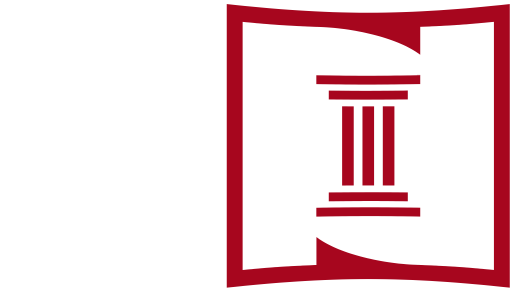


InfoNotary

ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ

НА

КВАЛИФИЦИРАНИЯ ДОСТАВЧИК НА УДОСТОВЕРИТЕЛНИ УСЛУГИ

ИНФОНОТАРИ ЕАД

ВЕРСИЯ 2.3

В сила от 1.07.2021 г.

СЪДЪРЖАНИЕ

1. ВЪВЕДЕНИЕ

Настоящия документ ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ на Доставчика на удостоверителни услуги ИНФОНОТАРИ ЕАД е изготвен в съответствие с 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 (ЕС) 910/2014), Закона за електронния документ и електронните удостоверителни услуги и приложимото законодателство на Република България и се позовава на целите или на част от следните общоприети международни стандарти и спецификации:

- EN 319 401 v2.2.1 General Policy Requirements for Trust Service Providers;
- EN 319 411 Policy and security requirements for Trust Service Providers issuing certificates;
- EN 319 411-1 v1.2.2: General requirements;
- EN 319 411-2 v2.2.2: Requirements for trust service providers issuing EU qualified certificates;
- EN 319 421 v1.1.1: Policy and Security Requirements for Trust Service Providers issuing Electronic Time-Stamps;
- EN 319 412 Certificate Profiles
- 319 412-1 v1.1.1: Overview and common data structures;
- 319 412-2 v2.1.1: Certificate profile for certificates issued to natural persons;
- 319 412-3 v1.1.1: Certificate profile for certificates issued to legal persons;
- 319 412-4 v1.1.1: Certificate profile for web site certificates issued to organizations;
- 319 412-5 v2.2.1: QCStatements;
- EN 319 422 v1.1.1 Time-stamping protocol and electronic time-stamp profiles;
- RFC 3647: Internet X.509 Public Key Infrastructure – Certificate Policies and Certification Practices Framework;
- RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
- RFC 3739: Internet X.509 Public Key Infrastructure – Qualified Certificates Profile;
- RFC 6960: X.509 Internet Public Key Infrastructure - Online Certificate Status Protocol - OCSP;
- RFC 3279: Algorithms and Identifiers for Internet X.509 Public Key Infrastructure Certificate and CRL Profile;

- RFC 3161: Internet X.509 Public Key Infrastructure: Time-Stamp Protocol (TSP);
- TS 119 495 v1.2.1: Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive (EU) 2015/2366.
- РЕШЕНИЕ ЗА ИЗПЪЛНЕНИЕ (ЕС) 2016/650 НА КОМИСИЯТА от 25 април 2016 година за определяне на стандарти за оценка на сигурността на устройствата за създаване на квалифициран електронен подпис и печат съгласно член 30, параграф 3 и член 39, параграф 2 от Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета;
- 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.
- ETSI TS 119 431-1/2 - Electronic Signatures and Infrastructures (ESI);Policy and security requirements for trust service providers;
- Part 1: TSP service components operating a remote QSCD /SCDev;
- Part 2: TSP service components supporting AdES digital signature creation
- ETSI TS 119 432 - Electronic Signatures and Infrastructures (ESI); Protocols for remote digital signature creation;
- БДС EN 419 241-1:2018 Надеждни системи, поддържащи сървърно подписване. Част 1: Общи изисквания за сигурност на система (EN 419241-1:2018. Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements).

Международните стандарти и спецификации се ползват в техните актуални и валидни версии.

Основната цел на документа Практика при предоставяне на квалифицирани удостоверителни услуги, наричан още (Практиката или InfoNotary Qualified CPS), е чрез подробно описание на правилата и

политиките, които ИНФОНОТАРИ ЕАД е въвела и съблюдава за извършване на дейността ѝ по предоставяне на квалифицирани удостоверителни услуги, да ги направи публични за потребителите и да предостави средства за всички заинтересовани страни за установяване на съответствието на дейността на Доставчика с разпоредбите и изискванията на Регламент (ЕС) 910/2014, приложимото законодателство на Република България и на надеждността и сигурността на осъществяваната удостоверителна дейност.

InfoNotary Qualified CPS описва техническите и процедурни практики за всички услуги свързани с предоставянето на удостоверителни услуги по издаване и управление на удостоверения за квалифициран електронен подпис, квалифициран електронен печат и квалифицирани електронни времеви печати, както и свързаната с това политика при предоставяне на квалифицирани удостоверителни услуги.

InfoNotary Qualified CPS е публичен документ, разработен в съответствие и покриващ формалните изисквания за съдържание, структура и форма на общопризнатата международна спецификация на Internet Engineering Task Force (IETF) RFC 3647: "Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework.

InfoNotary Qualified CPS може да бъде променян при необходимост, при промяна на нормативни, технологични и процедурни изисквания, като всяка промяна в него е публично достъпна от всички заинтересовани лица на адрес: http://repository.infonotary.com и https://repository.infonotary.com.

1.1. Основни положения

1.1.1. Доставчик на удостоверителни услуги

ИНФОНОТАРИ ЕАД е Доставчик на квалифицирани удостоверителни услуги съгласно Регламент (ЕС) № 910/2014 и е с предоставен квалифициран статут от Надзорния орган на България при предвидените в Регламент № (ЕС) 910/2014 условия и в съответствие с 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 InfoNotary.

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

Услуги по издаване на квалифицирани удостоверения:

- приемане и проверка на заявления за издаване на квалифицирани удостоверения;
- създаване на квалифицирани удостоверения на базата на установената самоличност, идентичност и валидни данни за Титуляр и Създател на печат;
- подписване на квалифицирани удостоверения;
- издаване на квалифицирани удостоверения.

Услуги по управление на квалифицирани удостоверения:

- отразяване на промените в статуса на валидност на издадено квалифицирано удостоверение;
- услуги по спиране, възобновяване и прекратяване действието на квалифицирано удостоверение;
- водене на регистър на издадените квалифицирани удостоверения;
- публикуване в регистъра на всяко издадено квалифицирано удостоверение;
- публикуване в регистъра на списък на спрените и прекратени квалифицирани удостоверения.

Услуги за достъп до квалифицирани удостоверения:

- предоставяне на достъп на трети лица до регистъра с издадените удостоверения;
- предоставяне на достъп на трети лица до списъците на спрените и прекратени удостоверения;
- предоставяне на услуги за ограничение на достъпа до публикуваните 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**).

Услуги по удостоверяване на времето на подписан документ:

- издаване на квалифициран времеви печат за удостоверяване на дата и час на представяне на електронен подпис, създаден за определен електронен документ;
- предоставяне на услуги по проверка на издаден от Доставчика квалифициран времеви печат за дата и час на електронен документ.

Услуги по генериране на криптографски ключове:

- генериране на двойка публичен и частен ключ от асиметрична криптосистема посредством устройство за създаване на квалифициран електронен подпис/печат (QSCD).

Услуги по сигурно генериране и съхранение на криптографски ключове за облачен квалифициран електронен подпис/печат:

- генериране и сигурно съхранение по възлагане от Титуляр/Създател на двойка публичен и частен ключ от асиметрична криптосистема посредством устройство за създаване на подпис/печат InfoNotary Remote Qualified Signature Creation Device (RQSCD);
- удостоверено управление и ползване на хостнатите криптографските ключове, единствено под контрола на Титуляря за създаване на електронен подпис/Създателя за създаване на електронен печат.

Услуги по отдалечено подписване или подпечатване с облачен квалифициран електронен подпис/печат:

- удостоверено управление и ползване на хостнатите криптографските ключове, единствено под контрола на Титуляря за създаване на електронен подпис или Създателя за създаване на електронен печат.

При осъществяване на дейността си 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.

1.2. ИМЕНУВАНЕ И ИДЕНТИФИКАЦИЯ НА ДОКУМЕНТА

Документа **„Практика при предоставяне на квалифицирани удостоверителни услуги на ИНФОНОТАРИ ЕАД"** (Практиката), се именува **"InfoNotary Qualified CPS"** и се идентифицира посредством следния идентификатор на обект в издаваните удостоверения: OID:1.3.6.1.4.1.22144.3

Идентификаторът на обект (OID) представлява поредица от цели числа, която се присвоява на регистриран обект и е уникален сред всички идентификатори на обекти в конкретната област.

Идентификатора на Инфонотари ЕАД, който се ползва за означаване на организацията и е уникален за нея е регистриран като Private Enterprise Number (PEN) в IANA (http://www.iana.org/assignments/enterprise-numbers) iso.org.dod.internet.private.enterprise (1.3.6.1.4.1)

Стойност на PEN на Инфонотари ЕАД: 22144

Структурата на индентификаторите на обекти, които ИНФОНОТАРИ ЕАД използва е следната:

InfoNotary Plc	InfoNotary CSP	InfoNotary TTP	InfoNotary TSP	Roots	CAs	End Entity
1.3.6.1.4.1.22144	1	2	3	1	1	1

Практиката е свързана с Удостоверителните политики при предоставяне на квалифицирани удостоверения за квалифициран електронен подпис (КУКЕП), квалифициран електронен печат, усъвършенстван електронен подпис, усъвършенстван електронен печат, квалифицирани удостоверения за автентичност на уебсайт, квалифицирани електронни времеви печати и други удостоверителни услуги.

Практиката включва:

- описание на условията, които Доставчикът спазва и следва при издаване на квалифицирани удостоверения, както и приложимостта на тези удостоверения с оглед на нивото на сигурност и ограниченията при използването им;
- съвкупност от конкретни процедури, които се спазват в процеса на издаване и управление на квалифицирани удостоверения, първоначалната идентификация и автентификация на Титулярите на удостоверения, условията и необходимите нива на сигурност при създаване на електронния подпис и печат и съхраняване на частния ключ от Титулярите и Създателите на печати.
- определя приложимостта и степента на доверие във включената в квалифицираните удостоверения информация.

Удостоверителните политики, приложими към различните типове квалифицирани услуги и квалифицирани удостоверения, издавани от Доставчика на крайни потребители, се обозначават със следните идентификатори на обекти в удостоверенията:

Policy name	Identifier (OID)
InfoNotary TSP Root	1.3.6.1.4.1.22144.3
InfoNotary Qualified Natural Person Signature CP	1.3.6.1.4.1.22144.3.1.1
InfoNotary Qualified Delegated Signature CP	1.3.6.1.4.1.22144.3.1.2
InfoNotary Qualified Legal Person Seal CP	1.3.6.1.4.1.22144.3.2.1
InfoNotary Qualified Legal Person Seal for PSD2 CP	1.3.6.1.4.1.22144.3.2.2
InfoNotary Qualified Validated Domain CP	1.3.6.1.4.1.22144.3.3.1
InfoNotary Qualified Organization Validated CP	1.3.6.1.4.1.22144.3.3.2
InfoNotary Qualified PSD2 WA CP	1.3.6.1.4.1.22144.3.3.3
InfoNotary Qualified TimeStamping Service CP	1.3.6.1.4.1.22144.3.4.1
InfoNotary Qualified OCSP CP	1.3.6.1.4.1.22144.3.5.1
InfoNotary Qualified Validation Service CP	1.3.6.1.4.1.22144.3.5.2
InfoNotary Qualified Certificate for Natural Person AESignature CP	1.3.6.1.4.1.22144.3.6.1

InfoNotary Qualified Certificate for Delegated AESignature CP	1.3.6.1.4.1.22144.3.6.2
InfoNotary Qualified Certificate for Legal Person AESeal CP	1.3.6.1.4.1.22144.3.7.1
InfoNotary Qualified Certificate for PSD2 AESeal CP	1.3.6.1.4.1.22144.3.7.2

1.3. Участници в удостоверителната инфраструктура

1.3.1. Удостоверяващ орган

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

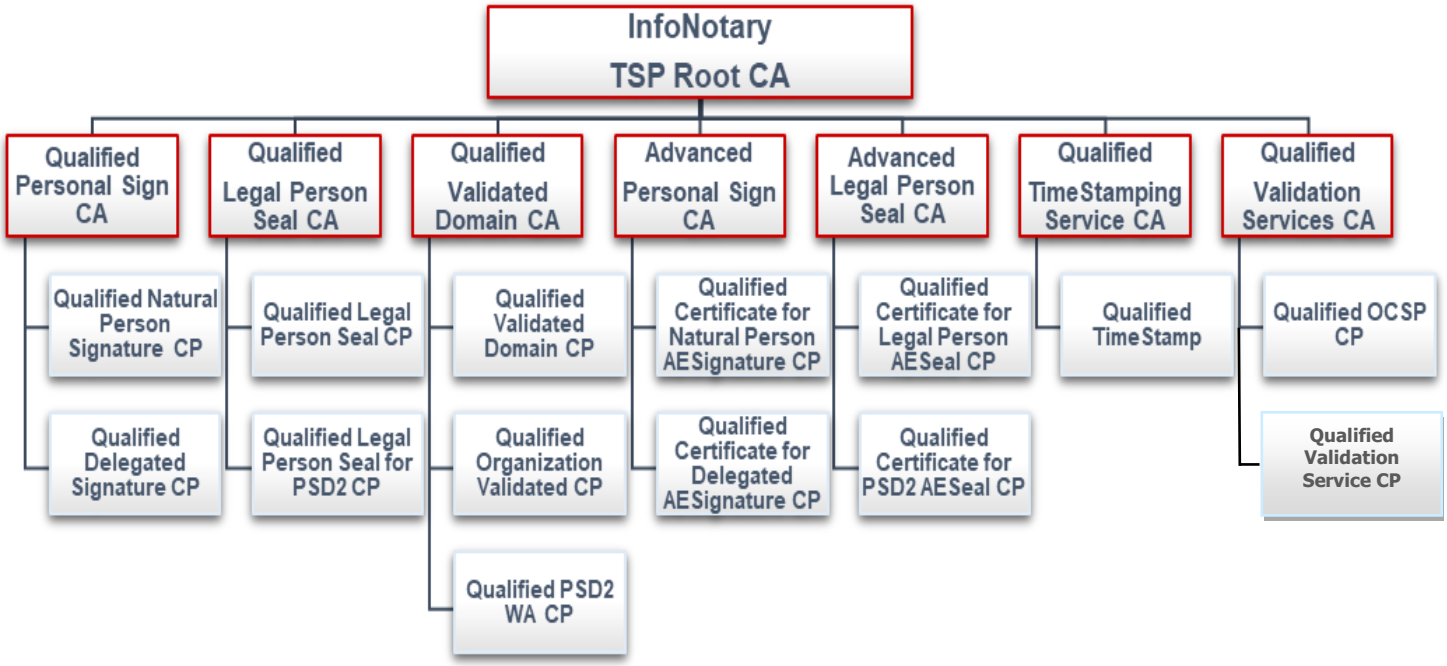
Удостоверяващият орган (root CA) контролира удостоверителните политики на Доставчика, определящи съдържащата се в различните типове удостоверения за крайни потребители индивидуализираща Титуляря/Създателя информация, ограничения в приложението и отговорности.

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

Удостоверяващият орган на Доставчика ползва едностепенна или двустепенна удостоверителна архитектура за диференциация на дейността по издаване и управление на удостоверенията, в зависимост от удостоверителната политика за различните типове удостоверения, както е показано в таблицата:

Name	Type	OID
InfoNotary TSP Root CA	Root CA	1.3.6.1.4.1.22144.3
InfoNotary Qualified Personal Sign CA	Operational CA	1.3.6.1.4.1.22144.3.1
InfoNotary Qualified Legal Person Seal CA	Operational CA	1.3.6.1.4.1.22144.3.2
InfoNotary Qualified Validated Domain CA	Operational CA	1.3.6.1.4.1.22144.3.3
InfoNotary Qualified TimeStamping Service CA	Operational CA	1.3.6.1.4.1.22144.3.4
InfoNotary Qualified Validation Services CA	Operational CA	1.3.6.1.4.1.22144.3.5
InfoNotary Advanced Personal Sign CA	Operational CA	1.3.6.1.4.1.22144.3.6
InfoNotary Advanced Legal Person Seal CA	Operational CA	1.3.6.1.4.1.22144.3.7

При извършване на дейността си Удостоверяващият орган на Доставчика използва следния модел на удостоверителна инфраструктура:



1.3.2. Регистриращ орган

Доставчикът предоставя своите услуги на крайни потребители чрез мрежа от обособени Регистриращи органи.

Регистриращите органи на Доставчика извършват дейности по:

- извършване на проверки с допустими средства и потвърждаване на самоличността на физически лица, идентичността на юридически лица и организации и на физически лица, представляващи юридически лица във връзка с предоставяне на удостоверителни услуги от Доставчика;
- приемане, проверка, одобряване или отхвърляне на искания за издаване на удостоверения;
- регистриране на подадените искания до Удостоверяващия орган за удостоверителни услуги по управление на удостоверенията: спиране, възобновяване, прекратяване и подновяване;
- извършване на проверки с допустими средства на искането, данните за самоличността и идентичността на заявителите (Титуляря и Създателя на печат) и други данни, в зависимост от типа на удостоверенията и в съответствие с удостоверителните политики на Доставчика;
- иницииране на издаване на удостоверението след положителна проверка и одобряване на искането, като уведомяват Удостоверяващия орган;
- генериране на двойка ключове от асиметрична криптосистема върху устройство за създаване на квалифициран електронен подпис/печат (QSCD) по искане на Титуляря/Създателя;
- записване на удостоверението и предаване на устройството (QSCD) и данните за активиране (ПИН и АИН) на Титуляря/Създателя или на упълномощени от тях лица;
- сключване на договори по предоставяне на квалифицирани удостоверителни услуги с клиенти от името и за сметка на Доставчика.

Всички или част от регистрационните дейности могат да се изпълняват от Регистриращ орган на Доставчика:

- във физически офис, при личното присъствие на физическото лице – заявител на удостоверителна услуга в лично качество, в качеството му на упълномощен представител на друго физическо лице, на упълномощен представител на юридическо лице или

организация или в качеството му на законен представител на юридическо лице или организация;

- в онлайн информационна система или мобилно приложение на Доставчика/Регистриращия орган, което е достъпно и се ползва отдалечено от физическото лице – заявител на удостоверителна услуга в лично качество, в качеството му на упълномощен представител на друго физическо лице, на упълномощен представител на юридическо лице или организация или в качеството му на законен представител на юридическо лице или организация. Регистриращият орган може да проверява отдалечено самоличността на Физическото лице чрез средства за сигурна видео идентификация, средства за електронна идентификация, КУКЕП и други законови средства за сигурна отдалечена идентификация.

Доставчикът може да делегира права и да оторизира и трети лица да извършват дейност като Регистриращ орган от името и за сметка на "ИНФОНОТАРИ" ЕАД.

Доставчикът възлага извършването на дейностите като Регистриращ орган на базата на двустранен писмен договор.

Оторизираните Регистриращи органи извършват дейността си в съответствие с InfoNotary Qualified CPS, удостоверителните политики на Доставчика и документирани вътрешни процедури и правила.

Актуален списък на оторизираните Регистриращи органи на Доставчика е публикуван и е публично достъпен на официалната интернет страница на Доставчика на адрес https://www.infonotary.com.

Част от функциите на Регистриращите органи могат да бъдат изпълнявани от Локални регистрационни офиси, които действат под контрола на Регистриращите органи.

1.3.3. Абонат

"Абонат" е физическо или юридическо лице, което има сключен писмен договор с Доставчика за предоставяне на квалифицирани удостоверителни услуги.

Когато е практически възможно, при предоставяне на удостоверителните услуги и продуктите, свързани с ползването на услугите, Доставчикът осигурява тяхната достъпност и ползваемост от хора с увреждания.

1.3.4. Доверяващи се страни

"Доверяващи се страни" са физически или юридически лица, които използват удостоверителните услуги с квалифицирани удостоверения, издадени от Доставчика и се доверяват на тези квалифицирани удостоверения и/или усъвършенствани/квалифицирани електронни подписи/ усъвършенствани/квалифицирани електронни печати, които могат да бъдат проверени чрез публичния ключ, записан в квалифицираното удостоверение на абоната.

Доверяващите се страни следва да имат умения да ползват удостоверения за електронен подпис/печат и за автентичност на уебсайт, като се доверяват на издадени от Доставчика квалифицирани удостоверения само след проверка на статуса на удостоверението в Списъка на спрените и прекратени удостоверения (CRL) или на автоматичната информация, предоставена от Доставчика посредством OCSP протокол.

Доверяващите се страни са длъжни да извършват проверките на валидността, спирането или прекратяването на действието на удостоверения посредством актуална информация за техния статус и да вземат под внимание и да съобразяват действията си с всички ограничения на ползването на удостоверението, включени в самото удостоверение или InfoNotary Qualified CPS и удостоверителните политики.

1.3.5. Титуляр

"Титуляр" е физическо лице, което притежава издадено от Доставчика квалифицирано удостоверение и е вписано в него като такъв.

Само Титуляр има право на достъп до частния ключ за подписване на електронни изявления.

Титуляря държи под свой контрол устройството на създаване на квалифициран електронен подпис (QSCD) използвано от него за генериране и съхранение на двойка публичен и частен ключ от асиметрична криптосистема и данните за достъп до частния ключ, съответстващ на публичния ключ, вписан в квалифицираното удостоверението за квалифициран електронен подпис.

Титуляря може да възложи на Доставчика дейностите по генериране и сигурно съхранение на двойка публичен и частен ключ от асиметрична криптосистема посредством отдалечено устройство за създаване на подпис/печат InfoNotary Remote Qualified Signature Creation Device (RQSCD)-обособена част от инфраструктурата на Доставчика, като данните

за достъп до частния ключ, съответстващ на публичния ключ, вписан в облачно квалифицирано удостоверение за квалифициран електронен подпис са единствено под негов контрол.

1.3.6. Създател на печат

Създател на печат е юридическо лице, което създава електронни печати и е вписано в удостоверението за електронен печат като такъв.

Само създателя на печат има право на достъп до частния ключ за подпечатване на електронни изявления.

Създателя на печат държи под свой контрол устройството на създаване на квалифициран електронен печат (QSCD) използвано от него за генериране и съхранение на двойка публичен и частен ключ от асиметрична криптосистема и данните за достъп до частния ключ, съответстващ на публичния ключ, вписан в квалифицираното удостоверението за квалифициран електронен печат.

Създателя на печат може да възложи на Доставчика дейностите по генериране и сигурно съхранение на двойка публичен и частен ключ от асиметрична криптосистема посредством устройство за създаване на печат InfoNotary Remote Qualified Seal Creation Device (RQSCD)- обособена част от инфраструктурата на Доставчика, като данните за достъп до частния ключ, съответстващ на публичния ключ, вписан в облачно квалифицирано удостоверение за квалифициран електронен печат са единствено под негов контрол.

1.3.7. Представители

„Представител” е надлежно овластено от Абоната, Титуляря/Създателя на печат физическо лице, което извършва действия от негово име по издаване и управление на удостоверения за електронен подпис/електронен печат, удостоверения за автентичност на уебсайт или за ползване на други удостоверителни услуги пред Доставчика.

Представителят е лице, различно от Абоната, Титуляря/Създателя на печат, не е вписано в удостоверението, и не може да извършва електронни изявления, подписани с електронния подпис на Титуляря или подпечатани с електронния печат на Създателя на печат и от името на Титуляря/Създателя.

1.3.8. Платформа за облачни квалифицирани удостоверения и отдалечено подписване и подпечатване на електронни документи

Платформата за облачни квалифицирани удостоверения и отдалечено подписване и подпечатване на електронни документи на ИНФОНОТАРИ е обособена част (хардуер и софтуер) от удостоверителната инфраструктура на Доставчика и осигурява предоставянето на:

Услуги по сигурно генериране и съхранение на криптографски ключове за облачен квалифициран електронен подпис/печат:

- генериране и сигурно съхранение по възлагане от Титуляр/Създател на двойка публичен и частен ключ от асиметрична криптосистема посредством отдалечено устройство за създаване на подпис/печат InfoNotary Remote Qualified Signature Creation Device (RQSCD), което е обособена част от инфраструктурата на Доставчика;
- удостоверено управление и ползване на криптографските ключове в RQSCD, единствено под контрола на Титуляря/Създателя на печат.

Услуги по отдалечено подписване или подпечатване с облачен квалифициран електронен подпис/печат:

- удостоверено управление и ползване на хостнатите криптографските ключове, единствено под контрола на Титуляря за създаване на електронен подпис или Създателя за създаване на електронен печат към представен в Платформата електронен документ.

1.4. Употреба на удостоверенията

1.4.1. Типове удостоверения и употреба

1.4.1.1. Удостоверения на удостоверяващия орган

1.4.1.1.1. Базово удостоверения (Root)

Базовото удостоверение за публичния ключ на Удостоверяващия орган на Доставчика, именуващо се като: **InfoNotary TSP Root** е самоиздадено и самоподписано удостоверение за квалифициран електронен подпис, подписано с базовия частен ключ на Доставчика.

