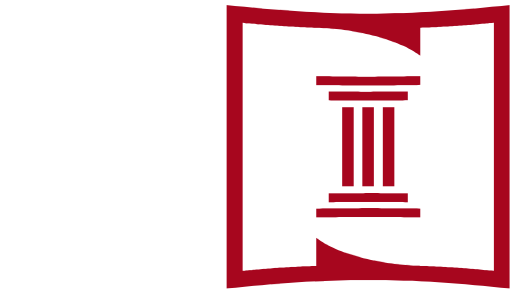

InfoNotary

ПОЛИТИКА ЗА

ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ ЗА УСЪВЪРШЕНСТВАН ЕЛЕКТРОНЕН ПОДПИС

НА

КВАЛИФИЦИРАНИЯ ДОСТАВЧИК НА УДОСТОВЕРИТЕЛНИ УСЛУГИ

ИНФОНОТАРИ ЕАД

ВЕРСИЯ 1.0

В сила от 09.07.2019 г.

СЪДЪРЖАНИЕ

1. ВЪВЕДЕНИЕ 4

1.1. ОСНОВНИ ПОЛОЖЕНИЯ 5
1.2. ИМЕНУВАНЕ И ИДЕНТИФИКАЦИЯ НА ДОКУМЕНТА 5
1.3. УЧАСТНИЦИ В УДОСТОВЕРИТЕЛНАТА ИНФРАСТРУКТУРА 7
1.4. УПОТРЕБА НА УДОСТОВЕРЕНИЯТА 9
1.5. Управление на удостоверителната политика на Доставчика 12
1.6. ТЕРМИНИ И СЪКРАЩЕНИЯ 13

2. ЗАДЪЛЖЕНИЯ ЗА ПУБЛИКУВАНЕ И ПОДДЪРЖАНЕ НА РЕГИСТРИ 17

2.1. Регистри 17
2.1. Публикуване на информация за удостоверенията 17
2.1. Честота на публикациите 18
2.1. Достъп до регистъра на удостоверенията 18

3. ИДЕНТИФИКАЦИЯ И АВТЕНТИФИКАЦИЯ 19

3.1. Първоначална идентификация и потвърждаване на самоличността 19
3.2. Идентификация и автентификация при заявка за прекратяване на удостоверение 22
3.3. Идентификация и автентификация при заявка за спиране на удостоверение 23

4. ОПЕРАТИВНИ УСЛОВИЯ 24

4.1. Искане за издаване на удостоверение 24
4.2. Процедура по заявяване на Удостоверение 25
4.3. Издаване на удостоверение 27
4.4. Тайна на данните при квалифицираните удостоверителни услуги и употреба на удостоверенията 28
4.5. Подновяване на Удостоверението 28
4.6. Прекратяване на удостоверение 31
4.7. Спиране на удостоверение 34

5. КОНТРОЛ НА ОБОРУДВАНЕТО,ПРОЦЕДУРИТЕ И УПРАВЛЕНИЕТО 36

5.1. Физически контрол 36
5.2. Процедурен контрол 38
5.3. Контрол на персонала, квалификация и обучение 39
5.4. Процедури по изготвяне и поддържане на журнал на данни от проверки 40
5.5. Архив 41
5.6. Компрометиране на ключове и възстановяване след бедствия и непредвидени случаи 43
5.7. Процедури по прекратяване дейността на Доставчика 44

6. КОНТРОЛ НА ТЕХНИЧЕСКАТА СИГУРНОСТ 46

6.1. Генериране и инсталация на двойка ключове 46
6.2. Защита на Частния ключ и технически контрол на криптографския модул 49
6.3. Други аспекти от управлението на двойката ключове 52
6.4. Данни за активиране 53
6.5. Контрол на компютърната сигурност 53
6.6. Техническият контрол на жизнен цикъл 54
6.7. Контрол на сигурността на мрежата 54

7. ПРОФИЛИ НА УДОСТОВЕРЕНИЯТА 55

7.1. Профил на базовото удостоверение InfoNotary TSP Root 55

7.2. Профил на оперативното удостоверение InfoNotary Qualified Personal Sign CA 57
7.3. Профил на квалифицираното удостоверение за електронен подпис на физическо лице InfoNotary Qualified Natural Person Signature CP 59
7.4. Профил на квалифицираното удостоверение за електронен подпис на физическо лице с делегирани правомощия InfoNotary Qualified Delegated Signature CP 63

8. ПРОВЕРКА И КОНТРОЛ НА ДЕЙНОСТТА 67

8.1. Обхват на проверката 67
8.2. Предприемане на действия за отстраняване на недостатъците 68

9. ДРУГИ БИЗНЕС И ПРАВНИ УСЛОВИЯ 69

9.1. Цени и такси 69
9.2. Финансови отговорности 70
9.3. Конфиденциалност на информацията 72
9.4. Поверителност на личните данни 73
9.5. Права върху интелектуалната собственост 74
9.6. Задължения, отговорност и гаранции 75
9.7. Отказ от отговорност 78
9.8. Ограничение на отговорността на Доставчика 78
9.9. Компенсации за Доставчика 78

1. ВЪВЕДЕНИЕ

Настоящия документ ПОЛИТИКА ЗА ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ ЗА УСЪВЪРШЕНСТВАН ЕЛЕКТРОНЕН ПОДПИС 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) и приложимото законодателство на Република България и се позовава на целите или на част от следните общоприети международни стандарти и спецификации:

- EN 319 401 v2.1.1 General Policy Requirements for Trust Service Providers;
- EN 319 411 Policy and security requirements for Trust Service Providers issuing certificates
- 319 411-1 v1.1.1: General requirements;
- 319 411-2 v2.1.1: Requirements for trust service providers issuing EU qualified certificates;
- 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;
- 319 412-5 v2.1.1: QCStatements;
- RFC 3647: Internet X.509 Public Key Infrastructure – Certificate Policies and Certification Practices Framework;
- RFC 3739: Internet X.509 Public Key Infrastructure – Qualified Certificates Profile;
- RFC 3279: Algorithms and Identifiers for Internet X.509 Public Key Infrastructure Certificate and CRL Profile.

