ограниченията за валидиране. Процесът на валидиране трябва да осигури DA достъп до подписаните атрибути, присъстващи в подписа, самоличността на подписалия.	Процесът на валидиране на подписите/печатите показва индикатор TOTAL-PASSED въз основа на следните съображения: • проверката на формата е успешна; • успешни криптографски проверки на подписа (включително проверки на хеш на отделни обекти от данни, които са подписани непряко); • всички ограничения, приложими към удостоверението на подписващия, са положително потвърдени; и • подписът/печатът е валидиран успешно спрямо ограниченията за валидиране и следователно се счита за съответстващ на тези ограничения.
TOTAL-FAILED НЕВАЛИДЕН	Процесът на валидиране извежда допълнителна информация, поясняваща статусът TOTAL-FAILED за всяко от валидиращите ограничения, взети предвид, и за които са представени отрицателни резултати.	Процесът на валидиране на подписите/печатите показва индикатор TOTAL-FAILED, тъй като проверката на формата е неуспешна, криптографските проверки на подписа/печата са неуспешни (включително проверки на хешове на отделни обекти от данни, които са били подписани индиректно) или е доказано, че удостоверението за подпис/печат е било невалидно по време на генериране на подписа/печата.

INDETERMINATE НЕОПРОДЕЛЕН	Процесът на валидиране извежда допълнителна информация, за да обясни индикаторът INDETERMINATE и да помогне на проверяващия да определи, където е уместно, какви данни липсват, за да завърши процеса на валидиране. По-специално, той трябва да предоставя индикации за резултатите от валидирането за онези ограничения за валидиране, които са били взети предвид и за които е възникнал неопределен резултат.	Наличната информация е недостатъчна, за да се установи дали подписът е ВАЛИДЕН или НЕВАЛИДЕН.

При статус на валидиране НЕВАЛИДЕН (TOTAL-FAILED) и НЕОПРЕДЕЛЕН (INDETERMINATE), докладът за валидиране съдържа и допълнителни индикатори, както следва:

Данни свързани с информацията в доклада			**Значение**
Основни статус-индикатори	**Под-индикатори**	**Под-индикатори свързани с информацията в доклада**	
TOTAL-FAILED НЕВАЛИДЕН	*FORMAT_FAILURE*	Процесът на валидиране предоставя всяка налична информация, според която анализът на подписа/печата е неуспешен.	Подписът/печатът не съответства на един от основните стандарти и криптографска проверка не може да го обработи.
	HASH_FAILURE	Процесът на валидиране осигурява идентификатор(и) (напр. URI или OID), еднозначно идентифициращ елемент в данните на подписания обект (като атрибутите на подписа или подписаните данни), който е причинил неуспеха.	Процесът на валидиране води до индикатор TOTAL-FAILED защото най-малко един хеш на подписан обект, който е включен в процеса на подписване/подпечатване не съответства на съответната хеш стойност в подписа/печата.
	SIG-CRYPTO-FAILURE	Процесът на валидиране извежда удостоверението за електронен подпис/печат, използвано в процеса на валидиране	Процесът на валидиране води до индикатор TOTAL-FAILED, тъй като стойността на подписа не може да бъде проверена с помощта на публичния ключ в удостоверението, използвано за подписване/подпечатване.
	REVOKED	Процесът на валидиране осигурява/проверява следното: - Удостоверителната верига, използвана в процеса на валидиране; - Времето и, ако е налице, причината за прекратяване на удостоверението за подпис/печат.	Процесът на валидиране води до индикатор TOTAL-FAILED защото: • удостоверението за подпис/печат е прекратено; и • има доказателство, че подписът/печатът е създаден след времето за прекратяване.
INDETERMINATE	*SIG_CONSTRAINTS_FAILURE*	Процесът на валидиране осигурява следното: Наборът от ограничения, които не са изпълнени от подписа/печата	Процесът на проверка на води до индикатор INDETERMINATE защото един или повече атрибути на подписа/печата не съответстват на ограничения за валидиране