Базовият частен ключ на Доставчика, удостоверен посредством удостоверението за неговия публичен ключ **InfoNotary TSP Root**, се

ползва за подписване на удостоверенията на оперативните удостоверяващи органи на Доставчика и на други данни, свързани с управлението на издадените от Доставчика удостоверения, включително и на Списъка на спрени и прекратени удостоверения, издадени от него (root-ca.crl).

Доставчикът ползва и други базови частни ключове и издава и други самоподписани удостоверения за публичните им ключове, за дейностите, които извършва, и услугите, които предоставя на крайни потребители извън пределите на регламентираните удостоверителни услуги в Регламент (ЕС) № 910/2014.

Базовото удостоверение **InfoNotary TSP Root** съдържа следната основна информация:

InfoNotary TSP Root			
Основни x509 атрибути:			
Атрибут			Стойност
Version			3 (0x02)
Serial number			Уникален за регистъра на Доставчика; 16-байтово число
Valid from			Дата и час на подписване
Valid to			Дата и час на подписване + 20 години
Signature Algorithm			SHA256/RSA
Issuer:			
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 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	InfoNotary 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 4096 bits		
Certificate Policies (Non Critical)	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.22144.3 [1.1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://repository.infonotary.com/cps/qualified-tsp.html		
Subject Key Identifier	SubjectKeyIdentifier		

1.4.1.1.2. Удостоверения на оперативните удостоверяващи органи (InfoNotary Operational CAs)

Оперативните удостоверяващи органи на Доставчика издават и подписват удостоверенията на крайните потребители и подписват данните

за статуса на удостоверенията издадени от тях.

Оперативните удостоверяващи органи на Доставчика издават квалифицираните удостоверения за потребителите в съответствие с Практиката и Политиката за предоставяне на квалифицирани удостоверителни услуги.

1.4.1.1.2.1. Оперативен удостоверяващ орган за издаване на квалифицирани удостоверения за квалифициран електронен подпис на физически лица InfoNotary Qualified Personal Sign CA

Удостоверението за публичния ключ на Оперативния Удостоверяващ Орган за удостоверения за квалифициран електронен подпис на физически лица (**InfoNotary Qualified Personal Sign CA**), **OID: 1.3.6.1.4.1.22144.3.1**, се подписва с частния ключ на базовия удостоверяващ орган **InfoNotary TSP Root, OID: 1.3.6.1.4.1.22144.3**.

С частния ключ на оперативния орган (**InfoNotary Qualified Personal Sign CA**) се подписват квалифицираните удостоверения за квалифициран електронен подпис на физически лица: **InfoNotary Qualified Natural Person Signature** и квалифицираните удостоверения за квалифициран електронен подпис на физически лица с делегирани правомощия: **InfoNotary Qualified Delegated Signature** на крайни потребители, съобразно съответната удостоверителна политика и InfoNotary Qualified CPS.

С частния ключ на оперативния орган (**InfoNotary Qualified Personal Sign CA**) се подписва Списъкът на спрени и прекратени удостоверения на крайни потребители, издадени от него (qualified-natural-ca.crl).

Удостоверението на Оперативния удостоверяващ орган **InfoNotary Qualified Personal Sign CA** съдържа следната основна информация:

InfoNotary Qualified Personal Sign 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 Personal Sign CA
Domain Component	Домейн компонент	DC	qualified-natural-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=1.3.6.1.4.1.22144.3.1 [1.1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://repository.infonotary.com/cps/qualified-tsp.html Unotice: InfoNotary Qualified Personal Sign CA
Subject Key Identifier	subjectKeyIdentifier
Authority Key Identifier	authorityKeyIdentifier=keyid,issuer

1.4.1.1.2.2. Оперативен удостоверяващ орган за издаване на удостоверения за квалифициран електронен печат за юридически лица InfoNotary Qualified Legal Person Seal CA

Удостоверението за публичния ключ на Оперативния Удостоверяващ Орган за квалифицирани удостоверения за квалифициран електронен печат на юридически лица (**InfoNotary Qualified Legal Person Seal CA**), OID: 1.3.6.1.4.1.22144.3.2, се подписва с частния ключ на базовия удостоверяващ орган InfoNotary TSP Root, OID: 1.3.6.1.4.1.22144.3.

С частния ключ на оперативния орган (**InfoNotary Qualified Legal Person Seal CA**) се подписват квалифицираните удостоверения за квалифициран електронен печат на юридически лица: **InfoNotary Qualified Legal Person Seal** на крайни потребители, съобразно съответната удостоверителна политика и InfoNotary Qualified CPS.

С частния ключ на оперативния орган (**InfoNotary Qualified Legal Person Seal CA**) се подписва Списъкът на спрени и прекратени удостоверения на крайни потребители, издадени от него (qualified-**legal**-ca.crl).

Удостоверението на Оперативния удостоверяващ орган **InfoNotary Qualified Legal Person Seal CA** съдържа следната основна информация:

InfoNotary Qualified Legal Person Seal 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 Legal Person Seal CA
Domain Component	Домейн компонент	DC	qualified-legal-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=1.3.6.1.4.1.22144.3.2 [1.1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://repository.infonotary.com/cps/qualified-tsp.html Unotice: InfoNotary Qualified Legal Person Seal CA		
Subject Key Identifier	subjectKeyIdentifier		
Authority Key Identifier	authorityKeyIdentifier=keyid,issuer		

1.4.1.1.2.3. Оперативен удостоверяващ орган за издаване на квалифицирани удостоверения за автентичност на уебсайт InfoNotary Qualified Validated Domain CA

Удостоверението за публичния ключ на Оперативния Удостоверяващ Орган за квалифицирани удостоверения за автентичност на уебсайт (**InfoNotary Qualified Validated Domain CA**), OID: 1.3.6.1.4.1.22144.3.3, се подписва с частния ключ на базовия удостоверяващ орган InfoNotary TSP Root, OID: 1.3.6.1.4.1.22144.3.

С частния ключ на оперативния орган (**InfoNotary Qualified Validated Domain CA**) се подписват съобразно съответната удостоверителна политика и InfoNotary Qualified CPS квалифицирани удостоверения за автентичност на уебсайтове на крайни потребители от следните видове:

- квалифицирано удостоверение за автентичност на уебсайт InfoNotary Qualified Validated Domain Certificate;
- квалифицирано удостоверение за автентичност на уебсайт за организация InfoNotary Qualified Organization Validated Certificate;
- квалифицирано удостоверение за автентичност на уебсайт по PSD2 InfoNotary Qualified PSD2 WA Certificate.

С частния ключ на оперативния орган (**InfoNotary Qualified Validated Domain CA**) се подписва Списъкът на спрени и прекратени удостоверения на крайни потребители, издадени от него (**qualified-domain-ca.crl**).

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

InfoNotary Qualified Validated Domain 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 Validated Domain CA
Domain Component	Домейн компонент	DC	qualified-domain-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=1.3.6.1.4.1.22144.3.3 [1.1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://repository.infonotary.com/cps/qualified-tsp.html Unotice:InfoNotary Qualified Validated Domain CA
Subject Key Identifier	subjectKeyIdentifier
Authority Key Identifier	authorityKeyIdentifier=keyid,issuer

1.4.1.1.2.4. Оперативен удостоверяващ орган за издаване на квалифициран електронен времеви печат (InfoNotary Qualified TimeStamping Service CA

Удостоверението за публичния ключ на Оперативния Удостоверяващ Орган за издаване на квалифицирани електронни времеви печати (**InfoNotary Qualified TimeStamping Service CA**), **OID: 1.3.6.1.4.1.22144.3.4**, се подписва с частния ключ на базовия удостоверяващ орган **InfoNotary TSP Root, OID: 1.3.6.1.4.1.22144.3.**

С частния ключ на оперативния орган (**InfoNotary Qualified TimeStamping Service CA**) се подписват квалифицирани електронните времеви печати за крайни потребители, съобразно съответната удостоверителна политика и InfoNotary Qualified CPS.

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

InfoNotary Qualified TimeStamping Service 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 TimeStamping Service CA
Domain Component	Домейн компонент	DC	qualified-timestamp-ca
Country Name	Държава	C	BG
Locality Name	Град	L	Sofia

Organization Name	Организация	O	InfoNotary PLC
Organizational Unit Name	Организационно звено	OU	InfoNotary 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=1.3.6.1.4.1.22144.3.4 [1.1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://repository.infonotary.com/cps/qualified-tsp.html Unotice: InfoNotary Qualified TimeStamping Service CA		
Subject Key Identifier	subjectKeyIdentifier		
Authority Key Identifier	authorityKeyIdentifier=keyid,issuer		

1.4.1.1.2.5. Оперативен удостоверяващ орган за услуги по валидиране (InfoNotary Qualified Validation Services CA)

Удостоверението за публичния ключ на Оперативния Удостоверяващ Орган за предоставяне на услуги по валидиране на квалифицирани удостоверения, квалифициран електронен подпис и квалифициран електронен печат (**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.

С частния ключ на оперативния орган (**InfoNotary Qualified Validation Services CA**) се подписва квалифицираното удостоверение за усъвършенстван електронен печат, с който се подпечатват отговорите на заявки за валидиране и доклади за валидиране на квалифицирани сертификати, квалифициран електронен подпис и квалифициран електронен печат съобразно съответната удостоверителна политика (OID: 1.3.6.1.4.1.22144.3.5.1; OID: 1.3.6.1.4.1.22144.3.5.2) и настоящата Практика.

Удостоверението на Оперативния удостоверяващ орган **InfoNotary Qualified Validation Services CA** 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

1.4.1.1.2.6. Оперативен удостоверяващ орган за издаване на квалифицирани удостоверения за усъвършенстван електронен подпис на физически лица (InfoNotary Advanced Personal Sign CA)

Удостоверението за публичния ключ на Оперативния Удостоверяващ Орган за квалифицирани удостоверения за усъвършенстван електронен подпис на физически лица (**InfoNotary Advanced Personal Sign CA**), **OID: 1.3.6.1.4.1.22144.3.6**, се подписва с частния ключ на базовия удостоверяващ орган **InfoNotary TSP Root, OID: 1.3.6.1.4.1.22144.3**.

С частния ключ на оперативния орган (**InfoNotary Advanced Personal Sign CA**) се подписват квалифицираните удостоверения за усъвършенстван електронен подпис на физически лица: **InfoNotary Qualified Certificate for Natural Person AESignature** и квалифицираните удостоверения за усъвършенстван електронен подпис на физически лица с делегирани правомощия: **InfoNotary Qualified Certificate for Delegated AESignature** на крайни потребители, съобразно съответната удостоверителна политика и InfoNotary Qualified CPS.

С частния ключ на оперативния орган (**InfoNotary Advanced**

Personal Sign CA) се подписва Списъкът на спрени и прекратени удостоверения на крайни потребители, издадени от него (qualified-natural-aes-ca.crl).

Удостоверението на Оперативния удостоверяващ орган **InfoNotary Advanced Personal Sign CA** съдържа следната основна информация:

InfoNotary Advanced Personal Sign 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 Advanced Personal Sign CA

Domain Component	Домейн компонент	DC	qualified-natural-aes-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=1.3.6.1.4.1.22144.3.6 [1.1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://repository.infonotary.com/cps/qualified-tsp.html Unotice: InfoNotary Advanced Personal Sign CA
Subject Key Identifier	subjectKeyIdentifier
Authority Key Identifier	authorityKeyIdentifier=keyid,issuer

1.4.1.1.2.7. Оперативен удостоверяващ орган за издаване на квалифицирани удостоверения за усъвършенстван електронен печат за юридически лица (InfoNotary Advanced Legal Person Seal CA)

Удостоверението за публичния ключ на Оперативния Удостоверяващ Орган за квалифицирани удостоверения за усъвършенстван електронен печат на юридически лица (**InfoNotary Advanced Legal Person Seal CA**), OID: 1.3.6.1.4.1.22144.3.7, се подписва с частния ключ на базовия удостоверяващ орган InfoNotary TSP Root, OID: 1.3.6.1.4.1.22144.3.

С частния ключ на оперативния орган (**InfoNotary Advanced Legal Person Seal CA**) се подписват квалифицираните удостоверения за усъвършенстван електронен печат на юридически лица: **InfoNotary Qualified Certificate for Legal Person AESeal и InfoNotary Qualified Certificate for PSD2 AESeal** на крайни потребители, съобразно съответната удостоверителна политика и InfoNotary Qualified CPS.

С частния ключ на оперативния орган (**InfoNotary Advanced Legal Person Seal CA**) се подписва Списъкът на спрени и прекратени удостоверения на крайни потребители, издадени от него (qualified-legal-aes-ca.crl).

Удостоверението на Оперативния удостоверяващ орган **InfoNotary Advanced Legal Person Seal CA** съдържа следната основна информация:

InfoNotary Advanced Legal Person Seal 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 Advanced Legal Person Seal CA
Domain Component	Домейн компонент	DC	qualified-legal-aes-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=1.3.6.1.4.1.22144.3.7 [1.1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://repository.infonotary.com/cps/qualified-tsp.html Unotice: InfoNotary Advanced Legal Person Seal CA
Subject Key Identifier	subjectKeyIdentifier
Authority Key Identifier	authorityKeyIdentifier=keyid,issuer

1.4.1.2. Удостоверения за крайни потребители

Квалифицираните удостоверения издавани от Доставчика на крайни потребители, могат да бъдат с различно предназначение, съобразно Политиките за тези удостоверения.

Квалифицираните удостоверения, които Доставчикът издава, съдържат разширенията, дефинирани в X.509 v.3 стандарта, и допълнителни ограничения и разширение съобразно дефинирани такива от Международната организация по стандартизация (ISO).

Квалифицираните удостоверения съдържат разширението "Key Usage", което определя ограничение на приложението на удостоверението. Атрибутът е от категорията „критичен – critical".

Удостоверенията, издавани от Доставчика, съгласно удостоверителната им политика могат да бъдат ползвани със следните предназначения:

- автентификация (authentication) – установяване на авторството;
- конфиденциалност (confidentiality) – използване за криптиране и декриптиране на данни;
- интегритет (integrity) – осигуряване целостта и непроменимостта на подписаните данни;
- неотменимост (non-repudiation) – невъзможност за отхвърляне на подписването.

Квалифицираните удостоверения съдържат разширението „Extended Key Usage", което детайлизира приложението на удостоверението с оглед предназначението му. Атрибутът е от категорията "некритичен – non

critical".

1.4.1.2.1. Типове квалифицирани удостоверения

ИНФОНОТАРИ ЕАД, в качеството си на квалифициран доставчик на удостоверителни услуги издава квалифицирани удостоверения за квалифициран електронен подпис и квалифициран електронен печат, квалифициран електронен времеви печат, квалифицирани удостоверения за автентичност на уебсайт, както и квалифицирани удостоверения за усъвършенстван електронен подпис и усъвършенстван печат и извършва услуги по валидиране на електронни подписи, печати и удостоверения за автентичност на уебсайт в пълно съответствие с разпоредбите и изискванията на Регламент (ЕС) 910/2014.

InfoNotary Qualified Natural Person Signature Certificate Квалифицирано удостоверение за квалифициран електронен подпис на физическо лице

Удостоверението се издава на физическо лице (Титуляр) и може да бъде използвано за електронна персонална идентификация, при извършване на финансови трансакции, защитена и криптирана комуникация, електронна кореспонденция, подписване на електронни документи и извършване на електронни изявления, дейности по автентификация и криптиране на данни. Удостоверението е свързано с двойка криптографски ключове, които са генерирани и се съхраняват само на устройство за сигурно създаване на квалифициран електронен подпис (QSCD). Устройството (QSCD), както и данните за достъп до устройството (ПИН, АИН) и за активиране на частния ключ за създаване на електронен подпис, са достъпни и са под контрола само на Титуляря.

Квалифицираното удостоверението може да бъде издадено от Доставчика и като Облачно удостоверение за квалифициран електронен подпис, като Титуляря възлага обслужването на устройството за създаване на квалифициран електронен подписи на Доставчика, при въведени подходящи механизми и процедури, гарантиращи, че Титулярят разполага с едноличен контрол върху използването на данните, свързани със създаването на електронния му подпис. Двойката криптографски ключове, свързани с удостоверението, са генерирани и се съхраняват само на устройство за сигурно създаване на квалифициран електронен подпис от разстояние (RQSCD), което се управлява от Доставчика от името на Титуляря на електронния подпис. Данните за достъп до устройството RQSCD и за отдалечено активиране на частния ключ за създаване на електронен подпис от разстояние, са достъпни и са под контрола само на Титуляря.

InfoNotary Qualified Delegated Signature Certificate
Квалифицирано удостоверение за квалифициран електронен подпис на физическо лице с делегирани правомощия

Удостоверението се издава на физическо лице (Титуляр) и съдържа информация за Юридическо лице, което е делегирало правомощия на Титуляря и може да бъде използвано за персонална идентификация пред интернет приложения, при извършване на финансови трансакции, защитена и криптирана комуникация, електронна кореспонденция, подписване на електронни документи и извършване на електронни изявления, дейности по автентификация и криптиране на данни.

Удостоверението е свързано с двойка криптографски ключове, които са генерирани и се съхраняват само на устройство за сигурно създаване на квалифициран електронен подпис (QSCD). Устройството (QSCD), както и данните за достъп до устройството (ПИН, АИН) и за активиране на частния ключ за създаване на електронен подпис, са достъпни и са под контрола само на Титуляря.

Квалифицираното удостоверението може да бъде издадено от Доставчика и като Облачно удостоверение за квалифициран електронен подпис, като Титуляря възлага обслужването на устройството за създаване на квалифициран електронен подписи на Доставчика, при въведени подходящи механизми и процедури, гарантиращи, че Титулярят разполага с едноличен контрол върху използването на данните, свързани със създаването на електронния му подпис. Двойка криптографски ключове, свързани с удостоверението, са генерирани и се съхраняват само на устройство за сигурно създаване на квалифициран електронен подпис от разстояние (RQSCD), което се управлява от Доставчика от името на Титуляря на електронния подпис. Данните за достъп до устройството RQSCD и за отдалечено активиране на частния ключ за създаване на електронен подпис от разстояние, са достъпни и са под контрола само на Титуляря.

InfoNotary Qualified Legal Person Seal Certificate
Квалифицирано удостоверение за квалифициран електронен печат на юридическо лице

Удостоверението се издава на Юридическо лице (Създател на електронен печат) и може да бъде използвано за идентификация на Юридическото лице пред интернет приложения, при извършване на финансови трансакции, защитена и криптирана комуникация, електронна кореспонденция, подпечатване на електронни документи и извършване на дейности по гарантиране на интегритета (целостта) и произхода на

подпечатаните електронни данни и информация. Електронния печат може да бъде ползван и за удостоверяване на цифровите активи на юридическото лице, като софтуерен код, схеми и изображения.

Удостоверението е свързано с двойка криптографски ключове, които са генерирани и се съхраняват само на устройство за сигурно създаване на квалифициран електронен печат (QSCD). Устройството (QSCD), както и данните за достъп до устройството (ПИН, АИН) и за активиране на частния ключ за създаване на електронен печат, са достъпни и са под контрола само на Създателя на печат.

Квалифицираното удостоверението може да бъде издадено от Доставчика и като Облачно удостоверение за квалифициран електронен печат, като Създателя възлага обслужването на устройството за създаване на квалифициран електронен печат на Доставчика, при въведени подходящи механизми и процедури, гарантиращи, че Създателя разполага с едноличен контрол върху използването на данните, свързани със създаването на електронния му печат. Двойка криптографски ключове, свързани с удостоверението, са генерирани и се съхраняват само на устройство за сигурно създаване на квалифициран електронен печат от разстояние (RQSCD), което се управлява от Доставчика от името на Създателя на електронния печат. Данните за достъп до устройството RQSCD и за отдалечено активиране на частния ключ за създаване на електронен печат от разстояние, са достъпни и са под контрола само на Създателя.

InfoNotary Qualified Certificate for Legal Person Seal for PSD2
Квалифицирано удостоверение за квалифициран електронен печат на юридическо лице по PSD2

Удостоверението се издава на Юридическо лице (Създател на електронен печат) – Доставчик на платежна услуга по PSD2. Удостоверението да бъде използвано за идентификация на Юридическото лице пред интернет приложения, при извършване на финансови трансакции, защитена и криптирана комуникация, електронна кореспонденция, подпечатване на електронни документи и извършване на дейности по гарантиране на интегритета (целостта) и произхода на подпечатаните електронни данни и информация. Квалифицираното удостоверение съдържа специфични атрибути, осигуряващи необходимата информация за идентификация на Доставчика на платежна услуга по PSD2.

InfoNotary Qualified Validated Domain Certificate
Квалифицирано удостоверение за автентичност на уебсайт

Удостоверението се издава на Физическо или Юридическо лице (Титуляр) и може да бъде използвано за удостоверяване на автентичността на уебсайт, който е вписан в него. Удостоверението се издава в съответствие с изискванията на Регламент (ЕС) 910/2014 и може да бъде ползвано като средство, с което посетител на уебсайт може да бъде уверен, че зад уебсайта стои реален и легитимен субект.

InfoNotary Qualified Organization Validated Certificate
Квалифицираното удостоверение за автентичност на уебсайт за организация

Удостоверението се издава на Юридическо лице/Организация (Титуляр) и може да бъде използвано за удостоверяване на автентичността на уебсайт, информационен ресурс който е вписан в него. Удостоверението се издава в съответствие с изискванията на Регламент (ЕС) 910/2014 и може да бъде ползвано като средство, с което посетител на уебсайт може да бъде уверен, че зад уебсайта стои реален и легитимен субект.

InfoNotary Qualified PSD2 WA Certificate
Квалифицираното удостоверение за автентичност на уебсайт по PSD2

Удостоверението се издава на Юридическо лице/Организация (Титуляр) - Доставчик на платежна услуга по PSD2 Директивата и може да бъде използвано за удостоверяване на автентичността на уебсайт с домейн, който е вписан в него. Удостоверението се издава в съответствие с изискванията на Регламент (ЕС) 910/2014 и PSD2 Директивата и може да бъде ползвано като средство, с което посетител на уебсайт може да бъде уверен, че зад уебсайта стои реален и легитимен субект – Доставчик на платежна услуга. Квалифицираното удостоверение съдържа специфични атрибути, осигуряващи необходимата информация за идентификация на Доставчика на платежна услуга по PSD2.

InfoNotary Qualified TimeStamp Certificate
Квалифициран електронен времеви печат

Електронния времеви печат са данни в електронна форма, които свързват други данни в електронна форма с конкретен момент във времето и представляват доказателство, че последните данни са съществували в съответния момент. Електронния времеви печат издаден от Доставчика удостоверява дата и час на представяне на електронен документ, подписан с частен ключ, съответстващ на публичния ключ, включен в удостоверение за квалифициран електронен подпис, издадено от

Доставчика. Квалифициран електронен времеви печат се издава на физически и на юридически лица, които са Титуляри или са доверяваща се страна.

InfoNotary Qualified Certificate for Natural Person AESignature Квалифицирано удостоверение за усъвършенстван електронен подпис на физическо лице

Удостоверението се издава на физическо лице (Титуляр) и може да бъде използвано за персонална идентификация пред интернет приложения, при извършване на финансови трансакции, защитена и криптирана комуникация, електронна кореспонденция, подписване на електронни документи и извършване на електронни изявления, дейности по автентификация и криптиране на данни.

InfoNotary Qualified Certificate for Delegated AESignature Квалифицираното удостоверение за усъвършенстван електронен подпис на физическо лице с делегирани правомощия

Удостоверението се издава на физическо лице (Титуляр) и съдържа информация за Юридическо лице, което е делегирало правомощия на Титуляря и може да бъде използвано за персонална идентификация пред интернет приложения, при извършване на финансови трансакции, защитена и криптирана комуникация, електронна кореспонденция, подписване на електронни документи и извършване на електронни изявления, дейности по автентификация и криптиране на данни.

InfoNotary Qualified Certificate for Legal Person AESeal Квалифицираното удостоверение за усъвършенстван електронен печат на юридическо лице

Удостоверението се издава на Юридическо лице (Създател на електронен печат) и може да бъде използвано за идентификация на Юридическото лице пред интернет приложения, при извършване на финансови трансакции, защитена и криптирана комуникация, електронна кореспонденция, подпечатване на електронни документи и извършване на дейности по гарантиране на интегритета (целостта) и произхода на подпечатаните електронни данни и информация. Електронния печат може да бъде ползван и за удостоверяване на цифровите активи на Юридическото лице, като софтуерен код, схеми и изображения.