Основната цел на документа **Политика за предоставяне на квалифицирано удостоверение за усъвършенстван електронен подпис**, наричан още (Политиката), е чрез подробно описание на правилата и политиките, които ИНФОНОТАРИ ЕАД е въвела и съблюдава при издаване и управление на квалифицирани удостоверения за **усъвършенстван електронен подпис**, 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.

Политиката 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.

Политиката може да бъде променяна при необходимост, като всяка промяна в нея 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 националния Надзорния орган при предвидените в Регламент № (ЕС) 910/2014 условия и в съответствие със националното право.

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

При осъществяване на дейностите по издаване и управление на квалифицирани удостоверения, 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 „Политика за предоставяне на квалифицирани удостоверения за усъвършенстван електронен подпис на ИНФОНОТАРИ ЕАД" (Политиката), се именува "InfoNotary CP-QAESign" и се идентифицира посредством следите идентификатори на обект в издаваните удостоверения:

Policy name	Identifier (OID)
InfoNotary Qualified Certificate for Natural Person AESignature	1.3.6.1.4.1.22144.3.6.1
InfoNotary Qualified Certificate for Delegated AESignature	1.3.6.1.4.1.22144.3.6.2

Политиката включва:

- описание на условията, които Доставчикът спазва и следва при издаване на квалифицирани удостоверения за усъвършенстван електронен подпис, 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 за усъвършенстван електронен подпис, първоначалната идентификация и автентификация на Титулярите на удостоверения, условията и необходимите нива на сигурност при създаване на електронния подпис и съхраняване на частния ключ от Титулярите.
- определя приложимостта и степента на доверие във включената в квалифицирани удостоверения за усъвършенстван електронен подпис информация.

Квалифицираните удостоверенията които се издават по настоящата Политиката включват следните идентификатори на политики, в съответствие с ETSI EN 319-411-2:

Policy name	Policy ID	Identifier (OID)
InfoNotary Qualified Certificate for Natural Person AESignature	QCP-n	0.4.0.194112.1.0
InfoNotary Qualified Certificate Delegated AESignature	QCP-n	0.4.0.194112.1.0

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 и електронен печат, 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 информация, ограничения в приложението и отговорности.

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

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:

- 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 други данни, в зависимост от типа на удостоверенията и в съответствие с удостоверителните политики на Доставчика;
- проверка за държането на двойка ключове от асиметрична криптосистема от Титуляря;
- иницииране на издаване на удостоверението след положителна проверка и одобряване на искането, като уведомяват Удостоверяващия орган;
- предаване на издаденото удостоверение на Титуляря.

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

1.3.3. Абонати

"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.

1.3.1. Доверяващи се лица

"Доверяващи се лица" са физически или юридически лица, които разчитат на електронна идентификация или удостоверителна услуга, които са адресати на подписани електронни изявления, Титулярите на които имат издадени удостоверения за електронен подпис от Доставчика. Доверяващите се страни следва да имат умения да ползват удостоверения за електронен подпис/печат и да 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.

1.3.2. Титуляр

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

Титуляря държи частния ключ за електронен подпис, съответстващ на публичния ключ, вписан в удостоверението и създава електронни подписи. Титуляря е също и собственик на средата за създаване на усъвършенстван електронен подпис, което отговаря на изискванията, предвидени в Регламент 910/2014 и използвано от него за генериране и

съхранение на криптографските ключове, квалифицирани удостоверения за усъвършенстван електронен подпис и данни за създаване на електронни подписи.

1.3.3. Представители

„Представител" е надлежно овластено от Титуляря физическо лице, което извършва действия от негово име по издаване и управление на удостоверения за електронен подпис пред Доставчика. Представителят е лице, различно от Титуляря, не е вписано в удостоверението, и не може да извършва електронни изявления, подписани с електронния подпис на Титуляря и от името на Титуляря.

1.4. УПОТРЕБА НА УДОСТОВЕРЕНИЯТА

1.4.1. Удостоверения на удостоверяващия орган

1.4.1.1. Базово удостоверение (Root)

Базовото удостоверение за публичния ключ на Удостоверяващия орган на Доставчика, именуващо се като: **InfoNotary TSP Root** е самоиздадено и самоподписано удостоверение за усъвършенстван 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.

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.

1.4.2. 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 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).

1.4.3. Квалифицирани удостоверения за усъвършенстван електронен подпис на физическо лице

ИНФОНОТАРИ ЕАД издава квалифицирани удостоверения за усъвършенстван електронен подпис на физически лица в пълно съответствие с разпоредбите и изискванията на Регламент (ЕС) 910/2014.

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
Квалифицирано удостоверение за 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.

1.4.1. 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.