	CHAIN_CONSTRAINTS_FAILURE	Процесът на валидиране извежда - Удостоверителната верига, използвана в процеса на валидиране. - Наборът от ограничения, които не изпълнени от удостоверителната верига	Процесът на проверка на води до индикатор INDETERMINATE защото удостоверителната верига, използвана в процеса на валидиране не съответства на свързаните с удостоверението ограничения за валидиране
	CERTIFICATE_CHAIN_GENERAL_FAILURE	Процесът на валидиране показва допълнителна информация относно причината довела до този индикатор	Процесът на проверка на води до индикатор INDETERMINATE защото проверката на удостоверителната верига извежда грешка, поради неустановена причина
	CRYPTO_CONSTRAINTS_FAILURE	Процесът на валидиране показва: • Идентификация на подпис/печат или удостоверение, които са генерирани с алгоритъм или размер на ключа под необходимото ниво на криптографска сигурност. • Ако е известено, времето, до което алгоритъмът или размерът на ключа са били считани за сигурни.	Процесът на проверка на води до индикатор INDETERMINATE, защото поне един от използваните алгоритми (за генериране на електронен подпис/печат или съответстващи удостоверения) или размерът на ключовете, които използват тези алгоритми, е под необходимото ниво за криптографска сигурност, както и: • 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 • електронен подпис/печат не е защитен с достатъчно надежден времеви печат, приложен преди времето, до което се смята че алгоритъма/ ключа, са били сигурни (ако такова време е известно).
	NOT_YET_VALID	-	Процесът на валидиране води до индикатор TOTAL-FAILED защото има доказателство, че подписът/печатът е създаден преди датата на издаване на удостоверението за подписване.
	EXPIRED	Процесът на валидиране извежда удостоверителната верига, използвана в процеса на валидиране	Процесът на проверка на води до индикатор INDETERMINATE защото има доказателство, че подписът/печатът е създаден след датата на валидност на удостоверението
	POLICY_PROCESSING_ ERROR	Процесът на валидиране показва допълнителна информация относно причината	Процесът на проверка на води до индикатор INDETERMINATE защото посоченият файл на приложимата политика не може да бъде обработен (не е

			достъпен, не може да се анализира и др.)
	SIGNATURE_POLICY_NOT_AVAILABLE	-	Процесът на проверка на води до индикатор INDETERMINATE защото електронният документ описващ политиката не е достъпен
	TIMESTAMP_ORDER_FAILURE	Процесът на валидиране извежда списъка с времеви печати, които не отговарят на ограниченията за подреждане.	Процесът на проверка на води до индикатор INDETERMINATE, защото не са спазени някои ограничения свързани с подреждане на времевите печати към подпис и/или подписаните данни
	NO_SIGNING_CERTIFICATE_FOUND	-	Процесът на проверка на води до индикатор INDETERMINATE, защото удостоверението за подпис/печат не може да бъде идентифицирано.
	NO_CERTIFICATE_CHAIN_FOUND	-	Процесът на проверка на води до индикатор INDETERMINATE, защото не е намерена удостоверителна верига свързана с идентифицираното удостоверение за подпис/печат
	REVOKED_NO_POE	-	Процесът на проверка на води до индикатор INDETERMINATE, защото удостоверението е прекратено към момента на валидиране. Алгоритъмът за валидиране, обаче не може да установи, дали времето на подписване е преди или след времето на прекратяване.
	REVOKED_CA_NO_POE	Процесът на валидиране осигурява: • удостоверителната верига, която включва прекратени удостоверения на удостоверяващ орган (CA certificate). • времето и причината за прекратяване.	Процесът на проверка на води до индикатор INDETERMINATE, защото е открита поне една удостоверителна верига, но удостоверението на CA е прекратено
	OUT_OF_BOUNDS_NO_POE	-	Процесът на проверка на води до индикатор INDETERMINATE, защото удостоверението за подпис/печат е изтекло или все още не е валидно към датата / часа на валидиране и Алгоритъмът за проверка на подпис/печат не може да установи, че времето за подписване е в рамките на интервала на валидност на удостоверението

	CRYPTO_CONSTRAINTS_FAILURE_NO_POE	Процесът на валидиране предоставя: Идентификация на електронен подпис/печат или на съответстващото удостоверение, генерирани с недопустима дължина на ключа или с алгоритъм, не отговарящи на криптографските изисквания за ниво на сигурност	Процесът на квалифицирано валидиране на електронни подписи и печати е INDETERMINATE, защото най-малко един от алгоритмите, които са били използвани в 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 валидиране извежда моментът, в който се очаква да бъде налице необходимата информация за прекратяване	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.