InfoNotary Qualified Certificate for PSD2 AESeal Квалифицираното удостоверение за усъвършенстван електронен печат на юридическо лице по PSD2

Удостоверението се издава на Юридическо лице (Създател на електронен печат) – Доставчик на платежна услуга по PSD2. Удостоверението да бъде използвано за идентификация на Юридическото лице пред интернет приложения, при извършване на финансови трансакции, защитена и криптирана комуникация, електронна кореспонденция, подпечатване на електронни документи и извършване на дейности по гарантиране на интегритета (целостта) и произхода на подпечатаните електронни данни и информация. Квалифицираното удостоверение съдържа специфични атрибути, осигуряващи необходимата информация за идентификация на Доставчика на платежна услуга по PSD2.

1.4.2. 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.

1.4.3. Ограничения на удостоверителното действие

Квалифицираните удостоверения, които се издават от Доставчика, в зависимост от техния тип и удостоверителна политика могат да бъдат с ограничено действие по отношение на предназначението – за електронен подпис, за електронен печат или електронна идентификация и автентификация и/или стойността на сделките и финансовия интерес.

Ограничението по отношение стойността на сделките и финансовия интерес се определя от Титуляря/Създателя и се вписва от Доставчика в удостоверението въз основа на Искането за издаване на удостоверението. Ограниченията се вписват в удостоверението в допълнителното разширение (QC Statement) QcLimitValue: id-etsi-qcs-QcLimitValue, OID: 0.4.0.1862.1.2.

Доставчикът не носи отговорност за вреди, настъпили вследствие на ползването на удостоверенията, издавани от него, извън разрешената им употреба и съобразно ограниченията на приложение по отношение на предназначението, на стойността на сделките и финансовия интерес и такава употреба ще доведе до анулиране на гаранциите, които "ИНФОНОТАРИ" ЕАД дава на Титуляря/Създателя на печат и на

Доверяващите се страни.

1.5. УПРАВЛЕНИЕ НА УДОСТОВЕРИТЕЛНАТА ПОЛИТИКА И ПРАКТИКА НА ДОСТАВЧИКА

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

Всички промени, редакции и допълнения на Практиката при предоставяне на квалифицирани удостоверителни услуги и удостоверителните политики за различните видове квалифицирани удостоверения се приемат от Съвета на директорите на "ИНФОНОТАРИ" ЕАД.

Новите версии на документите се публикуват след тяхното одобрение в Документния регистър на Доставчика и са публично достъпни на адрес: http://repository.infonotary.com и https://repository.infonotary.com

Всички коментари, запитвания за информация и разяснения по Практиката при предоставяне на квалифицирани удостоверителни услуги и удостоверителните политики 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. ТЕРМИНИ И СЪКРАЩЕНИЯ

Валидиране	Процеса на проверка и потвърждаване на валидността на електронен подпис или печат.
Данни за валидиране	Данни, които се използват за валидиране на електронен подпис или електронен печат.
Данни за идентификация на лица	Набор от данни, които позволяват да се установи самоличността на физическо или юридическо лице, или на физическо лице, представляващо юридическо лице.
Данни за създаване на електронен подпис	Уникални данни, които се използват от титуляря на електронния подпис за създаването на електронен подпис.
Данни за създаване на електронен печат	Уникални данни, които се използват от създателя на електронния печат за създаването на електронен печат
Доверяваща се страна	Физическо или юридическо лице, което разчита на електронна идентификация или удостоверителна услуга.
Доставчик на квалифицирани удостоверителни услуги	Доставчик на удостоверителни услуги, който предоставя една или повече квалифицирани удостоверителни услуги и е получил квалифицирания си статут от надзорен орган.
Електронен времеви печат	Данни в електронна форма, които свързват други данни в електронна форма с конкретен момент във времето и представляват доказателство, че последните данни са съществували в

	съответния момент.
Електронен документ	Всяко съдържание, съхранявано в електронна форма, по-специално текстови или звуков, визуален или аудио-визуален запис.
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.
Валидиране	Процес на проверка и потвърждаване на валидността на квалифицирано удостоверение, квалифициран електронен подпис или квалифициран електронен печат
Квалифицирано валидиране	Услугата по валидирене се предоставя от доставчик на квалифицирани удостоверителни услуги, в съответствие с Регламент 910/2014 (чл. 32, 33 и 40)
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 квалифицирано удостоверение за квалифициран електронен подпис; Политика за предоставяне на квалифицирано удостоверение за

	квалифициран електронен печат; Политика за предоставяне на квалифицирано удостоверение за автентичност на уебсайт; Политика за предоставяне на квалифицирано удостоверение за усъвършенстван електронен подпис; Политика за предоставяне на квалифицирано удостоверение за усъвършенстван електронен печат; Политика за предоставяне на квалифицирани услуги за удостоверяване на време 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.
Титуляр на електронен подпис	Физическо лице, което създава електронен подпис.
Удостоверение за автентичност на уебсайт	Удостоверение, което позволява да се удостовери автентичността на уебсайт, като го свързва с физическото или юридическото лице, на което е издадено удостоверението.
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

Удостоверяване на автентичност	Електронен процес, който позволява електронната идентификация на физическо или юридическо лице или потвърждаването на произхода и целостта на данни в електронна форма.
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.
Устройство за създаване на електронен печат (SSCD)	Конфигуриран софтуер или хардуер, който се използва за създаването на електронен печат.
Устройство за създаване на квалифициран електронен печат (QSCD)	Устройство за създаване на електронен печат, което отговаря на изискванията, предвидени в приложение II Регламент (ЕС) № 910/2014.
Отдалечено устройство за създаване на квалифициран електронен печат (RQSCD)	Устройство за създаване на електронен печат, което отговаря на изискванията, предвидени в приложение II Регламент (ЕС) № 910/2014, което е обособена част от инфраструктурата на Доставчика
Устройство за създаване на електронен подпис (SSCD)	Конфигуриран софтуер или хардуер, който се използва за създаването на електронен подпис.

Устройство за създаване на квалифициран електронен подпис (QSCD)	Устройство за създаване на електронен подпис, което отговаря на изискванията, предвидени в приложение II Регламент (ЕС) № 910/2014.
Отдалечено устройство за създаване на квалифициран електронен подпис (RQSCD)	Устройство за създаване на електронен подпис, което отговаря на изискванията, предвидени в приложение II Регламент (ЕС) № 910/2014, което е обособена част от инфраструктурата на Доставчика.
Платформа за облачни квалифицирани удостоверения и отдалечено подписване и подпечатване на електронни документи	Обособена част от удостоверителната инфраструктура на Доставчика, която отговаря на изискванията, предвидени в приложение II Регламент (ЕС) № 910/2014, и чрез която се генерират, съхраняват и управляват данните за създаване на облачен квалифициран електронен подпис/печат от Доставчика, по възлагане от Титуляря на електронния подпис или Създателя на електронния печат.
Усъвършенстван електронен подпис	Електронен подпис, който отговаря на следните изисквания: - свързан е по уникален начин с Създателя на печат на подписа; - може да идентифицира Създателя на печат на подписа; - създаден е чрез данни за създаване на електронен подпис, които Създателя на печат на електронния подпис може да използва с висока степен на доверие и единствено под свой контрол; - и е свързан с данните, които са подписани с него, по начин, позволяващ да бъде открита всяка последваща промяна в тях.
Усъвършенстван електронен печат	Електронен печат, който отговаря на следните изисквания: - свързан е по уникален начин със създателя на печата; - може да идентифицира създателя на печата; - създаден е чрез данни за създаване на електронен печат, които създателят на печата може да използва с висока степен на

	доверие и единствено под свой контрол; и - е свързан с данните, за които се отнася, по начин, позволяващ да бъде открита всяка последваща промяна в тях.
PSD2 Директива	Директива (ЕС) 2015/2366 на Европейския парламент и на Съвета от 25 ноември 2015 год. за платежните услуги във вътрешния пазар, за изменение на директиви 2002/65/ЕО, 2009/110/ЕО и 2013/36/ЕС и Регламент (ЕС) № 1093/2010 и за отмяна на Директива 2007/64/ЕО
Регламент GDPR	Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. 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

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
PSD2	Payment Service Directive 2
PSP	Доставчик на платежна услуга
PSP_AI	Account Information Service Provider
PSP_AS	Account Servicing Payment Service Provider
PSP_IC	Payment Service Provider issuing Card-based payment instruments
PSP_AI	Payment Initiation Service Provider
RA	Registration Authority – Регистриращ орган
RSA	Rivest-Shamir-Adelman – Криптографски алгоритъм за създаване на подпис
RQSCD	Отдалечено устройство за създаване на квалифициран електронен печат
SSCD	Secure Signature Creation Device – Устройство за сигурно създаване на подпис
QSCD	Qualified Seal Creation Device – Устройство за

	създаване на Квалифициран подпис/печат
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

2. ЗАДЪЛЖЕНИЯ ЗА ПУБЛИКУВАНЕ И ПОДДЪРЖАНЕ НА РЕГИСТРИ

Доставчикът публикува информация за квалифицираните удостоверителните услуги и издадените удостоверения, които предоставя в база данни и публично достъпни електронни регистри.

2.1. Регистри

2.1.1. Публичен документен регистър

Цялата публична информация, свързана с дейността на Доставчика, се публикува и поддържа актуална в електронен документен регистър, публично достъпен на адрес: http://repository.infonotary.com и https://repository.infonotary.com

В документния регистър се поддържат публикуваните версии и актуалните редакции на най-малко следните документи на Доставчика:

- Практика при предоставяне на квалифицирани удостоверителни услуги;
- Политики за предоставяне на квалифицирани удостоверения;
- Договор за предоставяне на квалифицирани удостоверителни услуги;
- Тарифа за предоставяне на квалифицирани удостоверителни услуги;
- Други публични документи и информация.

Достъпът за четене и изтегляне на публикуваните в регистъра документи е неограничен и безплатен.

2.1.2. Регистър на удостоверенията

Доставчикът води електронен регистър на удостоверения, в който публикува всички издадени от него удостоверения. Електронния регистър на удостоверенията е база данни, която се актуализира при издаване на удостоверение.

Доставчикът води и публикува в електронния регистър и отделни списъци на спрените и прекратени удостоверения за квалифициран електронен подпис, удостоверения за квалифициран електронен печат и удостоверения за автентичност на уебсайт.

2.2. Публикуване на информация за удостоверенията

Издадените удостоверения се публикуват в регистъра на удостоверенията своевременно след тяхното подписване от съответния удостоверяващия орган на Доставчика.

При спиране или прекратяване на удостоверения, промяната се вписва в базата данни на Доставчика и тези удостоверения се публикуват в Списъка на спрените и прекратени удостоверения от съответния удостоверяващия орган на Доставчика своевременно след тяхното спиране или прекратяване, но не по-късно от 24 часа след получаване на искането за промяна.

Възобновените удостоверения се изваждат своевременно от Списъка на спрените и прекратени удостоверения.

2.3. Честота на публикациите

Актуализирането на базата данни на удостоверенията се извършва автоматично незабавно след публикуване на издадено ново удостоверение и при промяна на статуса на удостоверение.

Актуализирането на списъците на спрените и прекратени удостоверения се извършва автоматично своевременно след включване в списъка на спряно удостоверение, на прекратено удостоверение и при изваждане от списъка на възобновено удостоверение.

Списъците на спрените и прекратени удостоверения се актуализират своевременно и не по-късно от 3 часа след последната публикация.

Периодът на актуалност на публикуван Списък на спрените и прекратени удостоверения е 3 часа.

Всички публикувани списъци на спрените и прекратени удостоверения се съхраняват в Архива на списъците с изтекъл период на актуалност и са достъпни на адрес: http://crl.infonotary.com/crl.

Промените в документите, публикувани в Документния регистър, се публикуват незабавно след тяхното приемане от Съвета на директорите на Инфонотари ЕАД.

2.4. Достъп до регистъра на удостоверенията

2.4.1. Публичен достъп до регистъра

Удостоверенията на Доставчика са публично достъпни посредством HTTP/HTTPS достъп на адрес: www.infonotary.com и посредством LDAP базиран достъп на адрес:

ldap://ldap.infonotary.com/dc=infonotary,dc=com

Всяко заинтересовано лице може да търси в Публичния регистър на удостоверенията по определени критерии и има право да чете и изтегля публикуваните удостоверения на адрес:

http://www.infonotary.com/site/?p=search

Доставчикът не ограничава по никакъв начин и под никаква форма достъпа до регистъра на удостоверенията. Регистърът е постоянно достъпен, освен в случаите на настъпили форсмажорни обстоятелства или събития извън контрола на Доставчика.

По изрично искане на Титуляря/Създателя на печат, Доставчикът ограничава достъпа за четене и изтегляне на удостоверението му, като при търсене в регистъра се предоставя информация за издаденото удостоверение и неговия статус.

2.4.2. Контрол на достъпа при водене на регистъра

Доставчикът осигурява пълен физически, технологичен и процедурен контрол при воденето и пазенето на регистъра, който обезпечава:

- само надлежно овластени служители да въвеждат данни в регистъра;
- извършването на промени на данните в регистъра да не е възможно;
- възможността за непозволена намеса да е сведена до минимум.

3. ИДЕНТИФИКАЦИЯ И АВТЕНТИФИКАЦИЯ

Доставчикът поддържа Регистриращи органи, които проверяват и потвърждават идентичността и самоличността и/или и други данни, включени в удостоверенията за квалифициран електронен подпис, квалифициран електронен печат и за автентичност на уебсайт.

Преди да бъде потвърдено издаването на удостоверение от Удостоверяващия орган на Доставчика, Регистриращият орган потвърждава самоличността на Титуляря.

Регистриращите органи на Доставчика съблюдават специфични процедури по проверка на имената, включително и на запазените данни в някои имена.

Регистриращите органи автентифицират заявките за прекратяване действието на удостоверенията съобразно разпоредбите на т. 3.4 на настоящия документ.

3.1. Именуване

Квалифицираните удостоверения имат формат, съответстващ на стандарта X.509. Регистрационните органи проверяват и гарантират, че имената в искането за издаване на сертификат отговарят на стандарта X.509.

Полето "Subject" в удостоверението съдържа името на Титуляря/Създателя на печат.

Името и другите отличителни данни на Титуляря в съответните полета за всеки тип удостоверение са в съответствие с DN (Distinguished Name), образувано съгласно стандартите X.500 и X.520.

3.1.1. Типове имена

При идентификацията на Титуляря/Създателя на печат в удостоверенията Доставчикът използва различни видове имена за името и индивидуализиращите ги данни, като X.500 уникални имена и RFC – 822 имена.

Имената, присвоени на Титуляря/Създателя на печат, в издадено от Доставчика удостоверение, са уникални и се използват винаги в комбинация с уникален номер на удостоверение.

Имената включени в Distinguished Name (DN) на Титуляря/Създателя на печат имат своето значение на български или друг чужд език. Структурата на DN зависи от вида на удостоверението и Титуляря. DN се състои от следните области (описанията са в съответствие с RFC 3280 и X.520):

- C – международната абревиатура на името на държавата (BG за България),

- CN – пълното име на физическото лице или на юридическото лице,
- GN – личното име на физическото лице,
- SN – фамилия на физическото лице,
- O – име на юридическото лице
- E – електронна поща,
- Serial Number – уникалния идентификатор на физическото лице,
- Други полета, които са детайлно описани в профила на съответното квалифицирано удостоверение, включен в неговата удостоверителна политика.

3.1.2. Псевдоними

Доставчикът не издава квалифицирани удостоверения на базата на ползване на псевдоним като средство за именуване на Титуляря.

3.1.3. Правила за интерпретиране на различните форми на имената

В квалифицираните удостоверения които Доставчикът издава, се включва само съдържащата се в заявката за издаване и потвърдена с документи информация, идентифицираща Титуляря/Създателя на печат.

За идентификация на Титуляр – Физическо лице, на удостоверение се включват следните данни в атрибута за име (CommonName) на (x509 Subject DN):

- личното, бащиното и фамилното име на Титуляря

Информацията за идентификация на Юридическо лице, различно от Титуляря, се вписва в полето за име на Организация (OrganizationName) и включва:

- пълното име на юридическото лице по документи за регистрация

В квалифицираните удостоверения на юридически лица, уникалното име (DN) задължително съдържа информация за юридическото лице Титуляр/Създател на печат.

3.1.4. Уникалност на имената

Доставчикът издава удостоверения с уникален номер в неговия регистър.

Уникалността на издадените удостоверения се осигурява чрез

комбинации от името на Титуляря/Създателя, типа на удостоверението, издателя, уникалният номер в регистъра на Доставчика и периода на валидност. Титуляр/Създател може да има повече от едно издадени валидни удостоверения.

3.1.5. Признаване, автентичност и роля на търговските марки

Доставчикът съблюдава процедури за проверка при издаване на удостоверенията за правата на Титулярите/Създателите на печат върху запазени търговски имена, марки, интернет домейни и др., заявени за включване в удостоверение.

Притежателите на правата на такива имена или марки и др. удостоверяват това свое право с официални документи при процедурата за регистрация пред Регистриращия орган на Доставчика.

При заявка за включване на такива данни в удостоверение, автентифицирана собственост на трети лица, Доставчикът може да откаже издаване на удостоверението.

Доставчикът не носи отговорност, ако включени в удостоверението данни нарушават авторски права или права върху собственост на име, марка и др.

Доставчикът не включва никакви графични запазени знаци, марки или други графични материали, обект на авторско право, в удостоверенията, които издава.

3.2. Първоначална идентификация и потвърждаване на самоличността

За първоначална идентификация и автентификация на Титуляря/Създателя на печат на искано за издаване квалифицирано удостоверение, Доставчикът извършва следните проверки за:

- държането на частния ключ, кореспондиращ на публичния ключ, представен на Доставчика от физическото лице, посочено като Титуляр в удостоверението за електронен подпис или от физическо лице, представител на юридическото лице – Създател на печат;
- проверка и потвърждаване на самоличността и идентичността на Физическото лице – Титуляр, Юридическото лице – Създател на печат и Юридическото лице – делегирало правомощия на физическо лице-Титуляр в удостоверение за квалифициран електронен подпис.

Процедурата за проверка и потвърждаване на самоличността и идентичността на Физическото лице – заявител на удостоверителна услуга в лично качество, в качеството му на упълномощен представител на друго физическо лице, на упълномощен представител на юридическо лице или организация или в качеството му на законен представител на юридическо лице или организация се извършва при личното присъствие на Физическото лице в офис на Регистриращия орган и може да се извърши и отдалечено по електронен път от Регистриращия орган чрез средства за сигурна видео идентификация, средства за електронна идентификация, КУКЕП и други законови средства за сигурна отдалечена идентификация при спазване на изискванията на Регламент (ЕС) № 910/2014.

3.2.1. Метод за потвърждаване на държането на Частния ключ

Държането на Частния ключ, кореспондиращ на публичния ключ, представен на Доставчика за включване в удостоверение, подлежи на проверка посредством различни методи в зависимост от Удостоверителните политики за типа удостоверения.

При заявка за издаване на удостоверение за квалифициран електронен подпис проверката на държането на частния ключ се извършва от Регистриращия орган посредством проверка на електронния подпис, с който е подписана заявката за издаване на удостоверение във формат PKCS#10.

Регистриращият орган извършва и проверка за държането на частния ключ преди иницииране на издаването на удостоверение към Удостоверяващия орган на Доставчика, независимо дали генерирането на двойката ключове, обвързана със заявката, е извършено от Титуляря/Създателя на печат самостоятелно или двойката ключове е генерирана от Доставчика, респективно Регистриращия орган.

При издаване на удостоверение за квалифициран електронен подпис Регистриращият орган извършва проверка и за наличие в устройството за създаване на квалифициран електронен подпис на частния ключ, кореспондиращ на публичния ключ, представен за включване в удостоверението, както и дали ползваното устройство отговаря на изискванията на Регламент (ЕС) №910/2014.

Доставчика предварително одобрява и определя устройствата за създаване на електронен подпис и електронен печат, които приема да бъдат ползвани от потребителите с издадени от него квалифицирани удостоверения за квалифициран електронен подпис/печат, да отговарят на

изискванията на Регламент (ЕС) №910/2014.

При издаване на облачното удостоверение за квалифициран електронен подпис/електронен печат Доставчикът предоставя на Титуляря услуга по генериране и сигурно съхранение по възлагане от Титуляр/Създател на двойка публичен и частен ключ от асиметрична криптосистема посредством устройство за създаване на подпис/печат InfoNotary Remote Qualified Signature Creation Device (RQSCD), което се управлява от Доставчика от името на Титуляря/Създателя. Данните за достъп до RQSCD устройството и за отдалечено активиране на частния ключ за създаване на електронен подпис от разстояние, са достъпни и са под контрола само на Титуляря/Създателя. Преди издаване на удостоверението, Титуляря/Създателя активира частния ключ в RQSCD устройството посредством персоналните си данни за отдалечено активиране (персонален код), с което се извършва проверка за държането на частния ключ.

3.2.2. Установяване на идентичността на Юридическо лице

За установяване и потвърждаване на идентичността на юридическо лице, направило искане за издаване на удостоверение, се прилагат процедури и спазват правила, определени от Доставчика, съобразно типа на исканото удостоверение и условията за неговото издаване.

Доставчикът си запазва правото да променя изискванията към информацията и документите, необходими за потвърждаване на идентификацията на Юридическо лице, при необходимост от изпълнение на свои удостоверителни политики или изисквания на закона.

При издаване на квалифицирано удостоверение на юридическо лице, проверките и потвърждаването на информацията се извършват от Регистриращия орган съобразно правилата за и процедурите на Доставчика и в пълно съответствие с настоящата практика и други вътрешни документи.

Регистриращият орган проверява и потвърждава следната информация, идентифицираща Юридическо лице:

- наименование на юридическото лице;
- адрес, град, държава, пощенски код;
- номер по национален данъчен регистър;
- номер по ЕИК;
- номер по БУЛСТАТ;
- име на домейн;

- правен статут и актуално състояние;
- право върху търговско име, марка, домейн и др.;
- информация за контакт и фактуриране.

Процедурата за проверка и потвърждаване на данните, идентифициращи юридическото лице може да се осъществи и отдалечено, в случай че е налице възможност за автоматизирано извличане на необходимата информация от съответните държавни регистри, поддържани от първични администратори на данни.

За Юридическо лице, Доставчик на платежна услуга по PSD2 се проверява и потвърждава и следната специфична информация:

- роля/роли на Доставчик на платежна услуга;
- PSD2 оторизационен номер, издаден от Национален компетентен орган;
- име на Националния компетентен орган, оторизирал Доставчик на платежна услуга.

Законния представител на юридическото лице, респективно упълномощен представител на Създателя на печат представя лично пред Регистриращия орган следните документи:

- удостоверение за вписване в Търговски регистър, за регистрация или акт за възникване;
- удостоверение за актуално състояние, издадено не по-рано от 1 месец от датата на представяне;
- документ за регистрация по БУЛСТАТ;
- документ за доказване на право за ползване на име и др.
- пълномощно за овластяване на представителя на юридическото лице.

3.2.3. Установяване на идентичността на Физическо лице – Титуляр или Упълномощен Представител

За установяване и потвърждаване на самоличността на физическо лице, направило искане за издаване/ управление на удостоверение, се прилагат процедури и спазват правила, определени от Доставчика, съобразно типа на исканото удостоверение и условията за неговото издаване/управление.

Доставчикът си запазва правото да променя изискванията към информацията и документите, необходими за потвърждаване на самоличността на физическото лице, при необходимост от изпълнение на свои удостоверителни политики или изисквания на закона.

При издаване на квалифицирано удостоверение на физическо лице, проверките и потвърждаването на информацията се извършват от Регистриращия орган съобразно правилата за и процедурите на

Доставчика и в пълно съответствие с настоящата практика и други вътрешни документи.

Регистриращият орган проверява и потвърждава следната информация, идентифицираща Физическото лице:

- лично, бащино и фамилно име;
- дата на раждане;
- място на раждане;
- националност;
- пол;
- адрес, град, държава, пощенски код;
- Единен граждански номер (ЕГН), Личен номер на чужденец (ЛНЧ), Персонален идентификационен номер (ПИН) на чужд гражданин;
- номер на документ за самоличност: лична карта, паспорт;
- издател, дата на издаване и валидност на документа за самоличност;
- представителната власт на Титуляря/Упълномощения представител;
- информация за контакти и фактуриране.

Титуляря или Упълномощеният представител на юридическото лице представят лично пред Регистриращия орган следните документи:

- валиден документ за самоличност: лична карта или паспорт;
- нотариално заверено пълномощно за овластяване на Титуляря/Представителя на юридическо лице или упълномощен представител;
- документ, доказващ представителната власт на законния представител на юридическо лице – съдебно решение, удостоверение за актуално състояние, нотариално заверено пълномощно или друг овластяващ акт.

Процедурата за проверка и потвърждаване на самоличността и идентичността на Физическото лице се извършва при личното присъствие на Физическото лице във офис на Регистриращия орган.
Регистриращият орган може да проверява отдалечено самоличността и идентичността на Физическото лице чрез средства за сигурна видео идентификация, средства за електронна идентификация, КУКЕП и други законови средства за сигурна отдалечена идентификация, като предоставените от лицето данни чрез специален метод за сравнение и потвърждение могат да се валидират допълнително и със същите извлечени от съответните държавни регистри, поддържани от първични администратори на данни.

Процедурата за отдалечена проверка на самоличността и идентификация на физическо лице може да се прилага и при заявление за издаване на квалифицирано удостоверение от законния представител на юридическо лице, респективно негов упълномощен представител.

3.2.4. Непотвърдена информация

В някои случаи Доставчикът може да включи в издаваните удостоверения и непотвърдена информация за Титуляря/Създателя на печат, като електронна поща и др.

Непотвърдена информация е тази, която е извън обхвата на задължителните данни, включени в съдържанието на квалифицираното удостоверение в съответствие с Регламент (ЕС) 910/2014 удостоверението, и не може да бъде потвърдена от Доставчика въз основа на официални документи или по друг допустим от закона начин.

Доставчикът не носи никаква отговорност за такава непотвърдена информация, включена в удостоверението.

3.3. Идентификация и автентификация при заявка за подмяна на ключове в удостоверение

Не се поддържа от Доставчика.

3.4. Идентификация и автентификация при заявка за прекратяване на удостоверение

Прекратяване на действието на удостоверение се извършва от Удостоверяващия орган на Доставчика след иницииране за прекратяване от страна Регистриращия орган на Доставчика, съобразно разпоредбите на т. 4.9.3 на настоящия документ.

Регистриращият орган отправя искане за прекратяване до Доставчика след получаване на искане за прекратяване от Титуляря/Създателя на печат и извършването на действия по проверка на идентичността и самоличността на заявителите и потвърждаването им на място в регистрационен офис или отдалечено по електронен път.

Титулярят/Създателя на печат или упълномощения представител на Титуляря/Създателя на печат, направили искане за прекратяване на удостоверение, представят лично пред Регистриращия орган следните документи:

- валиден документ за самоличност: лична карта или паспорт;

- нотариално заверено пълномощно за овластяване на Представителя да представлява Титуляря/Създателя на печат пред Доставчика за издаване и управление на удостоверения;
- документ, доказващ представителната власт на законния представител на юридическо лице – съдебно решение, удостоверение за актуално състояние, нотариално заверено пълномощно или друг овластяващ акт;
- подписано Искане за прекратяване на удостоверение.

3.5. Идентификация и автентификация при заявка за спиране на удостоверение

Заявка за спиране действието на удостоверение, може да бъде отправена към Доставчика при условията и по реда на т.4.1 на настоящия документ.

Спиране действието на валидно удостоверение се извършва от Удостоверяващия орган на Доставчика за необходимия според обстоятелствата срок, но за не повече от 48 часа.

Доставчикът спира действието на удостоверението, без да извършва действия по идентификация и автентификация на заявителя при следните условия:

- по искане на Титуляря/Създателя на печат;
- по искане на лице, за което според обстоятелствата е видно, че може да знае за нарушения на сигурността на частния ключ или други обстоятелства;
- по разпореждане от страна на Надзорен орган – при непосредствена опасност за интересите на трети лица или при наличие на достатъчно данни за нарушение на закона.

Възобновяване действието на удостоверение се извършва от Удостоверяващия орган на Доставчика по реда на т.4.11 и след иницииране за възобновяване от Регистриращия орган.

Регистриращият орган извършва идентификация и автентификация на Титуляря/Създателя на печат, когато той е представил лично или чрез упълномощен представител подписано искане за възобновяване на удостоверение на място в регистрационен офис или отдалечено по електронен път.

Титуляря/Създателя на печат или негов упълномощен представител, направили искане за възобновяване на удостоверение, представят лично пред Регистриращия орган следните документи:

- валиден документ за самоличност: лична карта или паспорт;
- нотариално заверено пълномощно за упълномощаване на Представителя да представлява Титуляря/Създателя на печат пред Доставчика за издаване и управление на удостоверения;
- подписано Искане за възобновяване на удостоверение, съдържащо декларация, че Титулярят/Създателя на печат е узнал причината за спирането и искането за възобновяване е направено вследствие на узнаването.

4. ОПЕРАТИВНИ УСЛОВИЯ

Титулярите, Създателите на печат, Регистриращите органи и други участници в удостоверителната инфраструктура на Доставчика са длъжни да го уведомяват незабавно при настъпването на каквито и да било промени в информацията, съдържаща се и отнасяща се до издадено удостоверение, през периода на неговото действие и докато то не бъде прекратено.

Удостоверяващият орган на Доставчика издава, спира и прекратява действието на удостоверенията след удостоверено и надлежно подписано искане за това от негов Регистриращ орган.

4.1. Искане за издаване на удостоверение

Регистриращите органи на Доставчика приемат и обслужват всички искания за издаване на удостоверения и са длъжни да предоставят на Удостоверяващия орган вярна и потвърдена информация във връзка с получените заявки за издаване от крайни потребители.

4.1.1. Заявители

Искане за издаване на удостоверение до Доставчика могат да отправят всички лица, които:

- попълнят Искане за издаване на удостоверение;
- генерират двойка криптографски ключове самостоятелно или посредством Доставчика;
- предоставят на Удостоверяващия орган на Доставчика, публичния ключ, кореспондиращ на частния ключ;
- приемат условията на Договора за предоставяне на квалифицирани удостоверителни услуги и Практиката за предоставяне на квалифицирани удостоверителни услуги на Доставчика.

Искането за издаване на удостоверение до Доставчика може да бъде

направено лично от Титуляря/Създателя на печат или от негов упълномощен или законен представител.

4.1.2. Процес на заявяване за издаване на удостоверение

Искането за издаване на удостоверение е необходимо да съдържа следните данни:

- информация, индивидуализираща Титуляря, и овластяващото го юридическо лице, ако ще се съдържа такава информация;
- информация, индивидуализираща Създателя на печат;
- публичния ключ, кореспондиращ на частния ключ от двойката криптографски ключове;
- и типа на избраното удостоверение.

Искането за издаване на удостоверение е електронен документ във формат PKCS #10, подписан с частния ключ, кореспондиращ на публичния, включен в документа.

В зависимост от удостоверителната политика на различните типове удостоверения, издавани от Доставчика, в Искането за издаване на удостоверение може да бъде необходимо включването и на допълнителна информация.

Искането за издаване на удостоверение се подава лично от Заявителя или от упълномощено от него лице в офис на Регистриращ орган на Доставчика или по електронен път и в онлайн информационна система или мобилно приложение на Доставчика/Регистриращия орган, което е достъпно и се ползва отдалечено от физическото лице – заявител на удостоверителна услуга в лично качество или в качеството на упълномощен или законен представител на юридическо лице или организация.

Ползването на онлайн информационна система или мобилно приложение на Доставчика/Регистриращия орган изискват предварителна регистрация и отдалечена идентификация от Заявителя, която може да бъде ползвана за регистрация на данни и избор на услуги, както и за създаване и подаване на искане за издаване на удостоверение в едно с публичния ключ от двойката криптографски ключове, които са генерирани самостоятелно от Заявителя на устройство за създаване на квалифициран електронен подпис/печат (QSCD) или софтуерно.

При подаване на искане за издаване на удостоверение за облачен електронен подпис/печат, двойката криптографски ключове задължително

се генерира от Доставчика на HSM в RQSCD с изискуемото ниво на сигурност (CC EAL 4+ и по-високо) по възлагане от Заявителя. Частният ключ е достъпен отдалечено и се активира от Титуляря/Създателя на печат чрез личен код за достъп (ПИН), парола или ключ под негов контрол. Искането за издаване на облачно удостоверение и генериране на двойката криптографски ключове от Доставчика на HSM в RQSCD, може да бъде подадено пред Доставчика в офис на Регистриращ орган, посредством онлайн информационна система или мобилно приложение на Доставчика/Регистриращия орган.

Регистриращия орган на Доставчика предоставя услуга на всички лица по генериране на двойката криптографски ключове, създаване на искане за издаване на удостоверение с включен в нея публичен ключ, създаване на искане за издаване на облачно удостоверение и генериране на двойката криптографски ключове от Доставчика на HSM в RQSCD и подаване на исканията към Доставчика, при техническа възможност за това.

Когато Регистриращият орган на Доставчика извършва по искане от Заявителя генериране на двойка криптографски ключове, ползва устройство за сигурно създаване на квалифициран електронен подпис/печат (QSCD) и ги предоставя на Титуляря/Създателя на печат или упълномощено от него лице.

Правата за достъп до частния ключ – ПИН код или парола, се предоставят от Регистриращия орган на Титуляря/Създателя на печат или упълномощено от него лице в защитен вид.

След предаването от Регистриращия орган на устройство за сигурно създаване на квалифициран електронен подпис/печат, на което е генериран частният ключ и правата за достъп до него, Титулярят/Създателят на печат носи пълната отговорност за предотвратяване на компрометиране, загуба, разкриване, модифициране или друго неоторизирано използване на частния ключ.

4.2. Процедура по заявяване на Удостоверение

4.2.1. Изпълнение на функциите по извършване на идентификация и автентификация

Функциите по идентификация и автентификация на Заявителите на Искане за издаване на квалифицирано удостоверение се извършват от оторизиран Регистриращ орган на Доставчика.

Съблюдавайки утвърдените от Доставчика процедури и съгласно т.

3.2 на настоящия документ, въз основа на полученото искане за издаване на удостоверение, представените документи и в личното присъствие на Заявителя – Титуляря/Създателя на печат или упълномощено от него лице, Регистриращия орган проверява и потвърждава:

- самоличността и идентичността на Титуляря/Създателя на печат и упълномощения от него представител, ако има такъв;
- представителната власт на Титуляря и упълномощения от Титуляря/Създателя на печат представител.

Когато искането за издаване на облачно удостоверение се подава отдалечено, проверките се извършват (автоматично и от оператор на Регистриращия орган) в рамките на сесията по регистрация и отдалечена идентификация на Заявителя.

4.2.2. Потвърждаване или отхвърляне на заявките за удостоверения

Преди потвърждаване на подадено искане за издаване на удостоверение към Удостоверяващия орган на Доставчика, Регистриращият орган извършва необходимите проверки по изискванията на т. 3.2 на настоящия документ:

- проверява и потвърждава самоличността или идентичността на Заявителя, Титуляря/Създателя на печат или представляващото го лице по предоставените от тях документи;
- проверява и потвърждава представителната власт на Титуляря и упълномощеното от Титуляря да го представлява лице;
- проверява и потвърждава държането на частния ключ, кореспондиращ на публичния ключ включен в искането по времето на неговото създаване;
- проверява и потвърждава допълнителната информация, заявена за включване в удостоверението, с изключение на непотвърдената информация;
- проверява коректността на получената или направената подписана електронна заявка (във формат PKCS#10) за издаване на удостоверение;
- предоставя на Титуляря/Създателя на печат информацията, която е събрана и ще бъде включена в издаденото удостоверение, за приемане на съдържанието ѝ;
- потвърждава съгласието на Титуляря/Създателя на печат с условията на настоящия документ и на Договор за квалифицирани удостоверителни услуги и подписването на Договора;
- събира саморъчно заверени с дата и подпис от Заявителя, копия на документите, въз основа на които е извършена проверката

на самоличността и идентичността на Титуляря/Създателя на печат и овластяването на Титуляря и представителната власт на представителя.

Ако процесът на потвърждаване на заявката за издаване на удостоверение завърши успешно, Регистриращият орган потвърждава електронното искане за издаване на удостоверение към Удостоверяващия орган на Доставчика и утвърждава че:

- искането за издаване изхожда от Титуляря/Създателя на печат или от надлежно овластено от него лице;
- информацията относно Титуляря/Създателя на печат, представена за включване в удостоверението, е вярна и пълна;
- частният ключ е технически годен да бъде използван за създаване на квалифициран електронен подпис/печат и съответства на публичния ключ, така че чрез публичния ключ може да се удостовери, че определен електронен подпис/печат е създаден с частния ключ;
- частният ключ се държи от Титуляря/Създателя на печат;
- Титуляря/Създателя на печат има средства под негов контрол за персонален отдалечен достъп до частния ключ в RQSCD на Доставчика чрез мобилно приложение на Доставчика, персонална регистрация в информационна система на Доставчика или друго регистрирано средство за достъп до ключа.

Ако процесът на потвърждаване на заявката за издаване на удостоверение завърши неуспешно, Регистриращият орган отхвърля искането за издаване на удостоверение.

Регистриращият орган незабавно уведомява Заявителя и посочва причината за отхвърлянето.

Заявители, чиито искания за издаване на удостоверение са били отхвърлени, могат отново да подадат искане за издаване на удостоверение.

Регистриращият орган окомплектова и съхранява предоставените от Титуляря/Създателя на печат и упълномощения представител документи на хартия, както и записва и съхранява информацията, данните и цифрови копия на документи, предоставени му от Заявителя в процеса по отдалечена идентификация.

Доставчикът контролира точността на включената в удостоверенията информация, предоставена от Титуляря/Създателя на печат и потвърдена от Регистриращия орган, към момента на издаване на удостоверението.

За всички случаи и за всички типове удостоверения, издавани от Доставчика, Титуляря/Създателя на печат, има постоянното задължение да съблюдава за верността на предоставяната информация и да информира Доставчика за всякакви промени, настъпили след издаване на удостоверението.

4.2.3. Срок за обработка на заявките за удостоверение

Проверката и потвърждаването на информацията в направените искания за издаване на удостоверения се обработват в разумен срок и до 5 работни дни от датата на приемане на искането за издаване и представяне на необходимите данни и документи от Заявителя. Доставчикът издава удостоверението незабавно след потвърждаване на искането за издаване от Регистриращия орган.

4.3. Издаване на удостоверение

4.3.1. Действия на Удостоверяващия орган при издаване на Удостоверение

Удостоверяващият орган на Доставчика издава удостоверението, на база на получено искане за издаване от Регистриращия орган.

Искането за издаване на удостоверение от Регистриращия орган гарантира потвърждаването на валидността на заявката, направена от Заявителя, валидността на данните, съдържащи се в нея, и е подписано от оператор на Регистриращия орган, извършил проверките.

Удостоверяващият орган на Доставчика проверява идентичността на Регистриращия орган и самоличността на оператора на Регистриращия орган на база на представени пълномощия (специално административно удостоверение на оператор на Регистриращ орган).

4.3.2. Известяване на Титуляря/Създателя на печат от Удостоверяващия орган за издаването на удостоверението и доставянето му

Доставчикът незабавно уведомява Титуляря/Създателя на печат за издаденото му квалифицирано удостоверение, посредством изпращане на електронно писмо до Титуляря/Създателя на печат.

След издаване на удостоверението Доставчикът го доставя до Титуляря/Създателя на печат:

- чрез вписване на връзка за дънлоуд на удостоверението в изпратеното електронно писмо;
- посредством онлайн информационната система на Доставчика/Регистриращия орган до която има персонален достъп регистриран Титуляр/Създател на печат или упълномощеното от него лице;
- посредством Регистриращия орган чрез запис на издаденото удостоверение на QSCD под контрола на Титуляря/Създателя на печат или упълномощеното от него лице.

Облачното квалифицирано удостоверение не се предоставя на Титуляря/Създателя, а се съхранява в RQSCD на Доставчика по възлагане от Титуляря/Създателя.

4.4. Приемане и публикуване на удостоверението

4.4.1. Приемане на удостоверението

Доставчикът издава удостоверението в съответствие със съгласието на Титуляря/Създателя на печат.

Титуляря/Създателя на печат или упълномощено от него лице приема съдържанието на издаденото квалифицираното удостоверение с подписване на Протокол за приемане на удостоверение или потвърждаване на приемането в онлайн информационната система или мобилното приложение на Доставчика/Регистриращия орган. Удостоверението се счита за прието и без подписване на Протокол или потвърждаване на приемането, ако Титуляря/Създателя на печат не възрази пред Доставчика, във връзка с вписани в удостоверението грешни или непълни данни в срок до 3 дни от датата на издаване на удостоверението и публикуването му в Публичния регистър.

4.4.2. Публикуване на удостоверението от Удостоверяващия орган

Доставчикът публикува своевременно издаденото квалифицирано удостоверение в Публичния регистър на издадените удостоверения.

4.5. Тайна на данните при квалифицираните удостоверителни услуги и употреба на удостоверенията

4.5.1. Тайна на данните

Никой освен Титуляря/Създателя няма право на достъп до данните

за създаване на квалифициран електронен подпис, квалифициран електронен печат, квалифициран електронен времеви печат и данните за автентичност на уебсайт.

Титуляря/Създателя носи пълната отговорност за съхраняването и ползването на частния ключ и за предотвратяване на компрометиране, загуба, разкриване, модифициране или друго неоторизирано използване на частен ключ (данните за създаване на електронен подпис, електронен печат, електронен времеви печат и данни за автентичност на уебсайт).

Титулярят/Създателят, носи пълна отговорност за действия или пропуски на упълномощени от него лица, когато им е предоставил достъп за генериране, пазене, съхранение или унищожаване на своя частен ключ.

Титуляря/Създателя на печат ползва удостоверението и двойката ключове само в съответствие с разрешената употреба според удостоверителната политика и типа на удостоверението, в съответствие с разрешената употреба вписана в самото удостоверение и само в периода на неговата валидност.

4.5.2. Ползване на данните за валидиране от Доверяващите се лица и употреба на удостоверение

Доверяващите се лица ползват данните за валидиране, включени в издадено от Доставчика квалифицирано удостоверение за проверка на валидността на квалифицирания електронен подпис, квалифицирани електронен печат или автентичност на уебсайт.

4.6. Подновяване на Удостоверението

4.6.1. Условия за подновяване на удостоверение

Удостоверенията, които Доставчикът издава, са с различен период на валидност в зависимост от техния тип и удостоверителна политика. Периодът на валидност се вписва като реквизит в издаденото удостоверение.

Подновяване на удостоверение – издаване на удостоверение с нов период на валидност, без да се променят данните, включени в удостоверението, и двойката ключове, свързани с него, се поддържа като услуга от Доставчика при условия и изисквания съобразно типа на удостоверението и неговото приложение.

Облачните квалифицирани удостоверения не подлежат на подновяване. Доставчикът издава ново облачно удостоверение по искане

на Заявител, като изпълнява първоначална процедура по идентификация и установяване на самоличността.

Подновяване на удостоверение, издадено от Доставчика, може да бъде извършено само ако удостоверителната политика, по която е издадено позволява това, и ако всички данни в удостоверението са непроменени и съдържанието на новото удостоверение е идентично с действащото удостоверение, с изключение на срока на валидност, като в новото удостоверение се вписва новият срок.

Подновяване на валидно, с непрекратено действие удостоверение може да бъде направено само за още за един период на валидност, но до общо 3 годишен период на валидност.

4.6.2. Кой може да заяви искане за подновяване

Подновяване на удостоверението се заявява от Титуляря/Създателя на печат или упълномощено от него лице, вписан в действащото удостоверение, поне 10 (десет) дни преди изтичане периода на валидност на удостоверението.

4.6.3. Процедура по заявяване на подновяване

Искането за подновяване се подава лично от Титуляря/Създателя на печат или от упълномощено от него лице в офис на Регистриращ орган на Доставчика или по електронен път и в онлайн информационна система или мобилно приложение на Доставчика/Регистриращия орган, което е достъпно и се ползва отдалечено от физическото лице – заявител на удостоверителна услуга в лично качество или в качеството на упълномощен или законен представител на юридическо лице или организация.

Електронното заявление е необходимо да бъде подписано от Титуляря с валидното удостоверение за което се иска подновяване.

Регистриращият орган на Доставчика може да изиска от Заявителя актуални документи, доказващи точността и верността на информацията, включена в съдържанието на удостоверението към момента на получаване на искането за подновяване.

Заявителят декларира, че данните, предоставени при първоначалното издаване, и тези, вписани в удостоверението, са верни, точни и непроменени към настоящия момент.

Преди потвърждаване на подадено искане за подновяване на

удостоверение Регистриращият орган на Доставчика извършва необходимите проверки съобразно т. 3.2 и т. 4.2.

Ако процесът на потвърждаване на заявката за подновяване на удостоверение завърши успешно, Регистриращият орган потвърждава електронното искане за подновяване на удостоверение към Удостоверяващия орган на Доставчика и утвърждава че:

- искането за подновяване изхожда от Титуляря/Създателя или от надлежно овластено от него лице;
- информацията относно Титуляря/Създателя, включена в удостоверението е точна, вярна и актуална;
- частният ключ се държи от Титуляря/Създателя;
- удостоверението, за което се иска подновяване, е валидно.

Ако процесът на потвърждаване на заявката за подновяване на удостоверение завърши неуспешно, Регистриращият орган отхвърля искането за подновяване на удостоверението.

Регистриращият орган незабавно уведомява Заявителя и посочва причината за отхвърлянето.

Заявители, чиито искания за подновяване на удостоверение са били отхвърлени, могат да подадат искане за издаване на ново удостоверение.

Регистриращият орган окомплектова и съхранява предоставените от Титуляря/Създателя на печат и упълномощения представител документи на хартия, както и записва и съхранява информацията, данните и цифрови копия на документи, предоставени му от Заявителя в процеса по отдалечена идентификация.

Проверката и потвърждаването на информацията в направените искания за подновяване на удостоверения се обработват в разумен срок и Доставчикът издава удостоверенията до 5 работни дни от датата на приемане на искането и документите.

Удостоверяващият орган на Доставчика издава удостоверението с нов период на валидност на база на получено електронно искане за подновяване от Регистриращия орган.

Искането за подновяване на удостоверение от Регистриращия орган гарантира потвърждаването на валидността на заявката, направена от Заявителя, валидността на данните, съдържащите се в нея, и е подписано от оператора на Регистриращия орган, извършил проверките.

Удостоверяващият орган на Доставчика проверява идентичността на

Регистриращия орган и самоличността на оператора на Регистриращия орган на база на представени пълномощия (специално административно удостоверение на оператор на Регистриращ орган).

4.6.4. Известяване на Титуляря от Удостоверяващия орган за издаването на новото удостоверение

Доставчикът незабавно уведомява Титуляря/Създателя на печат за издаденото ново удостоверение, посредством изпращане на електронно писмо до Титуляря/Създателя на печат.

След издаване на удостоверението Доставчикът го доставя до Титуляря/Създателя на печат:

- чрез вписване на връзка за дънлоуд на удостоверението в изпратеното електронно писмо;
- посредством онлайн информационната система на Доставчика/Регистриращия орган, до която има персонален достъп регистриран Титуляр/Създател на печат или упълномощеното от него лице;
- посредством Регистриращия орган чрез запис на издаденото удостоверение на QSCD под контрола на Титуляря/Създателя на печат или упълномощеното от него лице.

4.6.5. Приемане на подновеното удостоверение

Доставчикът издава удостоверението в съответствие със съгласието на Титуляря/Създателя на печат.

Титуляря/Създателя на печат или упълномощено от него лице приема съдържанието на подновеното квалифицираното удостоверение с подписване на Протокол за приемане на удостоверение или потвърждаване на приемането в онлайн информационната система или мобилното приложение на Доставчика/Регистриращия орган. Удостоверението се счита за прието и без подписване на Протокол или потвърждаване на приемането, ако Титуляря/Създателя на печат не възрази пред Доставчика, във връзка с вписани в удостоверението грешни или непълни данни в срок до 3 дни от датата на издаване на удостоверението и публикуването му в Публичния регистър.

4.6.6. Издаване и публикуване на подновеното удостоверение от Удостоверяващия орган

Доставчикът публикува незабавно издаденото удостоверение в Публичния регистър на издадените удостоверения.

4.7. Подмяна на ключ в удостоверение

Не се поддържа от Доставчика.

4.8. Модификация на удостоверение

Не се поддържа от Доставчика.

4.9. Прекратяване на удостоверение

При прекратяване на базовия или на оперативните удостоверения на Удостоверяващия орган на Доставчика поради компрометиране на частните им ключове се прекратява действието на всички валидни удостоверения, подписани от Доставчика с тези ключове.

4.9.1. Условия за прекратяване на удостоверение

Действието на издадени валидни удостоверения от Доставчика се прекратява автоматично:

- с изтичането на срока на валидност на удостоверението;
- при прекратяване на юридическото лице на Доставчика на квалифицирани удостоверителни услуги без прехвърляне на дейността на друг квалифициран доставчик на квалифицирани удостоверителни услуги.

Доставчикът на удостоверителни услуги прекратява действието на удостоверението при:

- смърт или поставяне под запрещение на Титуляря;
- прекратяване на юридическото лице, когато удостоверението е издадено с вписване на Титуляр-юридическо лице;
- прекратяване на представителната власт на Титуляря по отношение на юридическо лице, когато удостоверението е издадено с вписване на данни за юридическото лице;
- установяване, че удостоверението е издадено въз основа на неверни данни.

Доставчикът предприема незабавни действия във връзка с прекратяването на действието на удостоверението при установяване на съответните основания за това.

Удостоверяващият орган на Доставчика прекратява действието на издадени от него удостоверения.

Доставчикът незабавно уведомява Титуляря/Създателя на печат за

обстоятелства относно валидността или надеждността на издаденото им удостоверение.

4.9.2. Кой може да заяви искане за прекратяване на удостоверение

Доставчикът на удостоверителни услуги е длъжен да прекрати действието на удостоверението по искане на Титуляря или Създателя, след като се увери в самоличността и представителната власт на Титуляря/Създателя.

4.9.3. Процедура за заявка за прекратяване

За осъществяване на действия по прекратяване на удостоверение от Удостоверяващия орган на Доставчика е необходимо:

- да бъде направено писмено искане за прекратяване на удостоверение от Титуляря/Създателя на печат или упълномощено от него лице до Доставчика;
- да се извърши проверка от Регистриращия орган на Доставчика за самоличността, идентичността и представителната власт на Титуляря/Създателя на печат или упълномощено от него лице.

Искането за прекратяване се подава лично от Титуляря/Създателя на печат или от упълномощено от него лице в офис на Регистриращ орган на Доставчика или по електронен път и в онлайн информационна система или мобилно приложение на Доставчика/Регистриращия орган, което е достъпно и се ползва отдалечено от физическото лице – заявител на удостоверителна услуга в лично качество или в качеството на упълномощен или законен представител на юридическо лице или организация.

Идентификацията и автентификацията на заявителите, подали искане за прекратяване на удостоверение, се извършват от Регистриращ орган на Доставчика по реда на т. 3.4.

Удостоверяващият орган на Доставчика прекратява удостоверението на база на получено искане за прекратяване от Регистриращия орган.

Искането за прекратяване на удостоверение от Регистриращия орган гарантира потвърждаването на валидността на заявката, направена от Заявителя, валидността на данните, съдържащи се в нея, и е подписано от оператора на Регистриращия орган, извършил проверките.

Удостоверяващият орган на Доставчика проверява идентичността на

Регистриращия орган и самоличността на оператора на Регистриращия орган на база на представени пълномощия (специално административно удостоверение на оператор на Регистриращ орган) и прекратява удостоверението.

След прекратяване на удостоверението Доставчикът го включва в Списъка на спрените и прекратени удостоверения и актуализира публично достъпния електронен регистър на удостоверенията.

След прекратяване на удостоверението Доставчикът уведомява Титуляря /Създателя директно посредством Регистриращия орган за извършените действия, както и с електронно писмо, в онлайн информационна система или мобилно приложение на Доставчика/Регистриращия орган, ако искането за прекратяване е отправено посредством тези системи.

Прекратените от Доставчика удостоверения не подлежат на възобновяване.

4.9.4. Период, през който Удостоверяващият орган трябва да обслужи заявката за прекратяване

Проверката и потвърждаването на информацията в направените искания за прекратяване на удостоверения се обработват в разумен срок и Доставчикът прекратява удостоверенията в срок до 24 часа от момента на приемане на документите.

4.9.5. Изисквания за проверка за прекратяване на удостоверение към Доверяващите се страни

Доверяващите се страни следва да се доверяват на издадени от Доставчика квалифицирани удостоверения само след проверка на статуса на удостоверението в Списъка на спрените и прекратени удостоверения или на автоматичната информация, предоставена от Доставчика посредством OCSP протокол.

Ако Доверяваща се страна не извърши надлежна проверка на статуса на удостоверение, Доставчикът не носи отговорност за настъпилите вреди за доверяващата се страна.

4.9.6. Честота на издаване на Списък с прекратени удостоверения

Издаване на нов Списък на спрените и прекратени удостоверения се извършва своевременно след включване на удостоверение в него.

Периодът на валидност на Списъка на спрените и прекратени удостоверения е 3 астрономически часа.

4.9.7. Максимално закъснение за публикуване на Списък на спрените и прекратени удостоверения

Актуализирането на Списъка на спрените и прекратени удостоверения се извършва автоматично не по-късно от 3 часа, след издаване на последния списък.

4.9.8. Възможност за проверка на статуса на удостоверение в реално време (OCSP)

Доставчикът предоставя услуга за проверка на статуса на издадените от него удостоверения в реално време посредством OCSP протокол. Услугата е публично достъпна на адрес: http://ocsp.infonotary.com/qualified.

4.9.9. Изисквания за ползване на OCSP

Доверяващите се страни могат да използват за проверка на статуса на удостоверение информацията, предоставена от автоматичната система, посредством OCSP протокол съобразно разпоредбите на настоящия документ.

4.10. Спиране на удостоверение

4.10.1. Условия за спиране на удостоверение

Удостоверяващият орган на Доставчика спира действието на издадени от него удостоверения при наличие на съответните основания и за необходимия от обстоятелствата срок.

Доставчикът предприема незабавни действия във връзка със спиране на действието на удостоверението при установяване на съответните основания за това.

Доставчикът незабавно уведомява Титуляря/Създателя на печат за обстоятелствата относно валидността или надеждността на издаденото им удостоверение.

За периода на временно спиране на удостоверението се счита за невалидно.

4.10.2. Кой може да заяви искане за спиране

Доставчикът спира действието на удостоверението, без да извършва действия по идентификация и автентификация на Заявителя при следните условия:

- по искане на Титуляря/Създателя на печат или упълномощено от него лице;
- по искане на лице, за което според обстоятелствата е видно, че може да знае за нарушения на сигурността на частния ключ или други обстоятелства;
- по разпореждане от страна на Надзорен орган – при непосредствена опасност за интересите на трети лица или при наличие на достатъчно данни за нарушение на закона.

4.10.3. Процедура за заявка за спиране

За осъществяване на действия по спиране на удостоверение от Удостоверяващия орган на Доставчика е необходимо той да получи:

- искане за спиране на удостоверение от Титуляря/Създателя на печат или упълномощено от него лице до Доставчика;
- искане за спиране от лице, за което според обстоятелствата е видно, че може да знае за нарушения на сигурността на частния ключ, като представител, съдружник, служител, член на семейството и др.;
- писмено разпореждане за спиране на удостоверението издадено от Надзорен орган, ако съществува основателно съмнение, че действието на удостоверението следва да бъде прекратено и
- заповед за спиране от Надзорен орган при непосредствена опасност за интересите на трети лица или при наличието на достатъчно данни за нарушение на закона.

Титуляря/Създателя на печат или упълномощено от него лице отправят искането за спиране чрез:

- онлайн информационна система или мобилно приложение на Доставчика, ако Заявителят е регистриран потребител и има съответните права за достъп;
- по телефон, по факс или електронна поща или
- лично в Регистриращ орган на Доставчика.

Предварителна идентификацията и автентификацията на Заявителите подали искане за спиране на удостоверение, и представителната им власт не се изисква.

Удостоверяващият орган спира действието на удостоверението в

разумен според обстоятелствата срок след получаване на искането и го публикува своевременно в Списъка на спрените и прекратени удостоверения.

4.10.4. Ограничение на периода на спиране на удостоверение

Доставчикът е длъжен да спре действието на издадено от него удостоверение за необходимия според обстоятелствата срок, но за не повече от 48 часа от получаване на искането за спиране.

4.10.5. Възобновяване действието на спряно удостоверение

Доставчикът възобновява действието на спряно удостоверение при:

- изтичане на срока за спиране (48 часа);
- отпадане на основанията за спиране;
- по искане на Титуляря/Създателя на печат или упълномощено от него лице след като Доставчикът, съответно Надзорния орган се увери, че той е узнал причината за спирането, както и че искането за възобновяване е направено вследствие на узнаването.

От момента на възобновяване на действието на удостоверението от Удостоверяващия орган на Доставчика то се счита за валидно.

4.11.Процедура по възобновяване действието на спряно удостоверение

4.11.1. Възобновяване по искане на Титуляря/Създателя на печат

Когато възобновяването се извършва по искане на Титуляря/Създателя на печат или упълномощено от него лице; проверка на искането и идентификация на Титуляря се извършва от Регистриращ орган на Доставчика по реда на т. 3.2.

След получаване на потвърждение за проверено искане за възобновяване на удостоверението от Регистриращия орган и верификацията му Удостоверяващият орган на Доставчика изважда спряното удостоверение от Списъка на спрените и прекратени удостоверения и го актуализира.

4.11.2. Възобновяване по разпореждане на Надзорен орган

Удостоверяващият орган на Доставчика възобновява действието на удостоверението и го изважда от Списъка на спрените и прекратени удостоверения след получаване на:

- писмено разпореждане за възобновяване на удостоверението издадено от Надзорен орган, ако е съществувало основателно съмнение, че действието на удостоверението следва да бъде прекратено и
- заповед от Надзорния орган, ако то е било спряно поради непосредствена опасност за интересите на трети лица или поради наличието на достатъчно данни за нарушение на закона.

4.11.3. Възобновяване след изтичане на срока на спиране на действието

След изтичане на срока на спиране на действието – 48 часа от момента на спиране на действието на удостоверението, Удостоверяващият орган на Доставчика автоматично възобновява действието на удостоверението и го изважда от Списъка на спрените и прекратени удостоверения, освен ако Титуляря/Създателя и/или Надзорния орган не поискат удължаване на срока на спиране.

4.12.Прекратяване на договора за квалифицирани удостоверителни услуги

Договорът за квалифицирани удостоверителни услуги на Доставчика с Абоната се прекратява, ако удостоверенията, издадени по него, са прекратени, с изтекъл период на валидност и на други основания, определени в договора.

4.13.Възстановяване на ключ и Key escrow

Не се поддържа от Доставчика

5. КОНТРОЛ НА ОБОРУДВАНЕТО,ПРОЦЕДУРИТЕ И УПРАВЛЕНИЕТО

5.1. Физически контрол

Доставчикът осигурява физическа защита и контрол на достъпа до всички критични части от неговата инфраструктура, които са разположени в негови собствени, ползвани под наем или по договор помещения.

Инфраструктурата на Удостоверяващия орган на Доставчика е логически и физически отделена и не се ползва от други отдели и организации на Доставчика.

5.1.1. Разположение и конструкция на помещенията

Помещенията, в които са разположени критичните компоненти на системата са специално проектирани, конструирани и оборудвани за съхранение на вещи и информация в условията на строг пропускателен режим на достъп.

5.1.2. Физически достъп

Доставчика осигурява висок контрол на достъпа до всички свои помещения и информационни ресурси, чрез денонощна физическа охрана, системи за електронно-пропускателен контрол на достъпа, системи за видеонаблюдение, сигнално-известителни системи и др.

Процедурите за контрол на достъпа, както и системите за контрол на физическия достъп – наблюдение, достъп и сигнално известяване, подлежат на периодичен и инцидентен одит и контрол.

Достъп до определени помещения и информационни ресурси на Доставчика имат само овластените лица от персонала на Доставчика, които строго спазват и следват разработени вътрешни процедури за персонификация, верификация и документиране на достъпа.

5.1.3. Електрическо захранване и климатични условия

Доставчика осигурява електрическото захранване на цялото оборудване от инфраструктурата на Доставчика да е защитено от прекъсване на захранването с допълнително осигурено захранване от дублирани източници.

Доставчика спазва всички изисквания от страна на производителите на техническото си оборудване по отношение на условията за съхранението и експлоатацията му и осигурява средства за контрол и поддържане на необходимите климатични условия.

Антенните системи, ползвани от Доставчика, са снабдени и защитени със система за защита от свръхнапрежение.

5.1.4. Наводнение

Доставчикът осигурява система за наблюдение и известяване при наводнение на помещенията си.

5.1.5. Противопожарно известяване и защита

Доставчикът осигурява средства за противопожарно известяване и система за защита при пожар в помещенията си.

5.1.6. Средства за съхранение на данни

Доставчикът ползва сигурни средства за физическо съхранение на данни и конфиденциална информация, като сейфове и метални шкафове с различна степен на защита.

5.1.7. Извеждане от употреба на технически компоненти

Доставчикът осигурява мерки за сигурното извеждане от употреба на технически компоненти и носители на данни и конфиденциална информация.

5.1.8. Дублиране на компоненти

Доставчикът дублира всички критични компоненти от инфраструктурата на Удостоверяващия орган, както и средства за наблюдения и автоматично подменя критичните компоненти при необходимост.

5.2. Процедурен контрол

Доставчикът съблюдава в своята дейност политика на управление и на управление на персонала, осигуряваща необходимата гаранция за доверност и стабилност при изпълнение на всички поети от него задължения и компетентност за извършване на дейността на Квалифициран Доставчик на удостоверителни услуги в съответствие с изискванията на Регламент (ЕС) 910/2014 и приложимото законодателство на България.

Описаните в InfoNotary Qualified CPS процедури, свързани с дейността на Удостоверяващия орган на Доставчика, се изпълняват в съответствие с разработени вътрешни правила и документи на Доставчика.

Всички лица от персонала на Доставчика подписват декларация за

липсата на конфликт на интереси, спазване на конфиденциалност на информацията и защита на личните данни.

Доставчикът осигурява двоен контрол за всички критични функции на Удостоверяващия орган.

За определени дейности Доставчикът може да ползва и външни лица.

5.2.1. Длъжности и функции

Доставчикът има на разположение необходимия брой квалифициран персонал, който във всеки момент от осъществяването на неговата дейност да осигурява изпълнението на задълженията му.

5.2.2. Брой на служителите за определена задача

Определените задачи, свързани с функционирането на Удостоверяващия орган на Доставчика се извършват поне от две лица от персонала.

5.2.3. Идентификация и автентификация за всяка длъжност

Доставчикът е разработил длъжностни характеристики за всяка една от длъжностите на персонала си.

5.2.4. Изисквания за разделяне на отговорностите при отделните функции

Длъжностите по т. 5.2.1 се изпълняват от различни лица от персонала на Доставчика.

5.3. Контрол на персонала, квалификация и обучение

Техническият персонал на Доставчика е внимателно подбран и притежава професионални познания в следните области:

- технологии за сигурност, криптография, инфраструктура на публични ключове (PKI);
- технически норми за оценка на сигурността;
- информационни системи;
- администриране на големи бази данни;
- мрежова сигурност;
- одитиране и др.

Доставчикът извършва проверка на бъдещите си служители въз основа на издадени справки от компетентни органи, трети страни или декларации.

Доставчикът осигурява обучение на своя персонал за изпълнение на дейностите и функциите в Удостоверяващия и Регистриращия орган на Доставчика.

Доставчикът осигурява периодично опресняващо обучение, за да създаде непрекъсваемост и актуалност на познанията на персонала и процедурите.

Доставчикът санкционира персонала си за неоторизирани действия, непозволено ползване на служебно положение и непозволено използване на системите на Доставчика.

5.3.1. Изисквания към независими доставчици

Независимите доставчици, ползвани от Доставчика, спазват същите правила и процедури на Доставчика, включително и за защита на конфиденциалната информация и лични данни както персоналът на Доставчика.

5.3.2. Документация, предоставена на служителите

Доставчикът предоставя документация – процедури и правила на персонала на Удостоверяващия орган и на Регистриращия орган, за първоначално обучение, повишаване на квалификацията и други.

5.4. Процедури по изготвяне и поддържане на журнал на данни от проверки

Процедурите по изготвяне и поддържане на журнал на данни от проверки включва документиране на събития и документиране на проверки на системите, имплементирани за целите на поддържане на защитена среда.

Доставчикът записва всички събития, свързани с дейностите на Удостоверяващия орган, включващи, но не ограничени само до:

- издаване на удостоверение;
- подписване на удостоверение;
- прекратяване на удостоверение;
- спиране на удостоверение;
- публикуване на удостоверение;

- публикуване на Списък на спрените и прекратени удостоверения.

Записите съдържат следната информация:

- идентификация на операцията;
- дата и час на операцията;
- идентификация на удостоверението, замесено в операцията;
- идентификация на лицето, извършило операцията;
- препратка към заявката за операцията.

Доставчикът записва всички събития, свързани с експлоатацията на хардуерните и софтуерните платформи, както следва:

- при инсталиране на нов и/или допълнителен софтуер;
- при спиране и стартиране на системите и приложенията в тях;
- при успешни и неуспешни опити за стартиране на и достъп до софтуерните PKI компоненти на системите;
- при системни софтуерни и хардуерни сривове на системите и др.;
- при управление и ползване на хардуерните криптомодули.

Съхраняват се и записи за действията, извършени от Регистриращите органи по регистрация на Абонати, идентификация на Титуляри, Създатели на печати и др.

Съхраняват се записи, създадени от комуникационните устройства на Доставчика.

5.4.1. Честота на създаване на записи

Записите се създават автоматично и се съхраняват на дискретни интервали за различните модули.

Оторизиран персонал на Доставчика на регулярни интервали проверява записите и логовете и установява и рапортува за аномалии.

5.4.2. Период на съхранение на записите

Записите и логовете се съхраняват за период от 10 (десет) години.

5.4.3. Защита на записите

Всички записи и логове, които се генерират от компонентите в удостоверителната инфраструктура, се съхраняват електронно.

Единствено квалифицирани овластени лица от персонала на Доставчика имат право на достъп и работа с тези записи и логове.

5.4.4. Процедура за създаване на резервни копия на записите

Резервни копия на записите и логовете се създават на дискретни интервали от няколко часа до едно денонощие за различните модули.

Резервните копия се записват на физически носители и се съхраняват в помещение с високо ниво на защита на контрола на достъпа.

5.5. Архив

Доставчикът съхранява като вътрешен архив следните документи:

- всички издадени удостоверения за период минимум от 10 (десет) години след изтичане периода на валидност на удостоверение;
- всички записи и логове, свързани с издаването на удостоверение, за период минимум от 10 (десет) години след издаване на удостоверение;
- всички записи и логове, свързани с прекратяването на удостоверение, за период минимум от 10 (десет) години след прекратяването на удостоверение;
- списъците на спрените и прекратени удостоверения за период минимум от 10 (десет) години след прекратяване или изтичане периода на валидност на удостоверение;
- всички документи, свързани с издаването и управлението на удостоверенията (искания, документи за идентификация и автентификация, договори и др.), за период минимум от 10 (десет) години след изтичане периода на валидност на удостоверение.

Доставчикът съхранява архива във формат, възможен за възстановяване.

Доставчикът осигурява целостта на физическите носители и осъществява механизъм за копирането им като превенция на загубата на данни.

Архивът е достъпен само от оторизиран персонал на Доставчика и Регистриращите органи, ако е необходимо.

5.5.1. Видове архиви

Доставчикът съхранява архив на удостоверенията, данните от проверки, информацията, свързана с искането за издаване и управление на удостоверения, логове, записи и документация, подпомагаща

удостоверителните услуги като хартиен и електронен архив.

5.5.2. Период на съхранение

Доставчикът съхранява архива за срок от 10 (десет) години. След изтичане на този период, архивираните данни могат да бъдат унищожени.

5.5.3. Защита на архива

Обезпечаването на сигурността на архива включва:

- само персоналът, оторизиран да води архива, да има достъп до него;
- защита от модификация на архива, като записването на данните върху средства за еднократен запис;
- защита от изтриване на архива;
- защита за сигурно унищожаване на носителите, на които архивът е бил записан, след изпълнение на действие по периодично прехвърляне на данните на нов носител.

5.5.4. Процедури по възстановяване на архива

При необходимост Доставчика възстановява данни от поддържания архив.

5.5.5. Изисквания за удостоверяване на дата и час на записи

Времето на създаването на отделни записи и документи от системите на Доставчика се удостоверява посредством заверка на датата и часа на създаването и подписването им посредством TimeStamp сървъра на Доставчика.

5.5.6. Съхраняване на архива

Архивната информация се съхранява в помещение с висока степен на физическа защита и при условия, позволяващи безопасното и дългосрочно съхранение на хартиени, магнитни, оптични и други носители.

5.5.7. Процедури за придобиване и проверка на информация от архив

Архивната информация, която е публична, се публикува и е достъпна в Публичните електронни регистри на Доставчика в четим вид.

5.6. Промяна на ключ на удостоверение

Не се поддържа от Доставчика.

5.7. Компрометиране на ключове и възстановяване след бедствия и непредвидени случаи

За да поддържа непрекъсваемостта и целостта на услугите си, Доставчикът внедрява, документира и периодично тества подходящи планове и процедури за непредвидени случаи и възстановяване след бедствия.

Доставчикът полага необходимите усилия да гарантира пълно и автоматично възобновяване на услугите си в случай на бедствие, сривове в компютърните ресурси, в софтуера или в информацията.

Приоритетно Доставчикът осигурява възстановяването на поддържането и публичния достъп до регистъра на удостоверенията и списъка на спрените и прекратени удостоверения.

В случай на компрометиране на частния ключ на Удостоверяващия орган на Доставчика се предприемат следните действия:

- удостоверението за електронния подпис на Доставчика се прекратява незабавно;
- уведомява се Надзорния орган за прекратяването на Удостоверението на Доставчика;
- уведомяват се потребителите на удостоверителните услуги на Доставчика, чрез публикуване на информация на публичния сайт и по електронна поща;
- Удостоверяващият орган на Доставчика се спира;
- инициира се процедура по генериране на нова двойка криптографски ключове;
- издава се ново удостоверение за електронния подпис на Доставчика;
- всички издадени и валидни удостоверения преди компрометиране на ключа се преиздават.

В случай на компрометиране на частния ключ на Титуляря, същият е задължен незабавно да уведоми Доставчикът за иницииране на процедура по прекратяване на действащо удостоверение.

5.7.1. Действие при бедствия и аварии

Архивните данни, съдържащи информация за искания за издаване, управление и прекратяване на удостоверения, както и записите на всички

издадени удостоверения в базата данни, се съхраняват на безопасно и надеждно място и се достъпни от оторизирани служители на Доставчика в случай на бедствие или авария.

За аварийни действия Доставчика има разработен "План за действие при непредвидени ситуации", който се проверява веднъж годишно.

Доставчика трябва да може да открие всеки възможен инцидент. След като се анализира какво се е случило, целта е да се предотвратят бъдещи инциденти въз основа на системни грешки или проблеми на услугите и технологиите. Доставчика следи всички системи и услуги без прекъсване (24 часа в денонощието) и разполага с телефон за информация и помощ, където потребителите могат да уведомяват за инциденти или проблеми при ползване на услугите.

Планът идентифицира приблизителното време за откриване на всякакви инциденти. Доставчикът гарантира, че всеки потенциален инцидент може да бъде открит. Доставчикът може да прави разлика между реални инциденти и фалшиви аларми. Сериозни инциденти се съобщават на ръководството. Планът идентифицира приблизителното време за известяване и потвърждение. Той определя ролите и отговорностите. Оценява вида на инцидента, подходящото време за реакция и по-нататъшните действия. Събитията се записват. Причините за аварията и начина, по който е засегната ефективността на работата, са документирани. Представените мерки (време за реакция и време за възстановяване на услугата или системата и др.) се записват. Всички данни се анализират и действията на Доставчика подлежат на промяна и подобрения при необходимост. В план са оказани тип архивиране и обезпечаване, което се ползва, на какви интервали се извършва архивирането, къде да се съхранява информацията и структурата и т.н.

5.7.2. Инциденти, свързани с повреди в хардуера, софтуера и / или данните

Цялата информация в случай на повреда или кражба на хардуер, софтуер и / или данни се предава на администратора по сигурността, който действа в съответствие с вътрешните процедури.

Тези процедури са свързани с анализ на ситуацията, разследване на инцидента, мерки за свеждане до минимум на последиците и предотвратяване на подобни инциденти в бъдеще.

В случай на повреда в хардуера, софтуера или данните, Доставчикът уведомява потребителите, възстановява компонентите на

инфраструктурата и възобновява приоритетно достъпа до публичния регистър и списъка с прекратени и спрени удостоверения (CRL).

За такива случаи доставчикът е разработил "План за управление на инциденти". Доставчикът има план за управление на всички инциденти, които засягат нормалното функциониране на удостоверителната си инфраструктура. Този план е в съответствие с Плана за непрекъснатост на бизнеса и Плана за възстановяване след бедствия и аварии.

5.8. Процедури по прекратяване дейността на Доставчика

5.8.1. Прекратяване на дейността

Дейността на Доставчика се прекратява по реда на действащото национално законодателство.

При прекратяването на дейността си Доставчикът уведомява Надзорния орган за намерението си не по-късно от 4 месеца преди датата на прекратяване и дали ще осъществи прехвърляне на дейността си към друг доставчик.

Доставчикът уведомява Надзорния орган в случай на иск за обявяване на дружеството в несъстоятелност, за обявяване на дружеството за недействително или за друго искане за прекратяване или за започване на процедура по ликвидация.

Доставчикът полага всички усилия и грижи, за да продължи действието на издадените от него удостоверения чрез прехвърлянето им към действащ квалифициран доставчик на квалифицирани удостоверителни услуги.

Доставчикът уведомява писмено Надзорния орган и потребителите дали дейността на Доставчика се поема от друг квалифициран доставчик най-късно към момента на прекратяване на дейността си.

Уведомление се публикува и в интернет портала на Доставчика и съдържа и информация за името и данните за контакт на Доставчика приемник.

Доставчикът уведомява потребителите си относно условията по поддръжка на прехвърлените техни удостоверения към Доставчика приемник.

Доставчикът надлежно предава цялата документация, свързана с

дейността му, на приемащия доставчик ведно с всички архиви, както и всички издадени удостоверения (валидни, прекратени и спрени).

В случай, че Доставчикът не успее да прехвърли дейността си на друг квалифициран доставчик, той прекратява действието на удостоверенията на удостоверяващите си органи, на всички издадени от него удостоверения и съхранява цялата документация, свързана с дейността му, ведно с всички архиви и всички издадени удостоверения (валидни, прекратени и спрени), за срок от 10 години.

Ако Регистриращ орган, лице което не е част от организацията на Доставчика, реши да прекрати представителството на Доставчика във връзка с предоставяните удостоверителни услуги, той е длъжен:

- да информира Доставчика за намерението си да прекрати дейността. Уведомлението се извършва в рамките на три месеца преди договорената дата на прекратяване;
- прехвърля на Доставчика цялата документация, свързана с обслужването на клиентите, включително архив и одиторски данни.

5.8.2. Прехвърляне на дейността на друг квалифициран доставчик на квалифицирани удостоверителни услуги

За да се осигури непрекъснатост при предоставянето на квалифицирани удостоверителни услуги на потребителите, Доставчикът може да прехвърли дейностите на друг квалифициран доставчик на удостоверителни услуги. В такъв случай Доставчикът е длъжен:

- да уведоми Надзорния орган за намерението си, но не по-късно от 4 месеца преди датата на прекратяване и прехвърляне на дейностите;
- да полага всички усилия и грижи за поддръжка на издадените удостоверения;
- да уведоми писмено Надзорния орган и ползвателите, че дейността му е поета от друг квалифициран доставчик.
- да информира Потребителите за условията за поддръжка на удостоверенията, прехвърлени на доставчика приемник;
- да променя статута на оперативните удостоверения на удостоверяващия орган и надлежно да предава на доставчика приемник цялата документация, свързана с дейностите, заедно с всички архиви и всички издадени удостоверения (валидни, спрени и прекратени);

- да извърши необходимите действия за прехвърляне на задълженията за поддръжка на информацията към доставчика приемник;
- да прехвърли управлението на вече издадените удостоверения за крайни потребители на доставчика приемник;
- при възможности да прехвърли управлението на RQSCD за издадените облачни удостоверения за крайни потребители на доставчика приемник;
- приемащият доставчик поема правата и задълженията на Доставчика със спрените дейности и продължава да управлява активните удостоверения и RQSCD за издадените облачни удостоверения до изтичане на валидността им.

5.8.3. Отнемане на квалифицирания статут на Доставчика

Ако бъде отнет квалифицирания статут на Доставчика, или квалифицирания статут на някоя от удостоверителните услуги, Инфонотари ЕАД ще уведоми по електронен път или в писмена форма притежателите на валидни квалифицирани удостоверения и/или Абонати на други квалифицирани услуги, третите страни, доверяващи се на удостоверителни услуги и субекти, които имат сключени договори, пряко свързани с предоставянето на квалифицираните удостоверителни услуги.

Информация за това ще бъде публикувана на уеб страницата на Доставчика на адрес: http: www.infonotary.com, ще бъде поставена на видно място и във всички регистрационни офиси или ще бъде публикувана по друг начин, посочен в приложимото национално законодателство.

Информация ще включва и изявление, в което се посочва, дали квалифицираните удостоверения, издадени от Доставчика, могат да се продължат да се използват в съответствие с разпоредбите на приложимото законодателство.

При отнемане на квалифицирания статут на Доставчика или на квалифицирания статут на някоя от предлаганите от Доставчика удостоверителни услуги, Инфонотари ЕАД в съответствие с разпоредбите на националното законодателство, ще предприеме необходимите действия по:

- спиране на издаването на нови квалифицирани удостоверения;
- прекратяване издаването на квалифицирани заверки за време;

- прекратяване предоставянето на други квалифицирани удостоверителни услуги;
- ако се изисква от разпоредбите на националното законодателство да прекрати действието на всички издадени квалифицирани удостоверения;
- осигуряване в съответствие с разпоредбите на националното законодателство, на прехвърлянето на поддръжката на цялата имаща отношение информация, във връзка с данните, издадени и получени в качеството на квалифициран доставчик на квалифицирани удостоверителни услуги и по-специално с оглед предоставяне на доказателство при съдебни производства и осигуряване на приемственост при предоставянето на услугата, на друго надеждно лице за достатъчно дълъг период.
- предприемане на действия по разумно компенсиране на Абонатите, пропорционални на оставащия период на валидност на прекратените поради загуба на квалифициран статут, удостоверения.

6. КОНТРОЛ НА ТЕХНИЧЕСКАТА СИГУРНОСТ

6.1. Генериране и инсталация на двойка ключове

Доставчикът защитава собствените си частни ключове съгласно разпоредбите на настоящата практика.

Доставчикът използва междинните и оперативните частни ключове за подписване на Удостоверяващия орган само за подписване на удостоверения и Списъци на спрени и прекратени удостоверения съгласно позволената употреба на тези ключове в настоящия документ.

Доставчикът ще се въздържа от употребата на частните си ключове, ползвани от Удостоверяващия орган, от употреба извън пределите на дейност на Удостоверяващия орган.

Потребителите на удостоверителните услуги на Доставчика генерират двойката си криптографски ключове - частен и публичен, за квалифицирани удостоверения за електронен подпис, електронен печат и автентичност на уебсайт:

- самостоятелно, при Потребителя - с хардуер и софтуер под техен контрол,
- при Доставчика, съответно при оторизиран от него Регистриращ орган - с хардуер и софтуер, които са под контрола на Оператора на Регистриращия орган;

- от Доставчика, при генериране на криптографски ключове за издаване на облачен КЕП се генерират в HSM в RQSCD с изискуемото ниво на сигурност (CC EAL 4+ и по-високо).

Когато генерирането на двойката ключове се осъществява от Доставчика или самостоятелно от Потребителя трябва да се използва устройство (смарт карти, HSM и други криптографски устройства) за създаване на квалифициран електронен подпис/електронен печат Qualified Signature Creation Device" – QSCD със защитен профил, определен в съответствие с общите изисквания ("Common Criteria"), ниво на сигурност EAL 4+ или по-високо, съгласно стандарта ISO 15408 или друга спецификация, определяща еквивалентни нива на сигурността и съответствие с разпоредбите на Регламент (ЕС) 910/2014.

Доставчикът може на базата на договорни отношения да предостави на Титулярите/Създателите одобрени по реда на Регламент (ЕС) 910/2014 и националното законодателство устройства за създаване на електронен подпис/електронен печат - технически средства (софтуер, смарт карти и други криптографски устройства), които отговарят на изискванията за ниво на сигурност и разпоредбите на Регламент (ЕС) 910/2014 за квалифицирани електронни подписи и печати и съответно, могат да бъдат ползвани като Qualified Signature Creation Device" – QSCD при създаване на квалифицирани подписи/печати.

Титулярят, съответно Създателят могат да използват и други устройства за създаване на квалифициран електронен подпис/електронен печат, отговарящи на изискванията на Регламент (ЕС) 910/2014, освен предоставяните от Доставчика, ако те са одобрени за употреба по реда на Регламент (ЕС) 910/2014, националното законодателство и предварително са приети за ползване с квалифицираните удостоверителни услуги на Доставчика.

При самостоятелно генериране и инсталация от Титуляря, съответно Създателя на криптографски ключове за квалифицирани удостоверения, издавани от Доставчика, е задължително ползването на лицензиран софтуер на производителя.

6.1.1. Генериране на двойка ключове

6.1.1.1. Генериране на частен ключ на Удостоверяващия орган на Доставчика

За генериране и инсталация на частните ключове на Удостоверяващия орган Доставчикът използва система с най-висока степен на надеждност и сигурност, следвайки документирана вътрешна

процедура.

За генериране и ползване на частните ключове на Удостоверяващия орган се използват хардуерни защитни модули, сертифициран на ниво на сигурност FIPS 140-2 Level 3, CC EAL 4+ или по-високо.

Осъществяването на документираната процедура по генериране, инсталиране и съхраняване на базовата (root) двойка ключове на Базовия Удостоверяващия орган на Доставчика и оперативните двойки ключове на Оперативните органи се извършва от оторизирани за това служители на Доставчика и в присъствието на член на Съвета на директорите на "ИНФОНОТАРИ" ЕАД.

Секретните части на базовия частен ключ, както и на всички оперативни частни ключове на Удостоверяващия орган се разпределят, съхраняват и се представят при необходимост за ползване от оторизирани от Доставчика за това лица.

Допълнителната защита от компрометирането и непозволеното ползване на частните ключове на Удостоверяващия орган на Доставчика е гарантирано от осъществявана от Доставчика допълнителна политика на контрол на достъп:

- до управлението на хардуерния модул посредством секретни данни, достъпни само за оторизирани лица, поделени между поне две от тези оторизирани лица;
- контрол на достъпа за управление и ползване на частните на базовия и оперативни ключове на Удостоверяващия орган посредством отделни секретни данни, достъпни само за оторизирани лица, поделени между поне две от тези оторизирани лица.

6.1.1.2. Генериране на двойка ключове на Абонат

Доставчикът предлага услуга по генериране на двойка ключове на Абонат, като при генерирането се използва устройство за създаване на електронен подпис/печат ("Qualified Signature Creation Device" – QSCD) със защитен профил, определен в съответствие с общите изисквания ("Common Criteria"), ниво на сигурност EAL 4+ или по-високо в съответствие със защитен профил за квалифициран електронен подпис/печат съгласно Регламент (ЕС) № 910/2014 върху технически средства за сигурно генериране и съхранение на двойка ключове - криптографски смарт карти и други криптографски устройства.

Частният ключ на Титуляр, съответно Създателя, се генерира/ върху техническо средство – смарт карта, токън или др., и автоматично и

необратимо се изтрива от средствата на Доставчика, ако такива са ползвани при генерирането му.

Двойката ключове на облачен квалифициран електронен подпис/печат се генерират от Доставчика, на HSM в RQSCD с изискуемото ниво на сигурност (CC EAL 4+ и по-високо) и защитен профил на SAD/SAP/SAM в RQSCD съгласно ETSI EN 419 241-2/3. Те се съхраняват от Доставчика в съответствие с утвърдени вътрешни правила и процедури за сигурност.

Частният ключ е достъпен отдалечено и се активира от Титуляря в чрез личен код за достъп (ПИН), парола или ключ под контрола на Титуляря.

6.1.2. Доставка на Частния ключ

Когато Доставчикът по възлагане от Титуляря, съответно Създателя генерира двойката ключове, частният ключ от тази двойка се:

- генерира/записва на устройство за създаване на електронен подпис/печат (QSCD-смарт карта или друго техническо средство), отговарящо на изискванията на Регламент (ЕС) № 910/2014 и достъпът до него се защитава с ПИН или парола. Техническото средство се предава на Титуляря/Създателя или упълномощено от него лице, заедно с правата за достъп (ПИН, АИН);
- генерира и съхранява в криптиран вид в HSM модул в RQSCD на Доставчика и достъпът до него се осъществява чрез личен код за достъп (ПИН), парола или ключ под контрола на Титуляря/Създателя на печат.

6.1.3. Доставка на Публичния ключ до издателя на Удостоверението

Тази процедура се изпълнява само от Титуляря, съответно Създателя, който генерира двойката ключове и който следва да достави публичния ключ на Доставчика за нуждите на процеса на издаване на удостоверение.

Електронната заявка за издаване на удостоверение, чрез която се доставя публичният ключ до Доставчика, следва да е в PKCS#10 файл, в DER формат.

Титулярят, респ. Създателя може да предостави електронната заявка:

- лично в Регистриращия орган или

- по електронен път и в онлайн информационна система на Доставчика/Регистриращия орган.

6.1.4. Доставка на Публичния ключ на Удостоверяващия орган до доверяващите се страни

Публичните ключове на Удостоверяващия орган на Доставчика са публично достъпни в интернет портала на Доставчика на адрес: http://www.infonotary.com.

Всяка Доверяваща се страна може да инсталира в системите под неин контрол служебните удостоверения на Доставчика.

6.1.5. Дължина на ключовете

Дължината на частния ключ на базовото удостоверение на Удостоверяващ орган – InfoNotary TSP Root CA е RSA - 4096 bits.

Дължината на частния ключ на оперативните удостоверения на Удостоверяващ орган RSA - 3072 бита.

За издаване на удостоверение за квалифициран електронен подпис, квалифициран електронен печат и автентичност на уебсайт, частният ключ на Титуляря, съответно Създателя следва да е с дължина най-малко 2048 бита за алгоритмите RSA.

6.2. Защита на Частния ключ и технически контрол на криптографския модул

6.2.1. Стандарти на криптографския модул

Удостоверяващият орган на Доставчика ползва сигурни и надеждни хардуерни криптографски модули, покриващи нормативните изисквания.

Хардуерните криптографски модули, които Доставчикът използва за съхранение на частните ключове на Удостоверяващия орган, са сертифицирани за високо ниво на сигурност и надеждност по FIPS 140-2, Level 3, FIPS 140-1 Level 2, CC EAL 4+ или по-високи.

Доставчика приема при издаване на квалифицирани удостоверения за квалифициран електронен подпис/печат, Титуляря/Създателя да използва устройство (смарт карти, HSM и други криптографски устройства) за създаване на електронен подпис/печат ("Qualified Signature Creation Device" – QSCD) със защитен профил, определен в съответствие с общите изисквания ("Common Criteria"), ниво на сигурност EAL 4+ или по-високо в

съответствие със защитен профил за квалифициран електронен подпис/печат съгласно Регламент (ЕС) № 910/2014 върху технически средства за сигурно генериране и съхранение на двойка ключове - криптографски смарт карти и други криптографски устройства.

6.2.2. Контрол на съхранението и ползването на Частен ключ

Едновременно с процедурата по генериране и инсталиране на ключовете на Удостоверяващия орган на Доставчика се извършва и процедура по съхраняване на частните ключове и тяхното архивиране.

Секретните части за достъп до базовия частен ключ, както и на всички оперативни частни ключове на Удостоверяващия орган се съхраняват поделени върху смарт карти, защитени с ПИН.

Предоставянето на поделените части на оторизираните за тяхното съхранение и представяне лица се документира писмено.

Частният ключ на Титуляря/Създателя се използва само в устройство за създаване на електронен подпис/печат или в устройство с еквивалентно ниво на сигурност (съгласно изискванията на Регламент (ЕС) № 910/2014).

Частният ключ на Титуляр/Създател на електронен печат на Облачно квалифицирано удостоверение се използва само в HSM на RQSCD на платформата за облачен КЕП на Доставчика и е достъпен през защитен профил на платформата чрез утвърдени защитни механизми за персонален контрол в съответствие с SAD/SAP/SAM (Signature Activation Data/Signature Activation Protocol/Signature Activation Module) и се активира чрез личен код за достъп (ПИН),парола или ключ под контрола на Титуляря.

6.2.3. Съхранение на Частните ключове

Частните ключове на Удостоверяващите органи на Доставчика се съхраняват в HSM и в криптиран вид, като за декриптирането са необходими секретните части за достъп до ключовете, които са поделени и се използват само от оторизираните за това лица, при наличие на необходим кворум от поне 2 лица. Съблюдаваната от Доставчика процедурата по съхранение на частните ключове, включва и процедурата при възстановяване на частните ключове за работа в резервен технически център, посредством резервен HSM при спазване на същите изисквания за споделено ползване на секретните части за достъп до ключовете от оторизирани за това лица и в определения кворум, но от минимум 2 лица.

Частният ключ на Титуляря/Създателя се съхранява на използваното за генериране на ключа устройство за създаване на квалифициран електронен подпис/печат съгласно изискванията на Регламент (ЕС) № 910/2014) – QSCD и е достъпен посредством ПИН и не може да бъде съхранен на друго устройство или извън него.

Частният ключ на Титуляря/Създателя на усъвършенстван подпис/печат се съхранява софтуерно и може да се репродуцира на друга система само под контрол Потребителя.

Частният ключ на Титуляр/Създателя на облачен електронен подпис/печат се генерира и съхранява в криптиран вид на RQSCD в платформата за облачен електронен подпис на Доставчика, съгласно изискванията на Регламент (ЕС) № 910/2014.

Съблюдаваната от Доставчика процедурата по съхранение на частните ключове на клиенти на RQSCD в платформата за облачен електронен подпис на Доставчика включва и процедурата при възстановяване на частните ключове за работа в резервен технически център, посредством резервен HSM на RQSCD. Копие на частните ключове на клиентите се съхранява в криптиран вид от Доставчика, единствено за целите на възстановяване при необходимост и за срок на управление на бекъпа на Доставчика.

6.2.4. Архивиране на Частните ключове

Доставчика архивира всички свои частни ключове на Удостоверяващите органи и ги съхранява за период от 10 години след изтичане периода им на валидност или след тяхното прекратяване.

Архивирането на ключовете се извършва от оторизирани за това служители на Доставчика.

Доставчика не прави копия и не архивира частните ключове на Титуляря/Създателя, които са генерирани на устройство за създаване на квалифициран електронен подпис/печат - QSCD.

При дефект, загуба или унищожаване на устройството за създаване на квалифициран електронен подпис/печат-QSCD от Титуляря/Създателя, Доставчика прекратява удостоверението, което е издадено във връзка с ключове, генерирани посредством това устройство.

За частният ключ на Титуляр/Създателя на облачен електронен подпис/печат, който е генериран в HSM на RQSCD в платформата за облачен електронен подпис на Доставчика, при дефект, загуба или

унищожаване на устройството, криптираните ключове се прехвърлят от бекъп копията в ново устройство, като е гарантиран персонален контрол върху ключа от страна на Титуляр/Създателя.

6.2.5. Прехвърляне на Частните ключове в и от криптографския модул

Доставчика генерира и съхранява всички свои частни ключове на Удостоверяващите органи във хардуерен криптографски модул (HSM) в криптиран вид, като прехвърлянето им може да бъде направено само в друго криптографско устройство в криптиран вид, при спазване на специална процедура за това, от оторизирани за целта служители на Доставчика и съгласно документираните и утвърдени вътрешни процедури и ползване на споделените права за достъп до секретните данни от минимум двама оторизирани служители.

Прехвърляне на частните ключове на Доставчика може да бъде извършено при необходимост от възстановяване след дефектиране на HSM или надграждане на технологичната инфраструктура на Доставчика.

Частният ключ на Титуляря/Създателя не може да бъде прехвърлен от/в устройството за създаване на квалифициран електронен подпис/печат съгласно изискванията на Регламент (ЕС) № 910/2014) на което е генериран.

Частният ключ на Титуляря/Създателя на облачен електронен подпис може да се прехвърли на друг HSM в криптиран вид в следните случаи:

- при необходимост от възстановяване след дефектиране на хардуерния криптографски модул, на който е създаден;
- надграждане на технологичната инфраструктура на Доставчика.

6.2.6. Активиране и деактивиране на Частни ключове

Частните ключове на Доставчика се активират в зависимост от типа на тяхната употреба.

Частния ключ на базовото удостоверение на Удостоверяващия орган (root CA) се съхранява деактивиран в режим „offline” на отделно криптографско устройство HSM и се активира по специална процедура от оторизирани за това лица, притежаващи поделени права за достъп до секретните дялове и в кворум минимум от 2 оторизирани лица и всички действия се документират и пазят в архива на Доставчика.

Частния ключ на Root CA се активира за изпълнение на подписване на новоиздадени удостоверения на Оперативни удостоверяващи органи и управление на вече издадени, включващо подписване на списъци с прекратени и спрени удостоверения CRL.

Частните ключове на Оперативните удостоверяващи органи се съхраняват и ползват в криптографско устройство HSM активирани, като при тяхното активиране и деактивиране се спазва специална процедура от оторизирани за това лица, притежаващи поделени права за достъп до секретните дялове и в кворум минимум от 2 оторизирани лица и всички действия се документират и пазят в архива на Доставчика.

Частен ключ на Титуляр/Създател се деактивира посредством изтриване на контейнерите, съдържащи частния ключ на устройството за създаване на квалифициран електронен подпис/печат или чрез физическо унищожаване на самото устройство.

Частен ключ на Титуляр/Създател на облачен електронен подпис/печат се активира чрез въвеждане на потребителския код за достъп към RQSCD (отдалеченото устройството за създаване на квалифициран електронен подпис/печат) и защитения потребителски профил в HSM за извършване на конкретна криптографска операция.

Частен ключ на Титуляр/Създател на облачен електронен подпис/печат се деактивира автоматично, след извършване на криптографската операция, за която е бил активиран и посредством преустановяване на логическия достъп до защитения потребителски профил в RQSCD на платформата за облачен подпис/печат.

6.2.7. Унищожаване на Частните ключове

Частните ключове на Доставчика се унищожават съгласно процедурата по унищожаване на частните ключове на Удостоверяващия орган на Доставчика от оторизирани за това служители на Доставчика.

Процедурата гарантира окончателното им унищожаване и невъзможността за тяхното възстановяване и ползване. Процесът по унищожаване на ключовете се документира и свързаните с това записи се съхраняват в архива на Доставчика.

Частен ключ на Титуляр/Създател се унищожава чрез изтриване на контейнера на устройството за създаване на квалифициран електронен подпис/печат или чрез физическо унищожаване на самото устройство.

Частен ключ на Титуляр/Създател на усъвършенстван електронен

подпис/печат се унищожава посредством неговото изтриване.

Частен ключ на Титуляр/Създател на облачен електронен подпис/печат се унищожава чрез изтриването му от защитения потребителски профил в RQSCD на платформата за облачен подпис/печат.

6.3. Други аспекти от управлението на двойката ключове

6.3.1. Архивиране на Публичен ключ

Доставчика архивира всички свои публични ключове и ги съхранява за период от 10 години след изтичане периода им на валидност или след тяхното прекратяване.

Публичните ключове на Титулярите/Създателите се съдържат в издадените за тях удостоверения и се съхраняват в Регистър на удостоверенията и се архивират и съхраняват за период от 10 години след изтичане периода им на валидност или след тяхното прекратяване.

6.3.2. Период на валидност на удостоверение и период на употреба на двойката ключове

доставчика издава квалифицирани удостоверения за електронен подпис, за квалифициран електронен печат, за автентичност на уебсайт на крайни потребители с определен период на валидност, който е вписан в съдържанието на удостоверението.

Удостоверенията издавани от Удостоверяващия орган на Доставчика за базовия публичен ключ и оперативните публични ключове се издават с определен период на валидност, който е вписан в съдържанието на удостоверението.

Периода на валидност на удостоверението е и период на валидност на употребата на двойката ключове свързани с него.

Създаването на подписи посредством ползването на частен ключ на удостоверение с изтекъл период на валидност е невалидно.

6.4. Данни за активиране

Доставчика записва на сигурни носители и архивира с високо ниво на защита данните за активиране, свързани с частните ключове на Удостоверяващия орган и дейности.

Титуляря/Създателя на печат е задължен да съхранява и пази от компрометиране персоналните данни за активиране на своя частен ключ.

6.4.1. Генериране и инсталиране на данни за активиране

Данни за активиране се създават при първоначална инициализация на устройство за създаване на квалифициран електронен подпис/ печат – QSCD или при генериране на двойка ключове.

Ако се използва QSCD и устройството се предоставя от Доставчика, то се инициализира в присъствието на Титуляря/Създателя и се генерират кодове за достъп: Потребителски (ПИН) – достъп до устройството и ключовете и Административен (АИН) – за разблокиране на ПИН и инициализация.

Кодовете за достъп са случайно генерирани от Регистриращия орган и се предоставят лично на Титуляря/Създателя или на упълномощено от тях лице. Кодовете се предават в запечатен, непрозрачен хартиен плик.

Титулярят/Създателят е длъжен да смени първоначалния ПИН и АИН за достъп посредством софтуера, който се предоставя заедно с устройството.

Ако Доставчика генерира двойка ключове за Титуляр/Създател, данните за активиране се предоставят лично на Титуляря/Създателя или на упълномощено от тях лице в едно с генерираната двойка ключове.

Генериране на двойката ключове за облачен подпис/печат на Титуляр/Създател се извършва в защитения потребителски профил на HSM на RQSCD на Доставчика, гарантиращ персонален контрол до частния ключ чрез данни за активиране на частния ключ, които са под контрола на Титуляря/Създателя.

Частния ключ се съхранява криптиран при Доставчика и се активира чрез персонален потребителския код за извършване на конкретна криптографска операция, който е изцяло под контрола Титуляря/Създателя.

Ако Титулярят/Създателят самостоятелно генерират двойката ключове, сами създават и управляват данните за активиране на ключовете.

6.4.2. Защита на данни за активиране

Титулярят/Създателят е задължен да съхранява и пази от компрометиране кодовете за достъп до устройството за създаване на квалифициран електронен подпис/ печат – QSCD и RQSCD за облачните подписи/печати.

При ползване на данните за активация на частния ключ и при определен брой неуспешни опити за използване на коректен код за достъп, достъпа до устройството се блокира и може да бъде разблокиран от Титуляря/Създателя с притежавания от него АИН (административен код за достъп).

Доставчика не съхранява копие от генерирани кодове за достъп и не може да възстанови персоналния достъп на Титуляря/Създателя до устройството след неговото блокиране.

6.5. Контрол на компютърната сигурност

6.5.1. Специфични изисквания към компютърната сигурност

Доставчикът осигурява и използва процедури и методи за управление на сигурността на ползваното техническо и технологично оборудване в своята инфраструктура в съответствие с общоприети международни стандарти за управление на информационната сигурност. Доставчикът осигурява и провеждане на изпитвания и проверки на техническото оборудване и технологиите посредством методика за оценка на сигурността, базирана на разработената към стандарта ISO Standard 15408 обща методика за оценка на сигурност.

Управлението на компютърните системи, на които работят всички критични компоненти от инфраструктурата на Доставчика в оперативен и резервен център, са осигурени за защита на достъпа до софтуера и информационните данни се изпълняват в съответствие с политиката за информационна сигурност на Доставчика.

Дружеството е въвело система за управление сигурността на информацията ISO/IEC 27001:2013 и извършва управлението на сигурността на ползваното техническо и технологично оборудване в своята инфраструктура в съответствие със стандарта.

6.5.2. Рейтинг на компютърната сигурност

Степента на надеждност на използваните от Доставчика техническо

оборудване, технологии и системи покрива нормативните изисквания за извършване на дейност като Доставчик на удостоверителни услуги и се определя в съответствие с Политиката за информационна сигурност на Инфонотари ЕАД.

6.6. Техническият контрол на жизнен цикъл

Доставчикът осигурява пълен технически контрол върху жизнения цикъл на системите, посредством които се предоставят удостоверителните услуги от Доставчика.

Във всички стадии от изграждането и експлоатацията на системите се спазват процедури и правила, описани във вътрешни документи на Доставчика.

Резултатите от тестовете се документират и съхраняват в архива на Доставчика.

6.7. Контрол на сигурността на мрежата

Доставчикът поддържа високо ниво на сигурност на мрежата си и средства за отчитане на непозволен достъп.

6.8. Удостоверяване на време

Доставчикът предоставя на Абонатите си услугата по удостоверяване на време, като издава квалифицирани електронни времеви печати.

Електронния времеви печат са данни в електронна форма, които свързват други данни в електронна форма с конкретен момент във времето и представляват доказателство, че последните данни са съществували в съответния момент.

Електронния времеви печат издаден от Доставчика удостоверява дата и час на представяне на електронен документ, подписан с частен ключ, съответстващ на публичния ключ, включен в удостоверение за квалифициран електронен подпис, издадено от Доставчика. Квалифициран електронен времеви печат се издава на физически и на юридически лица, които са титуляри или са доверяваща се страна.

Дейностите по удостоверяване на време и осигуряване на независим източник на време се изпълняват самостоятелно от Доставчика.

Системата на Доставчика, осигуряваща удостоверяването на време

InfoNotary Qualified TimeStamping Service е разработена и услугите се предоставят съгласно Регламент (ЕС) № 910/2014 и в пълно съответствие с ETSI EN 319 422, ETSI TS 119 421, IETF RFC 3161 и IETF RFC 5816 и ETSI TS 102 023 v.1.2.1 (2003-01) Policy Requirements for time-stamping authorities.

6.8.1. Процедура по предоставяне на услугата удостоверяване на време

Системата на Доставчика, осигуряваща удостоверяването на време InfoNotary Qualified TimeStamping Service приема заявки и връща отговори във формат, дефиниран от RFC 3161 - „Internet X.509 Public Key Infrastructure - Time-Stamp Protocol".

Издаваните квалифицирани електронни времеви печати (time stamp токъни) са съвместими с RFC 3161. Услугата издава RSA 2048 битови криптирани с алгоритъм SHA-256 удостоверения за време

В заявката е необходимо да се съдържа хеш на електронния подпис на документа, чието време на подписване се удостоверява, и версия на заявката.

Опционално може да съдържа и заявка за включване в отговора на подписващото удостоверение заедно с веригата от удостоверения на Удостоверяващия орган.

Заявката за удостоверяване на време може да се генерира чрез специализиран клиентския софтуер на "ИНФОНОТАРИ" ЕАД.

Квалифицирания електронен времеви печат (токън), издаван от Доставчика, заверява точната дата и час, в които клиентският електронен документ е регистриран в TimeStamp сървъра на Доставчика. Издадените времеви печати се записват в регистъра на Доставчика.

Точността, с която се издават електронен времеви печат от Доставчика, е +/- 500ms (половин секунда) или по-добро спрямо UTC.

Квалифицирания електронен времеви печат (токън), издаван от Доставчика, съдържа следните елементи:

- статус – цяло число, показващо дали подписването е минало успешно;
- версия на удостоверението за време (версия 1);
- хеш-а на подписа, който се е съдържал в заявката;
- последователен уникален сериен номер;
- време на подписване по UTC;

- идентификация на Timestamp удостоверителя – Доставчика.

Удостоверенията за време се подписват с частен ключ на Доставчика, предназначен само и единствено за тази дейност от оперативния орган InfoNotary Qualified TimeStamping Service CA.

Операцията по подписване на удостоверенията за време се извършва от хардуерен защитен модул с високо ниво на надеждност и сигурност.

Системата на Доставчика за удостоверяване на време е под режим на висок контрол на физически и технологичен достъп и се съхранява в специализирано помещение с контрол на достъпа на оторизирани служители.

Услугата за издаване на квалифицирани електронни времеви печат е достъпна на http://ts.infonotary.com/tsa

6.8.2. Независим източник на точно време

Доставчикът оперира собствена система за осигуряване на независим източник на точно време (Time Sinhronizator), поддържащ следните протоколи:

- NTPv2 (RFC 1119)
- NTPv3 (RFC 1305)
- NTPv4 (IETF Draft Standard)
- SNTP (RFC 2030)
- Daytime Protocol (RFC876)
- Time Protocol (RFC 868)
- SNMPv1 (RFC 1157), SNMPv3 (RFC 3411-3415)

Системата се синхронизира за точност посредством GPS, синхронизация от други NTP сървъри или Dial-up връзки.

Всички данни за точно време, предавани от TimeSinhronisator към TimeStapm сървъра, са криптирани от самия синхронизатор и защитени от модификация и компрометиране.

6.9. Валидиране

Доставчикът предоставя квалифицирана услуга за валидиране на квалифицирано удостоверение, квалифициран електронен подпис и квалифициран електронен печат **InfoNotary Qalified Validation Service – IQVS.**

Квалифицираната услуга за валидиране на квалифициран електронен подпис/печат, позволява да се извърши надеждна проверка на неговата валидност, както и на валидността на издадените удостоверения, включително удостоверяване на техния квалифициран статут.

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).

Резултатите от проверката се представят в доклад, който съдържа статус/заключение - ВАЛИДЕН (PASSED), НЕВАЛИДЕН (FAILED) или НЕОПРЕДЕЛЕН (INDETERMINATE). Докладът се подпечатва с квалифицирано удостоверение за електронен печат на Инфонотари, което гарантира целостта и верността на данните в доклада.

Системата на Доставчика, предоставяща услугата по валидиране, е разработена и проверката на валидността квалифицираните електронни подписи/печати и удостоверения се извършва в съответствие с Регламент (ЕС) № 910/2014 и ETSI стандартите: ETSI TS 119 441; ETSI TS 119 442; ETSI TS 119 101; ETSI EN 319 102-1; ETSI TS 119 102; ETSI TS 319 172-1.

Системата на Доставчика предоставяща услугата по валидиране е под режим на висок контрол на физически и технологичен достъп от оторизирани служители.

6.9.1. Предоставяне на услугата валидиране

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

Доставчикът предоставя услугата чрез web клиент (Signature Validation Aplication - SVA), който работи през браузър, и който използва защитен комуникационен канал/защитена сесия (чрез HTTPS протокол и удостоверение за автентичност на web 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 параментри на заявката и изпраща заявката към сървъра за валидиране.

Услугата може да се използва и в автоматичен режим, като условията се уреждат в договор между Доставчика и Доверяваща се страна.

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.

7. Профили

7.1. Профил на квалифицирано удостоверение

Квалифицираните удостоверения, които се издават от Доставчика съгласно удостоверителните му политики и настоящата практика, отговарят на изискванията на Регламент (EU)910/2014.

В квалифицираните удостоверения, които се издават от Доставчика, са имплементирани и се ползват и следните стандарти:

- Профилите на квалифицираните удостоверения за крайни потребители и профила на Списъка със спрени и прекратени удостоверения (CRL) кореспондират на формата включен в ITU-T X.509 v.3 standard.
- OCSP профила е съобразно RFC 6960, и

- Профила за квалифицирания електронен времеви печат е съобразно RFC 3161.

7.1.1. Номер на версия

Доставчикът издава удостоверения във формат X.509 v.3.

Номерът на версията на удостоверението е вписан в самото удостоверение.

7.1.2. Разширения в удостоверенията (Extensions)

7.1.2.1. Задължителни разширения

Атрибут "Basic Constrains"

Атрибутът оказва типа на Титуляря на удостоверението – Удостоверяващ орган или краен потребител. Атрибутът е критичен "Critical".

Атрибут "Key Usage"

Определя ограниченията в употребата на удостоверението според предназначението за ползване на ключа. Атрибутът е критичен "Critical".

Атрибутът се използва, за да се ограничи употребата на ключа спрямо възможните употреби:

- Digital Signature (цифров подпис) – за автентификация;
- Non-Repudiation (неотменяемост) – за доказване употребата на електронния подпис;
- Key Encipherment (шифриране на ключ) – за шифриране на ключове;
- Data Encipherment (шифриране на данни) – за шифриране на данни;
- Certificate Signing (електронно подписване на удостоверение) – използва се само от Удостоверяващи органи на Доставчика;
- CRL Signing (електронно подписване на Списък на спрени и прекратени удостоверения) – за подписване на CRLs, използва се само от Удостоверяващи органи.

Атрибут "Extended Key Usage"

Атрибутът се използва, за да укаже приложенията, в които може да бъде ползван ключът – защита на електронна кореспонденция, електронна автентификация и др.

Атрибут "Authority Key Identifier"

Атрибутът съдържа SHA1 от DER-кодирания публичен ключ на издателя.

Атрибут "Subject Key Identifier"

Атрибутът съдържа SHA1 от DER-кодирания публичен ключ.

Атрибут "CRL Distribution Points"

Атрибутът съдържа връзка към Списъка на спрените и прекратени удостоверения, който се поддържа от Доставчика.

Атрибут "Authority Info Access"

Атрибутът съдържа връзка към OCSP услугата, поддържана от Доставчика и предоставяща информация за статуса на удостоверението посредством OCSP протокол.

Атрибут "Qualified Certificate Statement"

Атрибутът е задължителен за удостоверенията за квалифициран електронен подпис, квалифициран електронен печат и автентичност на уебсайт, които Доставчикът издава, и съдържа информация дали удостоверението е издадено като квалифицирано и дали частния ключ е генериран и се съхранява върху устройства за създаване на електронен подпис (QSCD). Доставчикът може да вписва и други атрибути в зависимост от политиката и искането на Титуляря/Създателя.

Атрибут "Certificate Policy"

Атрибутът оказва политиките, при които Доставчикът издава удостоверението и съдържа идентификатор (OID) на съответната удостоверителна политика според типа на квалифицираното удостоверение.

	Име	InfoNotary Policy Identifier	ETSI Policy Identifier
Квалифицирано удостоверение за квалифициран електронен подпис на физическо лице	InfoNotary Qualified Natural Person Signature CP	1.3.6.1.4.1.22144.3.1.1	0.4.0.194112.1.2 (QCP-n-qscd)

Квалифицирано удостоверение за квалифициран електронен подпис на физическо лице с делегирани правомощия	InfoNotary Qualified Delegated Signature CP	1.3.6.1.4.1.22144.3.1.2	0.4.0.194112.1.2 (QCP-n-qscd)
Квалифицирано удостоверение за квалифициран електронен печат на юридическо лице	InfoNotary Qualified Legal Person Seal CP	1.3.6.1.4.1.22144.3.2.1	0.4.0.194112.1.3 (QCP-l-qscd)
Квалифицирано удостоверение за автентичност на уебсайт	InfoNotary Qualified Validated Domain CP	1.3.6.1.4.1.22144.3.3.1	0.4.0.194112.1.4 (QCP-w)
Квалифицирано удостоверение за автентичност на уебсайт за организация	InfoNotary Qualified Organization Validated CP	1.3.6.1.4.1.22144.3.3.2	0.4.0.194112.1.4 (QCP-w)
Квалифицирано удостоверение за автентичност на уебсайт за организация по PSD2	InfoNotary Qualified PSD2 WA CP	1.3.6.1.4.1.22144.3.3.3	0.4.0.194112.1.4 (QCP-w)
Квалифицирано удостоверение за усъвършенстван електронен подпис на физическо лице	InfoNotary Qualified Certificate for Natural Person AESignature CP	1.3.6.1.4.1.22144.3.6.1	0.4.0.194112.1.0 (QCP-n)
Квалифицирано удостоверение за усъвършенстван електронен подпис на физическо лице с делегирани правомощия	InfoNotary Qualified Certificate for Delegated AESignature CP	1.3.6.1.4.1.22144.3.6.2	0.4.0.194112.1.0 (QCP-n)
Квалифицирано удостоверение за усъвършенстван електронен печат на юридическо лице	InfoNotary Qualified Certificate for Legal Person AESeal CP	1.3.6.1.4.1.22144.3.7.1	0.4.0.194112.1.1 (QCP-l)

	InfoNotary Qualified Validaton Service CP	1.3.6.1.4.1.22144.3.5.2	0.4.0.19172.1 (id-etsi-sars-SigType5)
Квалифицирано удостоверение за усъвършенстван електронен печат на юридическо лице по PSD2	InfoNotary Qualified Certificate for PSD2 AESeal CP	1.3.6.1.4.1.22144.3.7.2	0.4.0.194112.1.1 (QCP-l)

Идентификаторите за политиките на квалифицираните удостоверения, включени в профилите на квалифицираните удостоверения са:

Квалифицирани политики

- QCP-n-qscd: Itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-natural-qscd (2);
- QCP-l-qscd: itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-legal-qscd (3);
- QCP-n: Itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-natural(0);
- QCP-l: itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-legal(1);
- QCP-w: itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-web(4);
- Natural Person Semantics: itu-t(0) identified-organization(4) etsi(0) id-cert-profile(194121) id-etsi-qcs-semantics-identifiers(1) id-etsi-qcs-semanticsId-Natural(1);
- Legal Person Semantics: itu-t(0) identified-organization(4) etsi(0) id-cert-profile(194121) id-etsi-qcs-semantics-identifiers(1) id-etsi-qcs-SemanticsId-Legal(2);
- QcCompliance: itu-t(0) identified-organization(4) etsi(0) qc-profile(1862) qcs(1) qcs-QcCompliance(1);
- Secure Signature Creation Device (SSCD): itu-t(0) identified-organization(4) etsi(0) qc-profile(1862) qcs(1) 4;
- id-etsi-qct-esign (oid=0.4.0.1862.1.6.1)
- id-etsi-qct-eseal (oid=0.4.0.1862.1.6.2)
- id-etsi-qct-web (oid=0.4.0.1862.1.6.3)
- id-etsi-psd2-qsStatement (oid=0.4.0.19495.2)
- id-etsi-sars-SigType 5

7.1.3. Идентификатори на алгоритмите на електронния подпис

Идентификаторът за алгоритъм на електронния подпис идентифицира:

- Hash-function: sha256-with-RSA;
- Алгоритъм за криптиране: RSA.

7.1.4. Форми на именуване

Виж т. 3.1.3 от документа.

7.1.5. Ограничения на имената

Виж т. 3.1.4 от документа.

7.2. Профил на Списъка на спрените и прекратени удостоверения (CRL)

7.2.1. Номер на версия

Списъците на спрените и прекратени удостоверения, които Доставчикът поддържа в Публичния регистър на удостоверенията, са във формат X.509 v.2.

7.2.2. Атрибути на списъка и на публикуваните в него удостоверения

7.2.2.1. Атрибути на Списъка

7.2.2.1.1. Основни x509 CRL атрибути

Атрибут	Стойност
Version	2 (0x01)
Publication date	Датата и часът на подписване на CRL
Subsequent publication date	Датата и часът на подписване на CRL+ 24 часа
Electronic signature algorithm on CRL	rsaWithSHA256
CRL issuer attributes *(x509 CRL Issuer DN)*	Атрибутите на Издателя на CRL съвпадат с атрибутите на Титуляря на подписващото удостоверение.

7.2.2.1.2. Допълнителни атрибути на Списъка:

Атрибут	OID	Стойност
/AuthorityKeyIdentifier	2.5.29.35	"SubjectKeyIdentifier" на подписващото удостоверение на Издателя
/cRLNumber	2.5.29.20	Номер на публикувания CRL в Публичния регистър на удостоверенията на Доставчика; 20-байтово число

7.2.2.1.3. Атрибути на Удостоверенията, включени в списъка:

Атрибут	Стойност	
Сериен номер	Уникалният номер на удостоверението в регистъра на Доставчика	
Дата на спиране/прекратяване	Датата, часът и минутата на спиране/прекратяване на удостоверението	
Причина за спиране/прекратяване	unspecified	0
	keyCompromise	1
	cACompromise	2
	affiliationChanged	3
	superseded	4
	cessationOfOperation	5
	certificateHold	6
	removeFromCRL	8
	privilegeWithdrawn	9
	aACompromise	10

Значение на кодовете за означаване на причината за спиране и прекратяване на удостоверение:

- Unspecified – удостоверение е прекратено по друга причина

- KeyCompromise – компрометиран частен ключ, съответстващ на публичния ключ, включен в съдържанието на квалифицираното удостоверение;
- CACompromise – компрометиран частен ключ на Удостоверяващия орган;
- AffiliationChanged – променен статус на Титуляря – промяна в юридическото лице или промяна в представителната власт, отнемане на представителната власт по отношение на юридическото лице;
- Superseded – удостоверение е заместено от друго удостоверение;
- CessationofOperation – прекратяване на ползването;
- CertificateHold – действието на удостоверение е спряно
- privilegeWithdrawn – променена привилегия

7.3. Профил на OCSP

7.3.1. Профил на OCSP Заявката

7.3.1.1. Атрибути на заявката

Атрибут	Стойност
Версия	1 (0x00)
Заявител	Игнорира се
Списък идентификатори на удостоверение	съобразно RFC 6960 (виж 1.2)
Разширения на заявката	Игнорира се

7.3.1.2. Идентификатор на Удостоверение (УЕП)

Атрибут	Стойност
Алгоритъм на криптографска контролна сума (ККС)	SHA-1
Издател на УЕП	SHA-1 от DER-кодираното DN на издателя
ККС на ключа на издателя на УЕП	SHA-1 от DER-кодираното subjectPublcKeyInfo на издателя (без T и L).
Сериен номер на УЕП	Уникален в регистъра на Доставчика; 8-байтово число

7.3.2. Профил на OCSP Отговор

7.3.2.1. Общи атрибути

Атрибут	Стойност
Статус	successfull – съобразно RFC 6960 malformedRequest – съобразно RFC 6960 internalError – *не се използва* tryLater – не се използва sigRequired – не се използва unauthorized – *не се използва*
Тип отговор	id-pkix-ocsp-basic (1.3.6.1.5.5.7.48.1.1)
Отговор (виж 2.2)	съобразно RFC 6960

7.3.2.2. Атрибути на отговора съобразно id pkix-ocsp-basic (1.3.6.1.5.5.7.48.1.1)

Атрибут	Стойност
Данни към отговора (виж 7.3.3)	съобразно RFC 6960
Алгоритъм на електронния подпис върху отговора	FIPS-186 DSS;
Електронен подпис	съобразно RFC 6960
Списък удостоверения на издатели	не се прилага

7.3.3. Данни към OCSP отговора

Атрибут	Стойност
Версия	1 (0x00)
Идентификатор на OCSP Responder	DN на подписващото УЕП
Дата на публикация	Датата, часът и минутата на подписване на отговора
Индивидуални отговори (виж 2.4)	съобразно RFC 6960
Разширения	не се прилагат

7.3.4. Индивидуални OCSP отговори

Атрибут	Стойност
Идентификатор на УЕП	съобразно RFC 6960 (виж 7.3.1.1.1)
Състояние	good – съобразно RFC 6960 revoked – съобразно RFC 6960 unknown – съобразно RFC 6960
Дата на публикация	Датата, часът и минутата на подписване на CRL
Дата на следваща публикация	Датата и часът на подписване на CRL+ 24 часа
Разширения	не се прилагат

7.4. Профил на TimeStamp

7.4.1. Профил на TimeStamp Заявката

Атрибут	Стойност
HTTP Content-Type	application/timestamp-query
Версия	1 (0x01)
Заявена политика	Празно или 1.3.6.1.4.1.22144.3.4.1

7.4.2. Профил на TimeStamp Отговор

Атрибут	Стойност	
HTTP Content-Type	application/timestamp-reply	
Статус:	granted	съобразно RFC 3161;
	grantedWithMods	съобразно RFC 3161, не се ползва;
	rejection	съобразно RFC 3161;
	waiting	съобразно RFC 3161, не се ползва;
	revocationWarning	съобразно RFC 3161, не се ползва;

Възможни грешки:	BadAlgIdentifier; badRequest; badDataFormat timeNotAvailable unacceptedPolicy unacceptedExtension addInfoNotAvailable systemFailure	съобразно RFC 3161;
Политика	1.3.6.1.4.1.22144.3.4.1	
Маркер за време	UTC, текущото време от GPS	
Прецизност	0,5 секунди	
Списък с удостоверенията на издателя	Съдържа веригата на издателя на TSA удостоверението	

7.5. Доклад за валидиране

Резултатите от процеса на валидиране се представят в основен и подробен доклад в съответствие с ETSI TS 119 102-1.

Основният доклад съдържа:

- Политиката на валидиране;
- Статус/заключение;
- Дата и час 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 (TOTAL-PASSED) или НЕВАЛИДЕН (TOTAL-FAILED).

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

8. ПРОВЕРКА И КОНТРОЛ НА ДЕЙНОСТТА

8.1. Регулярна или обстоятелствена проверка

Одитите, които се извършват на Доставчика, се отнасят до обработката на информационни данни и управлението на ключови процедури. Целта им е да контролират и "Практиката при предоставяне на квалифицирани удостоверителни услуги", доколкото тя е съвместима с интегрираната в дружеството система за управление, която включва изискванията на IEC 27001: 2013, с Регламент (ЕО) № 910/2014 и решенията и мерките за вътрешно управление.

Извършените одити на Доставчика се отнасят за всички Удостоверяващи органи, принадлежащи към базовия удостоверяващ орган, Регистрационните органни, както и други елементи на удостоверителната инфраструктура на Доставчика.

Дейността на Доставчика подлежи на постоянен вътрешен контрол, упражняван от Съвета на директорите на "ИНФОНОТАРИ" ЕАД.

За целите на вътрешния контрол Съветът на директорите на "ИНФОНОТАРИ" ЕАД назначава насрочени (рутинни) или непланирани одити по реда и обхвата съгласно вътрешните правила на Доставчика.

Доставчикът упражнява постоянен контрол върху дейността на Регистрационните органи и техните локални регистрационни офиси.

Доставчикът е обект на одит поне веднъж на всеки 24 месеца от орган за оценка на съответствието. Целта на одита е да потвърди, че ИНФОНОТАРИ ЕАД като квалифициран доставчик на удостоверителни услуги и предоставените от него квалифицирани удостоверителни услуги отговаря на изискванията, посочени в Регламент (ЕС) № 910/2014. Доставчикът представя на надзорния орган съответния доклад за оценка на съответствието в рамките на три работни дни от получаването му.

Надзорният орган може по всяко време да извърши одит или да поиска орган за оценка на съответствието да извърши оценка на съответствието на Доставчика.

8.2. Квалификация на проверяващите лица

Външен одит за оценка на съответствието на дейността на Доставчика в съответствие с разпоредбите на Регламент (ЕС) 910/2014 се извършва от акредитиран и независим орган за оценка на съответствието и се регулира от стандарт ISO / IEC 17065: 2012: Оценка на съответствието - Изисквания към органите, сертифициращи продукти, процеси и услуги.

Външната проверка от Надзорен орган се извършва по всяко време от упълномощени служители на Надзорния орган.

Вътрешният одит се извършва от служителите на Доставчика с необходимия опит и квалификация.

Дейността на Регистриращия орган се одитира от служители на Доставчика, специално упълномощени от Съвета на директорите на Доставчика, или от външни проверяващи лица.

8.3. Връзка между проверяващите лица и проверяваната организация

Ангажираните за извършване на проверки Проверяващи лица трябва да бъдат независими, несвързани директно или индиректно и нямащи никакви конфликтни интереси с Доставчика.

Отношенията между външните проверяващи лица и Доставчика се уреждат с писмен договор.

8.4. Обхват на проверката

Обхватът на извършваните проверки е съобразно вида на осъществявания контрол и проверяваните органи.