1.4.2. Ограничения на удостоверителното действие

Квалифицираните удостоверения за усъвършенстван електронен подпис, които се издават от Доставчика, въз основа на настоящата Политика могат да бъдат с ограничено действие по отношение на целите и/или стойността на сделките – за електронен подпис на физическо лице и електронен подпис на физическо лице, с делегирани правомощия от юридическо лице.

За квалифицираните удостоверения за усъвършенстван електронен подпис ограничението по отношение стойността на сделките се определя от Титуляря и се вписва от Доставчика в удостоверението въз основа на Искането за издаване на удостоверението. Ограниченията се вписват в удостоверението в допълнителното разширение 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 и на стойността на сделките и ще доведе до анулиране

на гаранциите, които "ИНФОНОТАРИ" ЕАД дава на Титуляря и на Доверяващите се страни.

1.5. Управление на удостоверителната политика на Доставчика

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

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

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

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

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

1.6. ТЕРМИНИ И СЪКРАЩЕНИЯ

Валидация	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.
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.
ПИН	Персонален Идентификационен Номер
Електронен документ	Всяко съдържание, съхранявано в електронна форма, по-специално текстови или звуков, визуален или аудио-визуален запис.
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.
Усъвършенстван електронен подпис	Усъвършенстван електронен подпис, който е създаден от устройство за създаване на усъвършенстван 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.

КРС	Комисия за регулиране на съобщенията
Практика	Практика при предоставяне на квалифицирани удостоверителни услуги **InfoNotary Qualified CPS**
Политика	Политика при предоставяне на квалифицирано удостоверение за усъвършенстван електронен подпис.
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
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 усъвършенстван електронен подпис	Устройство за създаване на електронен подпис, което отговаря на изискванията, предвидени в Регламент 910/2014
Устройство за създаване на електронен подпис	Конфигуриран софтуер или хардуер, който се използва за създаването на електронен подпис

Усъвършенстван електронен подпис	Електронен подпис, който отговаря на следните изисквания: свързан е по уникален начин с титуляря на подписа; може да идентифицира титуляря на подписа; създаден е чрез данни за създаване на електронен подпис, които титулярят на електронния подпис може да използва с висока степен на доверие и единствено под свой контрол; и е свързан с данните, които са подписани с него, по начин, позволяващ да бъде открита всяка последваща промяна в тях.

СЪКРАЩЕНИЯ

ASN.1	Abstract Syntax Notation One – Абстрактен език за описание на обекти в удостоверенията
CA	Certification Authority – Удостоверяващ орган
CC	Common Criteria – Общи критерии
CEN	European Committee for Standardization - Европейски стандартизационен комитет
CENELEC	European Committee for Electronic Standardization - Европейски комитет за електротехническа стандартизация
CP	Certificate Policy – Политика за предоставяне на удостоверителни услуги
CPS	Certification Practice Statement – Практика при предоставяне на удостоверителни услуги
CRL	Certificate Revocation List – Списък на спрените и прекратени удостоверения
DN	Distinguished Name – Уникално име
ETSI	European Telecommunications Standards Institute - Европейски институт за телекомуникационни стандарти
EU	European Union - Европейски съюз

FIPS	Federal Information Processing Standard – Федерален стандарт за обработка на информация
IEC	International Electrotechnical Commission - Международна електротехническа комисия
ISO	International Standardization Organization - Международна организация за стандартизация
LDAP	Lightweight Directory Access Protocol – Протокол за опростен достъп до регистър
OID	Object Identifier – Идентификатор на обект
OCSP	On-line Certificate Status Protocol – Протокол за проверка на статуса на удостоверения в реално време
PKCS	Public Key Cryptography Standards – Криптографски стандарт за пренос на публичен ключ
PKI	Public Key Infrastructure – Инфраструктура на публичния ключ
RA	Registration Authority – Регистриращ орган
RSA	Rivest-Shamir-Adelman – Криптографски алгоритъм за създаване на подпис
SSCD	Secure Signature Creation Device – Устройство за сигурно създаване на подпис
QSCD	Qualified Signature Creation Device – Устройство за създаване на Квалифициран подпис
SHA	Secure Hash Algorithm – Хеш-алгоритъм за извличане на хеш-идентификатор
SSL	Secure Socket Layer – Сигурен канал за предаване на данни
URL	Uniform Resource Locator – Единен ресурсен локатор

2. ЗАДЪЛЖЕНИЯ ЗА ПУБЛИКУВАНЕ И ПОДДЪРЖАНЕ НА РЕГИСТРИ

Доставчикът публикува информация за издадените квалифицирани удостоверения за усъвършенстван електронен подпис, 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 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.

2.1.1. Регистър на удостоверенията

Доставчикът води електронен регистър на удостоверения, в който публикува всички издадени от него квалифицирани удостоверения за усъвършенстван електронен подпис. 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 усъвършенстван електронен подпис.

2.2. Публикуване на информация за удостоверенията

Издадените квалифицирани удостоверения за усъвършенстван електронен подпис се публикуват в регистъра на удостоверенията своевременно след тяхното подписване от съответния удостоверяващия

орган на Доставчика - **Advanced Personal Sign CA.** 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

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 заинтересувано 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, Доставчикът ограничава достъпа за четене и изтегляне на квалифицираното му удостоверението за усъвършенстван електронен подпис, като при търсене в регистъра се предоставя информация за издаденото удостоверение и неговия статус.

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 квалифицираните удостоверения за усъвършенстван електронен подпис.

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 Практиката при предоставяне на квалифицирани удостоверителни услуги.

3.1. Първоначална идентификация и потвърждаване на самоличността

За първоначална идентификация и автентификация на Титуляря 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 или от физическо лице, овластен представител на юридическото лице;
- проверка и потвърждаване на самоличността и идентичността на Физическото лице – Титуляр и Юридическото лице.

3.1.1. 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. При заявка за издаване на удостоверение за усъвършенстван 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 от Титуляря преди иницииране на издаването на удостоверение към Удостоверяващия орган на Доставчика, независимо дали генерирането на двойката ключове, обвързана със заявката, е извършено от Титуляря самостоятелно или двойката ключове е генерирана от Доставчика, респективно Регистриращия орган. 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 искането 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 политика 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.

3.1.2. Установяване на идентичността на Юридическо лице

За установяване и потвърждаване на идентичността на юридическо лице, овластило физическо лице да бъде Титуляр в квалифицирано удостоверение и да направи 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 за усъвършенстван електронен подпис на Титуляр, овластен от юридическо лице, проверките и потвърждаването на информацията се извършват от Регистриращия орган съобразно правилата за и процедурите на Доставчика и в пълно съответствие с Практиката при предоставяне на квалифицирани удостоверителни услуги 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.

Законния представител на юридическото лице, респективно упълномощен представител на юридическото лице 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.

3.1.3. Непотвърдена информация

В някои случаи Доставчикът може да включи в издаваните удостоверения и непотвърдена информация за Титуляря, 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.

3.2. 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 Практиката при предоставяне на квалифицирани удостоверителни услуги. Регистриращият орган отправя искане за прекратяване до Доставчика след получаване на искане за прекратяване от Титуляря и извършването на

действия по проверка на идентичността и самоличността на заявителите и потвърждаването им.

Титулярят или упълномощения представител на Титуляря, 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 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.

3.3. 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, описан в Практиката при предоставяне на квалифицирани удостоверителни услуги. 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;
- 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, описан в Практиката при предоставяне на квалифицирани удостоверителни услуги и след иницииране за възобновяване от Регистриращия орган.

Регистриращият орган извършва идентификация и автентификация

на Титуляря, когато той е представил лично или чрез упълномощен представител подписано искане за възобновяване на удостоверение.

Титуляря 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 пред Доставчика за издаване и управление на удостоверения;
- подписано Искане за възобновяване на удостоверение, съдържащо декларация, че Титулярят е узнал причината за спирането и искането за възобновяване е направено вследствие на узнаването.

4. ОПЕРАТИВНИ УСЛОВИЯ

Титулярите на квалифицирани удостоверения за усъвършенстван електронен подпис, са длъжни да уведомяват Доставчика 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 и предоставят на Доставчика електронно заявка за издаване на удостоверение във формат PKCS#10;
- генерират двойка криптографски ключове и ползват частния ключ за подписване на заявката за издаване на удостоверение;

- 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 или от негов упълномощен 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;
- публичния ключ, кореспондиращ на частния ключ от двойката криптографски ключове, генерирани от Титуляря
- 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. Искането за издаване на удостоверение се подава лично от Заявителя в Регистриращ орган на Доставчик или с електронно заявление, ако Титулярят е регистрирани потребител и притежава валидни права за достъп до портала на Доставчика на адрес: https://www.infonotary.com и наличието на техническа възможност за това.

Титулярят носи пълната отговорност за предотвратяване на компрометиране, загуба, разкриване, модифициране или друго неоторизирано използване на частния ключ (средствата за създаване на усъвършенстван електронен подпис).

4.2. Процедура по заявяване на Удостоверение

Функциите по идентификация и автентификация на Заявителите на Искане за издаване на квалифицирано удостоверение за усъвършенстван електронен подпис се извършват от оторизиран Регистриращ орган на Доставчика. Съблюдавайки утвърдените от Доставчика процедури и съгласно Практиката при предоставяне на квалифицирани удостоверителни услуги, въз основа на полученото искане за издаване на удостоверение и представените документи и в личното присъствие на Заявителя – Титуляря или упълномощено от него лице, Регистриращият орган проверява и потвърждава пред Удостоверяващия орган:

- самоличността и идентичността на Титуляря или упълномощения от него Представител;
- представителната власт на Титуляря и упълномощения от Титуляря Представител;
- държането на частния ключ, кореспондиращ на публичния ключ включен в искането по времето на неговото създаване;
- допълнителната информация, заявена за включване в удостоверението, с изключение на непотвърдената информация;
- съгласието на Титуляря с условията на настоящия документ и подписването на Договор за квалифицирани удостоверителни услуги.

Преди потвърждаване на подадено искане за издаване на удостоверение Регистриращият орган на Доставчика извършва необходимите проверки по изискванията на Практиката при предоставяне на квалифицирани удостоверителни услуги:

- проверява и потвърждава самоличността или идентичността на Заявителя, Титуляря или представляващото го лице по предоставените от тях документи и проверка със законови средства в съответните публични регистри;
- проверява и потвърждава представителната власт на Титуляря и упълномощеното от Титуляря да го представлява лице;
- проверява коректността на получената или направената подписана електронна заявка (във формат PKCS#10) за издаване на удостоверение;
- предоставя на Титуляря информацията, която е потвърдена и ще бъде включена в издаденото удостоверение за приемане на съдържанието му;
- 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 и овластяването на Титуляря и представителната власт на Представителя.

Преди потвърждаване на подадено искане за издаване на удостоверение Регистриращият орган на Доставчика извършва необходимите проверки по изискванията на Практиката при предоставяне на квалифицирани удостоверителни услуги:

- искането за издаване изхожда от Титуляря или от надлежно овластено от него лице;
- информацията относно Титуляря, представена за включване в удостоверението, е вярна и пълна;

- частният ключ е технически годен да бъде използван за създаване на усъвършенстван електронен подпис и съответства на публичния ключ, така че чрез публичния ключ може да се удостовери, че определен електронен подпис е създаден с частния ключ, и
- частният ключ се държи от Титуляря.

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 и упълномощения Представител документи. Доставчикът контролира точността на включената в удостоверенията информация, предоставена от Титуляря, към момента на издаване на удостоверението.

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

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).

Доставчикът незабавно уведомява Титуляря за издаденото му квалифицирано удостоверение, посредством изпращане на електронно писмо до Титуляря. След издаване на удостоверението Доставчикът го доставя до Титуляря:

- чрез вписване на връзка за дънлоуд на удостоверението в изпратеното електронно писмо ;
- или посредством Регистриращия орган.

Доставчикът издава удостоверението в съответствие със съгласието на Титуляря. Приемане на съдържанието на квалифицираното удостоверение се извършва преди публикуването му в Регистъра на удостоверенията на Доставчика и се удостоверява с подписване на Протокол за приемане на удостоверение от Титуляря.

Доставчикът публикува своевременно издаденото квалифицирано удостоверение в базата данни на удостоверенията си.

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

4.4.1. Тайна на данните

Никой освен Титуляря на квалифицирано удостоверение за усъвършенстван електронен подпис няма право на достъп до данните за създаване на електронен подпис.

Титуляря 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).

Титулярят, 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.

4.4.2. 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 електронния подпис.

4.5. Подновяване на Удостоверението

4.5.1. Условия за подновяване на удостоверение

Квалифицираните удостоверения за усъвършенстван електронен

подпис, които Доставчикът издава, са с различен период на валидност. Периодът на валидност се вписва като реквизит в издаденото удостоверение. Подновяване на квалифицирано удостоверение за усъвършенстван електронен подпис, издадено от Доставчика, може да бъде извършено само 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.

Подновяване на удостоверението се заявява от Титуляря, вписан в действащото удостоверение, поне 10 (десет) дни преди изтичане периода на валидност на удостоверението.

4.5.2. Процедура по заявяване на подновяване

Искането за подновяване се прави чрез подаване на искане за подновяване на валидно удостоверение в Регистриращия орган или с подписано електронно заявление, ако Титулярят е регистрирани потребител и притежава валидни права за достъп до портала на адрес: https://www.infonotary.com и наличието на техническа възможност за това.

Електронното заявление е необходимо да бъде подписано от Титуляря с валидното квалифицирано удостоверение за усъвършенстван електронен подпис 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 подписва декларация, 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 Практиката при предоставяне на квалифицирани удостоверителни услуги.

След направените проверки и приемане на съдържанието на удостоверението от Титуляря, Регистриращият орган потвърждава искането за подновяване на удостоверение към Удостоверяващия орган на Доставчика и гарантира, че:

- искането за подновяване изхожда от Титуляря или от надлежно овластено от него лице;
- информацията относно Титуляря, включена в удостоверението е точна, вярна и актуална;
- частният ключ се държи от Титуляря;
- 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 документи (заверени копия и оригинали) заедно с искането за подновяване на удостоверение протокола за приемане на удостоверението.

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 документите.

Удостоверяващият орган на Доставчика издава новото удостоверение на база на получено 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).

Доставчикът незабавно уведомява Титуляря за издаденото им ново удостоверение, посредством изпращане на електронно писмо.

След издаване на удостоверението Доставчикът го доставя до Титуляря:

- чрез вписване на връзка за дънлоуд на удостоверението в изпратеното електронно писмо

- чрез Регистриращия орган.

Приемане на съдържанието на квалифицираното удостоверение се извършва преди публикуването му в Регистъра на удостоверенията на Доставчика и се удостоверява с подписване на Протокола за приемане на удостоверение от Титуляря.

Доставчикът публикува незабавно издаденото удостоверение в Регистъра на удостоверенията си.

4.6. 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.

4.6.1. 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 за обстоятелства относно валидността или надеждността на издаденото му удостоверение.

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

4.6.2. 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 до Доставчика;
- да се извърши проверка от Регистриращия орган на Доставчика за самоличността, идентичността и представителната власт на Титуляря.

Титулярят или упълномощеното надлежно от него лице подава искането за прекратяване на удостоверение лично в офис на Регистриращ орган на Доставчика с подписване на "Искане за прекратяване на удостоверение".

Идентификацията и автентификацията на заявителите, подали искане за прекратяване на удостоверение, се извършват от Регистриращ орган на Доставчика по реда, описан в Практиката при предоставяне на квалифицирани удостоверителни услуги

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 директно или посредством Регистриращия орган за извършените действия, както и с електронно писмо.

Прекратените от Доставчика удостоверения не подлежат на възобновяване.

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.

4.6.3. 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.

4.6.4. Честота на издаване на Списък с на спрените и 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.

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

Доставчикът предоставя услуга за проверка на статуса на издадените от него удостоверения в реално време посредством OCSP протокол. Доверяващите се страни могат да използват за проверка на статуса на удостоверение информацията, предоставена от автоматичната система, посредством OCSP протокол съобразно Практиката при предоставяне на квалифицирани удостоверителни услуги.

4.7. Спиране на удостоверение

4.7.1. 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 за обстоятелствата относно валидността или надеждността на издаденото им удостоверение. За периода на временно спиране на удостоверението то се счита за невалидно.

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

- по искане на Титуляря;
- 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.

4.7.2. 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 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.

Титулярят или упълномощено надлежно от него лице прави искането за спиране чрез:

- интернет портала 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.

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.

4.7.3. 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 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.

4.7.4. Процедура по възобновяване действието на спряно удостоверение

Когато възобновяването се извършва по искане на Титуляря, проверка на искането и идентификация на Титуляря се извършва от Регистриращ орган на Доставчика по реда, описан в Практиката при предоставяне на квалифицирани удостоверителни услуги. 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.

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.

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 в случаите, описани в Практиката при предоставяне на квалифицирани удостоверителни услуги.

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, пропускване 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 доверeност 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) 910/20124 и приложимото национално законодателство.

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;
- одитинг 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.

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.

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

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.

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.

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.

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

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.

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.

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

5.6. 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.

5.6.1. 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.

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. 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.

5.7. Процедури по прекратяване дейността на Доставчика

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 всички издадени от него удостоверения и предава цялата документация, свързана с дейността му, на Надзорния орган ведно с всички архиви, както и всички издадени удостоверения (валидни, прекратени и спрени).

Ако бъде отнет квалифицирания статут на Доставчика, информацията за това трябва да бъде предадена по електронен път или в писмена форма на притежателите на валидни квалифицирани удостоверения, на третите страни, доверяващи се на удостоверителни услуги и на субекти, които имат сключили 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, че квалифицираните удостоверения, издадени от Доставчика, вече не могат да се използват в съответствие с разпоредбите на приложимото законодателство.

6. КОНТРОЛ НА ТЕХНИЧЕСКАТА СИГУРНОСТ

6.1. Генериране и инсталация на двойка ключове

Доставчикът защитава собствените си частни ключове съгласно разпоредбите на настоящата политика. 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 Титуляря - с хардуер и софтуер под техен контрол,
- при Доставчика, съответно при оторизиран от него Регистриращ орган - с хардуер и софтуер, част от инфраструктурата на Доставчика.

Доставчикът може на базата на договорни отношения да предостави на Титуляря одобрени по реда на Регламент (ЕС) 910/2014 и националното законодателство устройства за създаване на усъвършенстван електронен подпис - 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 усъвършенствани електронни подписи и печати.

Титулярите могат да използват и други устройства за създаване на усъвършенстван електронен подпис, 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 на криптографски ключове за квалифицирани удостоверения, издавани от Доставчика, е задължително ползването на лицензиран софтуер на даден производител.

Потребителите на удостоверителните услуги на Доставчика генерират двойката си криптографски ключове - частен и публичен, за квалифицирани удостоверения за усъвършенстван електронен подпис самостоятелно, при Титуляря - с хардуер и софтуер под техен контрол, посредством устройство за създаване на усъвършенстван електронен подпис, което отговаря на изискванията за ниво на сигурност и разпоредбите на Регламент (ЕС) 910/2014 за усъвършенствани електронни подписи и печати.

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 или по-високо.

Осъществяването на документираната процедура по генериране и инсталиране на базовата (root) двойка ключове на Удостоверяващия орган на Доставчика се извършва от оторизиран за това служител на Доставчика и в присъствието на членовете 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 се 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;
- контрол на достъпа за управление и ползване на частните оперативни ключове на Удостоверяващия орган посредством отделни секретни данни, достъпни само за оторизирани лица.

6.1.1.2. Генериране на двойка ключове на Абонат

Титуляря генерира двойката ключове в сигурна среда за създаване на усъвършенстван електронен подпис, отговаряща на изискванията на Регламент (ЕС) № 910/2014. Контролът за достъп до частния ключ се защитава с ПИН или парола, които се ползват от Титуляра за създаване на усъвършенстван електронен подпис.

Титуляря носи пълна отговорност за сигурността и надежността на средата за създаване на усъвършенстван електронен подпис която ползва, както и за защитата на частния си ключ.

6.1.2. Доставка на Частния ключ

Когато Доставчикът по възлагане от Титуляря, съответно Създателя генерира двойката ключове, частният ключ от тази двойка се записва на устройство за създаване на електронен подпис/печат (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, съответно Създателя, заедно с правата за достъп (ПИН, АИН).

6.1.3. Доставка на Публичния ключ до издателя на Удостоверението

Тази процедура се изпълнява само от Титуляря, 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 може да предостави електронната заявка:

- лично в Регистриращия орган или
- по електронен път и на адрес https://www.infonotary.com.

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.

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 квалифицирано удостоверение за усъвършенстван електронен подпис частният ключ на Титуляря 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 усъвършенстван електронен подпис, устройството за създаване на усъвършенстван електронен подпис, в което се генерира и съхранява частния ключ на Титуляря да е с ниво на сигурност CC EAL 4+/FIPS 140-2 Level 3 или по-високо.

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 се използва само в устройство за създаване на усъвършенстван електронен подпис или в устройство с еквивалентно ниво на сигурност (съгласно изискванията на Регламент (ЕС) № 910/2014) и е достъпен посредством ПИН.

Доставчикът по никакъв начин не съхранява и не архивира частен ключ на Титуляр за създаване на електронен подпис.

6.2.3. Съхранение на Частните ключове

Частните ключове на Удостоверяващите органи на Доставчика се съхраняват Hardware Security Modul (HSM) 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 от 4 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 2 от 4.

Частният ключ на Титуляря се съхранява на използваното за генериране на ключа устройство за създаване на усъвършенстван електронен подпис съгласно изискванията на Регламент (ЕС) № 910/2014) и е достъпен посредством ПИН.

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, които са генерирани на устройство за създаване на усъвършенстван електронен подпис. При дефект, загуба или унищожаване на устройството за създаване на усъвършенстван електронен подпис, Доставчика прекратява удостоверение, което е издадено във връзка с ключове, генерирани посредством това устройство.

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 при ползване на споделените права за достъп до секретните данни.

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.

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 2 от 4 лица и всички действия се документират и пазят в архива на Доставчика. Частния ключ на Root CA се активиран 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 2 от 4 лица и всички действия се документират и пазят в архива на Доставчика.

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

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 при изтичане на периода на тяхната валидност 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 се унищожава чрез изтриване на контейнера на устройството за създаване на усъвършенстван електронен подпис или чрез физическо унищожаване на самото устройство.

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.

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, ползващ устройство за създаване на усъвършенстван електронен подпис за съхранение на частния си ключ е задължен да съхранява и пази от компрометиране персоналните данни за активиране на своето устройство за създаване на усъвършенстван електронен подпис - ПИН.

6.4.1. Генериране и инсталиране на данни за активиране

Данни за активиране се създават при първоначална инициализация на устройство за създаване на усъвършенстван електронен подпис лично от Титуляря.

6.4.2. Защита на данни за активиране

Титулярят е задължен да съхранява и пази от компрометиране кодовете за достъп до устройството за създаване на усъвършенстван електронен подпис.

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.

7. ПРОФИЛИ НА УДОСТОВЕРЕНИЯТА

7.1. Профил на базовото удостоверение InfoNotary TSP Root

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		

7.2. Профил на оперативното удостоверение InfoNotary Advanced Personal Sign CA

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		

7.3. Профил на квалифицираното удостоверение за усъвършенстван електронен подпис на физическо лице InfoNotary Qualified Certificate for Natural Person AESignature

InfoNotary Qualified Certificate for Natural Person AESignature			
Основни x509 атрибути:			
Атрибут			Стойност
Версия			3 (0x02)
Сериен номер			Уникален за регистъра на Доставчика; От 8 до 16-байтово число
Начало на периода на валидност			Дата и час на подписване
Край на периода на валидност			Дата и час на подписване + 1, 2 или 3 год.
Алгоритъм на електронния подпис			SHA256/RSA
Атрибути на Издателя:			
Атрибут			Стойност
Domain Component	Домейн компонент	DC	qualified-natural-aes-ca
Common Name	Име	CN	InfoNotary Advanced Personal Sign 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
Domain Component	Домейн компонент	DC	qualified-natural-aes-ca
Common Name	Име	CN	Пълно име

Given Name	Лично име	G	Собствено име по документ за самоличност (изписано на латиница)
Sur Name	Фамилия	Sn	Фамилно име по документ за самоличност (изписано на латиница)
Email	Електронен адрес	E	
Country Name	Държава	C	
Locality Name	Град	L	
Serial Number	Уникален идентификатор на физическото лице	2.5.4.5	PNOBG-XXXXXXXXX (ЕГН) PASBG-XXXXXXXXX (Номер на паспорт) IDCBG- XXXXXXXXX (Номер на лична карта) TINBG-XXXXXXXXX (ДДС идентификационен номер)
			PNOYY-XXXXXXXXX (National Personal Number) PASYY-XXXXXXXXX (Passport Number) IDCYY- XXXXXXXXX (National ID card Number) YY – Country code

Допълнителни атрибути на x509 разширения (x509v3 extensions):	
Атрибут	Стойност
Basic Constraints (Critical)	End entity
Key Usage (Critical)	Digital Signature, Non-Repudiation, Key Encipherment, Data Encipherment
Public Key	RSA 2048 bits
Authority Key Identifier	AuthorityKeyIdentifier
Subject Key Identifier	SubjectKeyIdentifier

Authority information Access	[1] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= https://repository.infonotary.com/qualified-natural-aes-ca.crt [2] Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL= http://ocsp.infonotary.com/qualified
CRL Distribution Point (Non Critical)	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.infonotary.com/crl/qualified-natural-aes-ca.crl
Certificate Policies (Non Critical)	[1]Certificate Policy: Policy Identifier=0.4.0.194112.1.0 [2]Certificate Policy: Policy Identifier=0.4.0.1456.1.2 [3]Certificate Policy: Policy Identifier=1.3.6.1.4.1.22144.3.6.1 [2.1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://repository.infonotary.com/cps/qualified-tsp.html UNotice: InfoNotary Qualified Certificate for Natural Person AESignature
Qualified Certificate Statement (Non Critical)	id-etsi-qcs-semanticsId-Natural (oid=0.4.0.194121.1.1) id-etsi-qcs-QcCompliance (oid=0.4.0.1862.1.1) id-etsi- qcs-QcLimitValue (oid=0.4.0.1862.1.2) id-etsi-qct-esign (oid=0.4.0.1862.1.6.1) id-etsi-qcs-QcPDS (oid=0.4.0.1862.1.5) PDSLocation=https://repository.infonotary.com/pds/pds_bg.pdf Language=bg PDSLocation=https://repository.infonotary.com/pds/pds_en.pdf Language=en
Extended Key Usage (Non Critical)	Email protection Client Authentication

7.4. Профил на квалифицираното удостоверение за усъвършенстван електронен подпис на физическо лице с делегирани правомощия
InfoNotary Qualified Certificate for Delegated AESignature CP

InfoNotary Qualified Certificate for Delegated AESignature			
Основни x509 атрибути:			
Атрибут			Стойност
Версия			3 (0x02)
Сериен номер			Уникален за регистъра на Доставчика; От 8 до 16-байтово число
Начало на периода на валидност			Дата и час на подписване
Край на периода на валидност			Дата и час на подписване + 1, 2 или 3 год.
Алгоритъм на електронния подпис			SHA256/RSA
Атрибути на Издателя:			
Атрибут			Стойност
Domain Component	Домейн компонент	DC	qualified-natural-aes-ca
Common Name	Име	CN	InfoNotary Advanced Personal Sign 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

Domain Component	Домейн компонент	DC	qualified-natural-aes-ca
Common Name	Име	CN	Пълно име
Given Name	Лично име	G	Собствено име по документ за самоличност (изписано на латиница)
Sur Name	Фамилия	Sn	Фамилно име по документ за самоличност (изписано на латиница)
Email	Електронен адрес	E	
Country Name	Държава	C	
Locality Name	Град	L	
Serial Number	Уникален идентификатор на физическото лице	2.5.4.5	PNOBG-XXXXXXXXXX (ЕГН) PASBG-XXXXXXXXXX (Номер на паспорт) IDCBG-XXXXXXXXXX (Номер на лична карта) TINBG-XXXXXXXXXX (ДДС идентификационен номер)
			PNOYY-XXXXXXXXXX (National Personal Number) PASYY-XXXXXXXXXX (Passport Number) IDCYY-XXXXXXXXXX (National ID card Number) YY – Country code
Organization	Име на юридическото лице	O	
Organizational Unit Name	Организационно звено	OU	
Organization Identifier	Уникален идентификатор на юридическото лице	2.5.4.97	NTRYY-XXXXXXXXXX (Национален идентификационен код) VATYY-XXXXXXXXXX (Данъчен номер) TINBG-XXXXXXXXXX (ДДС идентификационен номер) YY – код на държавата

Допълнителни атрибути на x509 разширения (x509v3 extensions):	
Атрибут	Стойност
Basic Constraints (Critical)	End entity
Key Usage (Critical)	Digital Signature, Non-Repudiation, Key Encipherment, Data Encipherment
Public Key	RSA 2048 bits
Authority Key Identifier	AuthorityKeyIdentifier
Subject Key Identifier	SubjectKeyIdentifier
Authority information Access	[1] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= https://repository.infonotary.com/qualified-natural-aes-ca.crt [2] Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL= http://ocsp.infonotary.com/qualified
CRL Distribution Point (Non Critical)	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.infonotary.com/crl/qualified-natural-aes-ca.crl
Certificate Policies (Non Critical)	[1]Certificate Policy: Policy Identifier=0.4.0.194112.1.0 [2]Certificate Policy: Policy Identifier=0.4.0.1456.1.2 [3]Certificate Policy: Policy Identifier=1.3.6.1.4.1.22144.3.6.2 [3.1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://repository.infonotary.com/cps/qualified-tsp.html UNotice: InfoNotary Qualified Certificate for Delegated AESignature

Qualified Certificate Statement (Non Critical)	id-etsi-qcs-semanticsId-Natural (oid=0.4.0.194121.1.1) id-etsi-qcs-QcCompliance (oid=0.4.0.1862.1.1) id-etsi-qcs-QcLimitValue (oid=0.4.0.1862.1.2) id-etsi-qct-esign (oid=0.4.0.1862.1.6.1) id-etsi-qcs-QcPDS (oid=0.4.0.1862.1.5) PDSLocation=https://repository.infonotary.com/pds/pds_bg.pdf Language=bg PDSLocation=https://repository.infonotary.com/pds/pds_en.pdf Language=en
Extended Key Usage (Non Critical)	Email protection Client Authentication

8. ПРОВЕРКА И КОНТРОЛ НА ДЕЙНОСТТА

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 органи, 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.

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.

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.

8.1. 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 й 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.

8.2. 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.

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 квалифицираното 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 на квалифицирано удостоверение в 3-дневен срок от публикуването му в Регистъра 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, 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.

9.2.1. 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. 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 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 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 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.

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

- всяка информация, за Титуляря и Абоната, извън публикуваната в удостоверението;
- причината за спиране или прекратяване действието на удостоверения, извън публикуваната информация за статуса на удостоверението;
- кореспонденция, свързана с дейността на Доставчика;
- частните ключове на Доставчика;
- Договора за предоставяне на квалифицирани удостоверителни услуги;
- архивите за направени искания за издаване, спиране, възобновяване и прекратяване на удостоверения;
- архиви на транзакции;
- записи на външни и вътрешни проверки и доклади;
- планове за възстановяване след бедствия и непредвидени случаи.

Не се третират като конфиденциални следните обекти 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;

- доклади от органа за оценяване на съответствието, други външни одитори и Надзорния орган.

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 когато е задължен по силата на специален закон да разкрие такава информация, пред 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 и в информацията за статуса на удостоверенията, 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 и е с осигурен публичен достъп на трети лица до нея.

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 съгласяват личните им данни, събрани от Доставчика, да бъдат включени в квалифицирано удостоверение и да са общодостъпни за всички заинтересовани лица от Регистъра на удостоверенията и Списъка на спрените и прекратени 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 й и съобразно политиката на издаване на удостоверението.

Доставчикът отговаря пред Титуляря 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.

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 към трети лица

Титуляря 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, 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 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 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 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 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.