2.4.2 Доклад за валидиране

Резултатите от процеса на валидиране се представят в основен и подробен доклад, както и в машинно четим XML формат, в съответствие с ETSI TS 119 102-1.

Основният доклад съдържа:

- Политиката на валидиране;
- Статус/заключение;
- Дата и час по UTC на създаване на подписа/печата;
- Формата/профила на валидирания подпис/печат;
- Име на Титуляря/Създателя на подписа/печата;
- Информация за подписания/подпечатан документ (име, брой подписи).

Статусът/заключението, което SVA предоставя след валидиране на конкретния формат/профил на подписа/печата съгласно Политиката на валидиране е:

- ВАЛИДЕН (TOTAL-PASSED) – проверките на всички криптографски характеристики/параметри на подписа/печата са успешни, както и тези в съответствие с Политиката за валидиране;
- НЕВАЛИДЕН (TOTAL-FAILED) - проверките на всички криптографски характеристики/параметри на подписа/печата са неуспешни, или подписът/печатът е създаден след отмяна/прекратяване на квалифицираното удостоверение или форматът не съответства на някой базовите формати;
- НЕОПРЕДЕЛЕН (INDETERMINATE) – резултатите от отделните/единични проверки не позволяват подписът/печатът да бъде оценен като ВАЛИДЕН или НЕВАЛИДЕН.

Подробният доклад включва пълна информация за проверката на всички ограничения за валидиране, възможни стойности и допълнителни отчетни данни, свързани с тези стойности, съгласно Политиката за валидиране.

3. ОГРАНИЧЕНИЯ ЗА ВАЛИДИРАНЕ

Процесът на валидиране се контролира от набор от ограничения за валидиране. Тези ограничения се задават при управление на Услугата и могат да бъдат дефинирани в следните общи групи:

- X.509 ограничения за валидиране;
- криптографски ограничения на подписа/печата;
- ограничения относно елементите на подписа/печата.

3.1. ОБЩИ ОГРАНИЧЕНИЯ ЗА ВАЛИДИРАНЕ

Статус-индикаторът от валидацията, съдържащ се в доклада показва само дали даден подпис/печат е технически валиден съгласно настоящата Политика за валидиране. Максималният размер на подписан/подпечатен файл с данни, който ще се проверява е 10 MB (мегабайта).

3.2. X.509 ОГРАНИЧЕНИЯ ЗА ВАЛИДИРАНЕ

Услугата за валидиране изпълнява следните ограничения при валидиране на X.509 удостоверения (ETSI TS 119 172-1 [4], точка A.4.2.1, таблица A.2 ред m).

Ограничение	**Стойност на ограничението при валидиране**
m) 1. X509CertificateValidationConstraints: (m) 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..	EU Trusted List
(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. (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) (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 електронен подпис/печат	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:	eitherCheck

(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: - 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	
(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	Да

3.3. КРИПТОГРАФСКИ ОГРАНИЧЕНИЯ

Криптографските ограниченията на Услугата за валидиране относно използваните криптографски алгоритми и параметри, използвани при създаване на подписи/печати или използвани при валидиране на подписани обекти (ETSI TS 119 172-1 [4], точка A.4.2.1, таблица A.2 ред p.) са:

Ограничение	**Стойност на ограничението при валидиране**
(p)1. CryptographicSuitesConstraints: Това ограничение показва изисквания за алгоритми и параметри, използвани при създаване на подписи или използвани при валидиране на подписани обекти, включени в процеса на валидиране или увеличаване (напр. Подпис, сертификати, CRL, отговори на OCSP, времеви печати).	Съгласно ETSI TS 119 312

3.4. ОГРАНИЧЕНИЯ ОТНОСНО ЕЛЕМЕНТИТЕ НА ПОДПИСА/ПЕЧАТА

Услугата за валидиране поддържа всички допълнителни ограничения към посочените по-горе X.509 удостоверенията и криптографски ограниченията на

елементите на подпис/печат както е посочено в ETSI TS 119 172-1 [ETSI 119 172-1], точка A.4.2.1, таблица A.2 ред b.