В обхвата на вътрешна проверка са всички дейности, документи и обстоятелства от оперирането на Доставчика, които могат да включват, но не се ограничават до:

- съответствието на оперативните процедури и принципи на работа на Доставчика с дефинираните в Практиката при предоставяне на квалифицирани удостоверителни услуги процедури и политики;

- управлението на инфраструктурата, включена в обслужването на удостоверителните услуги.

Проверката от Надзорния орган обхваща законовите изисквания за дейността на Доставчика съгласно приложимото законодателство в областта на квалифицираните удостоверителни услуги.

Одитът от органа за оценка на съответствието обхваща цялата операция на Доставчика за предоставяне на квалифицирани удостоверителни услуги и прилагане на всички стандарти и документи за стандартизация, свързани с Регламент (ЕС) № 910/2014: Документация; Архиви; Информационни данни, свързани с издаването и управлението на квалифицирани удостоверения; Физическа и информационна сигурност и надеждност на технологичната система и управление; Удостоверяващи органи.

Обхватът на вътрешните одити включва:

Проверка на дейността на доставчика и съответствието ѝ с Практиката при предоставяне на квалифицирани удостоверителни услуги; сравняване на практиките и процедурите, описани в този документ, с тяхната практическа реализация при осъществяване на дейността на Доставчика; проверка на дейността на Регистрационния орган; други обстоятелства, факти и дейности, свързани с инфраструктурата, по преценка на ръководството на ИНФОНОТАРИ ЕАД.

8.5. Предприемане на действия за отстраняване на недостатъците

Съвета на директорите на "ИНФОНОТАРИ" ЕАД определя действията, необходими за отстраняване на регистрираните недостатъци и сроковете за тяхното отстраняване.

8.6. Съобщаване на резултатите

Резултатите от направените проверки се съхраняват по условията и реда за съхраняване на данни и информация по настоящия документ.

Получените пълни доклади от Органа по оценяване на съответствието трябва да бъдат предадени на Надзорния орган до три дни от получаването им.

9. ДРУГИ БИЗНЕС И ПРАВНИ УСЛОВИЯ

9.1. Цени и такси

Доставчикът определя цени и абонаментни такси за ползване на предоставяните от него квалифицирани удостоверителни услуги и цените на стоки, свързани с тези услуги (смарт карти, четци, токъни и др.) и ги публикува в Тарифа за предоставяне на квалифицирани удостоверителни услуги (Тарифа, Тарифата), публично достъпна на адрес: http://www.infonotary.com/.

Доставчикът си запазва правото да променя едностранно Тарифата по всяко време от действието на договора, като промените се одобряват от Съвета на директорите на "ИНФОНОТАРИ" ЕАД и се публикуват и са публично достъпни на URL адрес: http://www.infonotary.com/.

Доставчикът уведомява Абонатите индивидуално или с факта на публикуване на промените. Промените влизат в сила и имат действие спрямо Абоната от деня, следващ уведомяването или публикацията.

Промените имат действие за в бъдеще и не засягат вече платени авансово еднократни или абонаментни такси, предхождащи влизането в сила на промяната.

9.1.1. Възнаграждения по Договор за квалифицирани удостоверителни услуги

Стойността на Договора за квалифицирани удостоверителни услуги, който Абонатът сключва с Доставчика, се формира от възнагражденията, дължими от Абоната за заявени за ползване от него услуги и стоки, въз основа Тарифа за предоставяне на квалифицирани удостоверителни услуги.

Авансово платени или абонаментни такси не подлежат на връщане на Абоната, ако в срока, за който са заплатени, не са консумирани.

В случай на предсрочно прекратяване на издадено и прието от Титуляря/Създателя на печат квалифицирано удостоверение и/или на договора за квалифицирани удостоверителни услуги по причини, за които Доставчикът не отговаря, на Абоната не се дължи връщане на остатъка от заплатената стойност за остатъка от срока на прекратеното квалифицирано удостоверение.

Всички дължими по договора суми се заплащат от Абоната по банков път, чрез системата ИЗИПЕЙ или ePay.bg. Плащането по банков път

се счита за извършено след получаване на потвърждение за заверяване на банковата сметка на Доставчика с пълния размер на дължимите суми. В стойността на стоките и услугите не са включени разходите за заплащане на дължимото по договор възнаграждение, които Абоната дължи на доставчиците на платежни услуги.

9.1.2. Фактуриране

Доставчикът издава на Абоната данъчна фактура за предоставяните услуги в до 5-дневен срок от плащането.

9.1.3. Политика за връщане на удостоверението и възстановяване на плащането

При направени възражения от Титуляря/Създателя на печат на квалифицирано удостоверение в 3-дневен срок от публикуването му в Публичния регистър на удостоверенията относно непълноти или неточности, съдържащи се в него, Доставчикът прекратява възразеното удостоверение и издава ново безплатно или възстановява направеното плащане за издаване на възразеното удостоверение.

9.2. Финансови отговорности

9.2.1. Финансова отговорност

ИНФОНОТАРИ ЕАД носи отговорност за предоставяните квалифицирани удостоверителни услуги пред Титуляря/ Създателя на печат, пред Абоната и пред всички трети лица, които се доверяват на издадените от Доставчика квалифицирани удостоверения.

ИНФОНОТАРИ ЕАД носи отговорност само за вредите, настъпили в резултат на използване на квалифицирано удостоверение в периода на неговата валидност и само ако не са налице обстоятелства, изключващи отговорността на Доставчика.

9.2.2. Застраховка на дейността

Инфонотари ЕАД има сключена подходяща застраховка с предмет отговорността на Доставчика на квалифицирани удостоверителни услуги за нанесени щети в съответствие с Регламент (ЕС) № 910/2014 и с националното право.

При настъпване на събитие, което би могло да доведе до предявяването на претенция, покрита по застраховката, увреденото лице е длъжно незабавно, не по-късно от 7 дни след като събитието му е станало

известно, да уведоми писмено Доставчика и Застрахователя на Доставчика.

Абонатите са длъжни незабавно да изпратят писмено уведомление на Доставчика за настъпилата вреда и да съдействат на Доставчика на неговия Застраховател при установяване на фактите, потвърждаващи претенцията.

9.2.2.1. Застрахователно покритие за крайните потребители

На обезщетение по застраховката на Доставчика подлежат всички суми, ненадхвърлящи максималния лимит на обезщетение съгласно националното законодателство, които Доставчика бъде задължен да заплати като компенсация за неимуществени и/или имуществени вреди, причинени на Титуляря/Създателя на печат на квалифицирано удостоверение и на всички трети лица вследствие небрежност, грешки или пропуски при осъществяване на застрахованата дейност, за които Доставчикът отговаря съгласно българското законодателство или законодателството на страната, в която е настъпила вредата.

Доставчика има право да откаже да изплати обезщетение за вреди, което надхвърля максималния лимит на обезщетение.

В отношенията на Доставчика с Абонатите и всички трети страни се прилагат тези лимити на обезщетение и условия, които са в сила към датата на настъпване на вредата.

Застраховката не покрива и Доставчикът не отговаря за претърпени вреди следствие от:

- неспазване на задълженията на Титулярите на квалифицирани удостоверения, Създателите на печат и Абонати съгласно Практиката за предоставяне на квалифицирани удостоверителни услуги, удостоверителната политика за съответния вид квалифицирано удостоверение и Договора за предоставяне на квалифицирани удостоверителни услуги;
- компрометиране или загуба на частен ключ на Титуляр, съответно Създател, поради неполагане на дължимата грижа за опазването или ползването му;
- неспазване на изискванията относно полагане на дължима грижа за проверка валидността на удостоверението за електронния подпис, удостоверението за електронния печат и на

квалифицирания електронен времеви печат от Доверяващите се страни;

- форсмажор, аварии и други събития, които са извън контрола на Доставчика.

9.3. Конфиденциалност на информацията

Доставчикът съблюдава всички приложими правила за защитата на личните данни и на конфиденциалната информация, събирана с оглед на дейността му.

9.3.1. Обхват на конфиденциалната информация

Доставчикът приема за конфиденциална информацията, съдържаща се в и отнасяща се до:

- всяка информация, за Титуляря/Създателя, упълномощения представител и Абоната, извън публикуваната в удостоверението;
- причината за спиране или прекратяване действието на удостоверение извън публикуваната информация за статуса на удостоверението;
- кореспонденция, свързана с дейността на Доставчика;
- частните ключове на Доставчика;
- частния ключ на Титуляря/Създателя на печат, когато се съхранява от Доставчика по възлагане от Титуляря/Създателя;
- Договори за предоставяне на квалифицирани удостоверителни и други услуги;
- архивите за направени искания за издаване, спиране, възобновяване и прекратяване на удостоверения;
- записи и архиви на логове, бази данни и друга непублична архивна информация;
- записи на външни и вътрешни проверки и доклади;
- планове за възстановяване след бедствия и непредвидени случаи
- доклади на органа за оценяване на съответствието, други външни одитори и Надзорния орган.

9.3.2. Информация извън обхвата на конфиденциалната информация

Не се третират като конфиденциални следните данни и информация:

- удостоверенията, публикувани в регистъра на Доставчика;
- данните, които се съдържат в удостоверенията;

- данните за статуса на удостоверенията, публикувани в Списъка на спрените и прекратени удостоверения.
- всички публични документи, публикувани в документния регистър на Доставчика.

9.3.3. Задължение за защита на конфиденциалната информация

Доставчикът не разкрива и не може да се иска от него да разкрива или да предоставя на трети лица каквато и да било конфиденциална информация, освен освен когато е задължен по силата на специален закон да разкрие такава информация или по искане на компетентен орган на властта.

Регистриращите органи, Абонатите, Титулярите, Създателите или упълномощените от тях лица нямат право да разпространяват или да допускат разпространяване на информация, станала им известна при или по повод изпълнение на задълженията им по договорите с Доставчика, без предварително изрично писмено разрешение от другата страна.

9.4. Поверителност на личните данни

Доставчикът е регистриран като администратор на лични данни от Комисията за защита на личните данни по реда на ЗЗЛД и осигурява законосъобразна обработка на личните данни, предоставени във връзка с квалифицираните удостоверителни услуги в съответствие с Регламент (ЕС) 2016/679 (GDPR) и националното право.

Доставчикът съхранява и обработва личните данни, които са му предоставени в качеството му на Квалифициран доставчик на квалифицирани удостоверителни услуги, в съответствие със Закона за защита на личните данни и Регламент (ЕС) 2016/679 (GDPR).

Видът и количеството на събираните лични данни е пропорционално на целите и употребата им. Личните данни се използват само във връзка с предоставяне на квалифицирани удостоверителни услуги.

Информацията, която се събира от Доставчика за Титуляря/Създателя на печат/ Упълномощен представител и Абонат, е само за целите на издаване и поддържане на квалифицирани удостоверения или предоставяне на друга квалифицирана удостоверителна услуга.

Информацията, включена в квалифицираните удостоверения може да съдържа лични данни за Титуляря/Създателя на печат по смисъла на

Закона за защита на личните данни и Регламент (ЕС) 2016/679 (GDPR). Тези данни се съхраняват и обработват в бази данни на Доставчика.

Доставчика осигурява публичен достъп на трети лица до регистъра на издадените удостоверения. По изрично искане на Титуляря/Създателя на печат, Доставчикът ограничава достъпа за четене и изтегляне на удостоверението му, като при търсене в регистъра се предоставя информация за издаденото удостоверение и неговия статус.

Информацията, която се събира от Доставчика за Титуляря/Създателя на печат/ Упълномощен представител и Абонат и не се включва в квалифицираните удостоверения и в информацията за техния статус и съставлява лични данни по смисъла на Закона за защита на личните данни и Регламент (ЕС) 2016/679 (GDPR) се събира само доколкото е необходима за нуждите на издаване и поддържане на квалифицираните удостоверения или ползване на друга удостоверителна услуга и не може да бъде ползвана за други цели или предоставяна на трети лица, без изричното съгласие на предоставилите я лица или ако това е позволено със закон.

Доставчикът предварително информира Титуляря/Създателя на печат/Упълномощен представител и Абонат на квалифицираните удостоверителни услуги за видовете информация, която събира за тях, начина на нейното предоставяне и съхранение и достъпа до нея на трети лица.

С подписване на Договора за квалифицирани удостоверителни услуги и приемането на разпоредбите на Практиката при предоставяне на квалифицирани удостоверителни услуги и на удостоверителните политики, Титуляря /Създателя на печат се съгласява личните му данни, които го идентифицират да бъдат включени в квалифицирано удостоверение и могат да бъдат достъпни за всички заинтересовани лица от Публичния регистъра на удостоверенията. Титулярят Създателят на печат може да ограничи достъпа до неговия сертификат, публикуван в Регистъра на издадените удостоверения.

9.5. Права върху интелектуалната собственост

Доставчикът притежава и си запазва всички права на интелектуална собственост върху бази данни, интернет страници, квалифицираните удостоверения, издадени от Доставчика, както и всякакви други документи и информация, произхождащи от Доставчика и включени в документния регистър на Доставчика.

Доставчикът разрешава удостоверенията, издадени от него и без

ограничение на достъпа до тях от Титуляря, да бъдат размножавани и разпространявани, при условие че те са репродуцирани и разпространени изцяло.

Всички права върху търговски имена, марки и запазени знаци се запазват от собствениците на тези права. Доставчикът използва обекти на такива права само за целите на предоставяне на квалифицирани удостоверителни услуги.

Частните и публичните ключове, както и средствата за достъп до тях (ПИН кодове, пароли и др.) са собственост на Титулярите им, които ги използват и съхраняват по правилен начин.

Двойките ключове, както и секретните части на частните ключове на Доставчика са собственост на Доставчика.

9.6. Задължения, отговорност и гаранции

Задълженията, отговорностите и гаранциите на Доставчика, Регистриращите органи, Титулярите, Създателите на печат, Абонатите на квалифицирани удостоверителни услуги и Доверяващите се страни са уредени в Регламент (ЕС) № 910/2014, в националното законодателство, в Практиката при предоставяне на квалифицирани удостоверителни услуги, в Удостоверителните политиките на Доставчика и в Договора за квалифицирани удостоверителни услуги.

9.6.1. Задължения, отговорност и гаранции на Доставчика

Доставчикът гарантира, че спазва всички разпоредби на Регламент (ЕС) № 910/2014, националното законодателство и настоящата Практиката при предоставяне на квалифицирани удостоверителни услуги, изпълнява стриктно заложените процедури и съблюдава политиките, установени в Удостоверителните политики за различните типове квалифицирани удостоверения при тяхното издаване и управление.

При издаване на квалифицираните удостоверения Доставчикът гарантира точността и актуалността на информацията, включена в съдържанието на удостоверението към момента на извършване на проверката ѝ и съобразно политиката на издаване на удостоверението.

Доставчикът отговаря пред Титуляря/ Създателя на печат и пред всички трети лица за вредите, причинени от:

- от неизпълнение на задълженията на Доставчика, съгласно Регламент (ЕС) № 910/2014 и националното право, регламентиращи издаването, управлението и съдържанието на квалифицираното удостоверение;
- от неверни или липсващи данни в квалифицираното удостоверение към момента на издаването му;
- това, че по време на издаването на квалифицираното удостоверение лицето, посочено като Титуляр/Създател, не е разполагало с частния ключ, съответстващ на публичния ключ, включен в издадено от Доставчика удостоверение;
- от алгоритмичното несъответствие между частния ключ и публичния ключ, вписван в квалифицираното удостоверение;
- пропуски в установяване на самоличност и или идентичността на Титуляря/ Създателя на печат.

9.6.2. Гаранции и отговорност на Регистриращия орган

Регистриращите органи са длъжни да изпълняват своите функции и задължения в съответствие с настоящата Практиката при предоставяне на квалифицирани удостоверителни услуги, изпълнява стриктно заложените процедури и съблюдава политиките, установени в Удостоверителните политики за различните типове квалифицирани удостоверения при тяхното издаване и управление и вътрешни документи на Доставчика.

Регистриращия орган се задължава да осигури защита на личните данни в съответствие със Закона за защита на личните данни, Регламент (ЕС) 2016/679 (GDPR) и относимото законодателство, да осигури защита на частните ключове на операторите и употребата им само за изпълнение на регистрационните дейности, за които са оторизирани.

9.6.3. Отговорност на Титуляря/Създателя на печат към трети лица

Титуляря/Създателя на печат отговаря спрямо третите добросъвестни лица:

- когато при създаването на двойката публичен и частен ключ е използвал алгоритъм и устройства за създаване на електронен подпис/печат, който не отговаря на изискванията на Регламент (ЕС) 910/2014;
- не изпълнява точно изискванията за сигурност, определени от Доставчика;
- не поиска от Доставчика спиране или прекратяване действието на удостоверението, когато е узнал, че частният ключ е

компрометиран, бил използван неправомерно или съществува опасност от неправомерното му използване;

- за неверни изявления, направени пред Регистриращия орган и Доставчика и имащи отношение към съдържанието или към издаването на удостоверението.

Титулярят/Създателя на печат, който е приел удостоверението при неговото издаване, отговаря спрямо третите добросъвестни лица и Доставчика, ако не е бил овластен да поиска издаването на удостоверението.

Титулярят/ Създателя на печат, отговаря спрямо Доставчика на квалифицирани удостоверителни услуги, ако е предоставил неверни данни, съответно е премълчал данни, имащи отношение към съдържанието или към издаването на удостоверението, и когато не е държал частния ключ, съответстващ на посочения в удостоверението публичен ключ.

Във всички случаи на неизпълнение на задълженията от страна на Титуляря, съответно Създателя на печат, произтичащи от Практиката за предоставяне на квалифицирани удостоверителни услуги, Доставчикът ще ангажира отговорността на Титуляря, съответно Създателя на печат за вреди.

9.6.4. Дължима грижа на Доверяващите се страни

Лицата, които се доверяват на квалифицираните удостоверителните услуги на Доставчика, следва да полагат дължимата грижа, като:

- имат технически умения да ползват квалифицирани удостоверения;
- информирани са за условията, при които трябва да се доверяват на квалифицираните удостоверения, съобразно политиките, при които са издадени и процедурите за извършваните проверки на информацията от Доставчика, описани подробно в настоящия документ;
- валидират издадени от Доставчика квалифицирани удостоверения посредством публикуваните данни за статуса на удостоверенията от Доставчика – Списъка на спрените и прекратени удостоверения;
- да използват механизъм за сигурна проверка на електронен подпис/ електронен печат, който гарантира:
- проверка на публичния ключ, проверка на частния ключ, проверка на съдържанието на подписания електронен документ; проверка на автентичността и валидността на квалифицираното удостоверение към момента на подписване, правилно представяне

на резултатите от проверката и възможност да бъдат установени всякакви промени;

- се доверяват на издадени от Доставчика квалифицирани удостоверения само ако резултатът от направените проверки за валидност е коректен и актуален.

Доверяващите се страни са длъжни да извършват проверките на валидността, спирането или прекратяването на действието на квалифицирано удостоверение посредством актуална информация за неговия статус и да вземат под внимание и да съобразяват действията си с всички ограничения на ползването на удостоверението, включени в самото удостоверение.

9.7. Отказ от отговорност

Доставчикът не отговаря в случаите, когато настъпилите вреди са следствие от небрежност, отсъствие на положена грижа или основни познания във връзка с работата с удостоверения за квалифицирани електронни подписи от страна на Титулярите, Създателите на печати или Доверяващите се страни.

Доставчикът не носи отговорност за вреди, настъпили поради несвоевременно прекратяване и спиране на удостоверения и проверка на статуса на удостоверения поради причини, които са извън неговия контрол.

Доставчикът не носи отговорност при използване на удостоверение извън пределите на предназначението и ограниченията за ползване, включени в него.

Доставчикът не носи отговорност за нарушаване на права на трети лица по отношение на техни търговски марки, търговски наименования или други имуществени или неимуществени права, когато информация, съдържаща се в издадени удостоверения, е довела до такива нарушения.

Доставчикът не отговоря за преки или косвени, предвидими или непредвидими вреди, настъпили вследствие от използване или доверяване на спрени, прекратени или с изтекъл срок на валидност удостоверения.

Доставчикът не отговаря за начина на ползване и за точността, автентичността и пълнотата на информацията, която е включена в тестови, безплатни или демонстрационни удостоверения.

Доставчикът не отговаря за сигурността, целостта и използването на софтуерните продукти и хардуерни устройства, използвани от Титуляри,

Създатели на печати или Доверяващи се страни.

9.8. Ограничение на отговорността на Доставчика

Максималния лимит на обезщетение в рамките на който Доставчикът отговаря за претърпени вреди при ползването на издадено от него квалифицирано удостоверение е в размер на максималния лимит определен съгласно националното законодателство.

9.9. Компенсации за Доставчика

Във всички случаи на неизпълнение на задълженията от страна на Титуляря, съответно Създателя на печат, произтичащи от Практиката за предоставяне на квалифицирани удостоверителни услуги и/или от Договора за квалифицирани удостоверителни услуги, Доставчикът ще ангажира отговорността на Титуляря, съответно Създателя за вреди.

9.10.Срок и прекратяване

9.10.1. Срок

Практиката при предоставяне на квалифицирани удостоверителни услуги влиза в сила от момента на нейното одобряване от Съвета на директорите на Инфонотари ЕАД и публикуването ѝ на адрес: http://repository.infonotary.com.

Практиката е валидна до нейната промяна или публикуване в Документния регистър и в интернет портала на Доставчика на информация за невалидността ѝ.

Срока на Договор за квалифицирани удостоверителни услуги е в зависимост от срока на валидност на издадените по него удостоверения или друг уговорен между страните срок.

9.10.2. Прекратяване и недействителност

Действието на Практиката при предоставяне на квалифицирани удостоверителни услуги се прекратява с прекратяване на дейността на Доставчика.

В случай, че някоя от клаузите на настоящата Практиката при предоставяне на квалифицирани удостоверителни услуги се окаже недействителна, това няма да влече други клаузи или части от Практиката или да доведе до недействителност на целия договор с Абонат. Недействителната клауза ще бъде заместена от повелителните норми на

закона.

Договорът за квалифицирани удостоверителни услуги се прекратява с прекратяване на действието на всички издадени въз основа на него квалифицирани удостоверения или при наличието на други основания за прекратяване, посочени в Практиката при предоставяне на квалифицирани удостоверителни услуги.

9.10.3. Ефект от прекратяването

След прекратяване на действието на Практиката при предоставяне на квалифицирани удостоверителни услуги за потребителя остават в сила разпоредбите за задълженията на Доставчика за поддържане на архив на документите и удостоверенията в обема и за периода, описани в Практиката.

9.11. Индивидуално уведомяване и комуникация между участниците

Всички заинтересовани страни могат да отправят съобщения до Доставчика във връзка с разпоредбите на Практиката при предоставяне на квалифицирани удостоверителни услуги и договорите посредством подписани електронни съобщения с квалифициран електронен подпис, писма с обратна разписка или писма, доставени от куриер до Доставчика.

Индивидуално уведомяване на Доставчика може да бъде направено на адреса за електронна кореспонденция: legal@infonotary.com или на адрес: гр. София 1000, ул. "Иван Вазов" 16.

За контакт с Абонатите си Доставчикът използва подписани с квалифициран електронен подпис/подпечатани с квалифициран електронен печат електронни писма, електронни писма, писма, доставени от куриер, писма с обратна разписка.

9.12. Промени в Практиката при предоставяне на квалифицирани удостоверителни услуги

Практиката при предоставяне на квалифицирани удостоверителни услуги може да бъде променяна по всяко време, като всяка промяна в нея се отразява след одобрение от Съвета на директорите на Инфонотари ЕАД и е публично достъпна от всички заинтересовани лица на адрес: https://www.infonotary.com и http://repository.infonotary.com.

Всяко лице може да отправя предложения за промени (структурни и съдържателни) и бележки за забелязани грешки на посочените в

настоящия документ електронни и пощенски адреси за контакти с Доставчика.

9.13.Решаване на спорове и подсъдност

Всички спорове, възникнали между страните във връзка с Договора за квалифицирани удостоверителни услуги, се уреждат по споразумение между страните, чрез разбирателство и дух на добра воля, а ако такова не бъде постигнато, се решават от компетентния български съд.

Всички жалби или претенции от Абонатите трябва да бъдат отправени към Доставчика в писмен вид и изпратени на адрес: гр. София 1000, ул. „Иван Вазов" №16 или електронно подписани на електронен адрес: legal@infonotary.com.

Жалбите и претенциите ще бъдат разглеждани своевременно и жалбоподателят следва да получи отговор в рамките на 14 дни от получаване на жалбата от Доставчика.

9.14.Приложимо право

За всички въпроси, неуредени в настоящата Практиката при предоставяне на квалифицирани удостоверителни услуги, се прилагат разпоредбите на националното право.

9.15.Съответствие с приложимото право

Настоящата Практиката при предоставяне на квалифицирани удостоверителни услуги е разработен в съответствие с изискванията на Регламент (ЕС) 910/2014 и националното законодателство.

9.16.Други разпоредби

Настоящия документ не съдържа други разпоредби.