Ограничение	Стойност на ограничението при валидиране
(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: (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
(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

4. СЪОТВЕТСТВИЕ С РЕГЛАМЕНТ 910/2014 (чл.32 и 33)

Изисквания съгласно чл. 32 от Регламент (EU) No. 910/2014	Изпълнение
Удостоверението в подкрепа на подписа към момента на подписването е било квалифицирано удостоверение за електронен подпис, отговарящо на Приложение I	Процесът на валидиране на удостоверенията е в съответствие с изискванията, описани в Решение 2015/1505 на ЕС и ETSI 319 412

Квалифицираното удостоверение е издадено от доставчик на квалифицирани удостоверителни услуги и е било валидно към момента на подписването	Процесът на валидиране на удостоверенията е в съответствие с изискванията, описани в Решение 2015/1505 на ЕС и ETSI 319 412
Данните за валидиране на подписа съответстват на данните, предоставени от доверяващата се страна	Процесът на валидиране предоставя на потребителите / Доверяващата се страна отчет, включващ удостоверение на Титуляра/ Създателя, съдържащ данните за валидиране (публичен ключ и др.).
Уникалният набор от данни, представляващи титуляря на електронния подпис в удостоверението, е надлежно предаден на доверяващата се страна	Процесът на валидиране предоставя на потребителите / Доверяващата се страна отчет, включващ удостоверение на Титуляра/ Създателя, съдържащ данните за валидиране (публичен ключ и др.).
Ако, към момента на подписването е бил използван псевдоним, то това е ясно указано на доверяващата се страна	Процесът на валидиране предоставя на потребителите / Доверяващата се страна отчет, включващ удостоверение на Титуляра/ Създателя, съдържащ данните за валидиране (публичен ключ и др.). Вижте отчета за валидиране в Ръководството за потребителя на DSS.
Електронният подпис е създаден от устройство за създаване на квалифициран електронен подпис	Процесът на валидиране на удостоверенията е в съответствие с изискванията, описани в Решение 2015/1505 и относими към квалифицираните доставчици, издаващи квалифицирани сертификати. Извършва се проверка за необходимия тип SSCD (QSCD).
Целостта на подписаните данни не е застрашена	Гарантира се чрез поддържания модел за валидиране, посочен в този документ. Вижте "Криптографски ограничения" ETSI TS 119-312
Изискванията по член 26 са били изпълнени към момента на подписването	Процесът на валидиране на подпис / печат проверява състоянието и атрибутите на удостоверението към момента на генериране на подписа
Изисквания съгласно чл. 33 от Регламент (EU) No. 910/2014	**Изпълнение**
Услугата по квалифицирано валидиране на квалифицирани електронни подписи/печати може да се предоставя единствено от доставчик на квалифицирани удостоверителни услуги	ИНФОНОТАРИ е квалифициран доставчик на удостоверителни услуги, съгласно Регламент (EU) No. 910/2014 и Закона за електронния документ и електронните удостоверителни услуги и е вписан в Европейския доверителен списък от Националния надзорен орган.

5. КОНТРОЛ НА ОБОРУДВАНЕТО, ПРОЦЕДУРИТЕ И УПРАВЛЕНИЕТО

В съответствие с т. 5 от документа на ИНФОНОТАРИ „ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ".

6. КОНТРОЛ НА ТЕХНИЧЕСКАТА СИГУРНОСТ

В съответствие с т. 6 от документа на ИНФОНОТАРИ „ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ".

7. ПРОВЕРКА И КОНТРОЛ НА ДЕЙНОСТТА

В съответствие с т. 8 от документа на ИНФОНОТАРИ „ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ".

8. ДРУГИ БИЗНЕС И ПРАВНИ УСЛОВИЯ

В съответствие с т. 9 от документа на ИНФОНОТАРИ „ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ".