



InfoNotary

**ПОЛИТИКА ЗА
ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНО
УДОСТОВЕРЕНИЕ ЗА АВТЕНТИЧНОСТ НА
УЕБСАЙТ**

НА
КВАЛИФИЦИРАНИЯ ДОСТАВЧИК НА
УДОСТОВЕРИТЕЛНИ УСЛУГИ
ИНФОНОТАРИ ЕАД

ВЕРСИЯ 2.1

В сила от 14.10.2019 г.

СЪДЪРЖАНИЕ

1.	ВЪВЕДЕНИЕ	4
1.1.	ОСНОВНИ ПОЛОЖЕНИЯ	5
1.2.	ИМЕНУВАНЕ И ИДЕНТИФИКАЦИЯ НА ДОКУМЕНТА	6
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.	ИМЕНУВАНЕ	19
3.1.	ПЪРВОНАЧАЛНА ИДЕНТИФИКАЦИЯ И ПОТВЪРЖДАВАНЕ НА САМОЛИЧНОСТТА	22
3.2.	ИДЕНТИФИКАЦИЯ И АВТЕНТИФИКАЦИЯ ПРИ ЗАЯВКА ЗА ПРЕКРАТЯВАНЕ НА УДОСТОВЕРЕНИЕ	23
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	24
4.3.	ИЗДАВАНЕ НА УДОСТОВЕРЕНИЕ	24
4.4.	ТАЙНА НА ДАННИТЕ ПРИ КВАЛИФИЦИРАНИТЕ УДОСТОВЕРИТЕЛНИ УСЛУГИ И УПОТРЕБА НА УДОСТОВЕРЕНИЯТА	24
4.5.	ПОДНОВЯВАНЕ НА УДОСТОВЕРЕНИЕТО.....	24
4.6.	ПРЕКРАТЯВАНЕ НА УДОСТОВЕРЕНИЕ.....	25
4.7.	СПИРАНЕ НА УДОСТОВЕРЕНИЕ	26
5.	КОНТРОЛ НА ОБОРУДВАНЕТО,ПРОЦЕДУРИТЕ И УПРАВЛЕНИЕТО	28
5.1.	ФИЗИЧЕСКИ КОНТРОЛ.....	28
5.2.	ПРОЦЕДУРЕН КОНТРОЛ	29
5.3.	КОНТРОЛ НА ПЕРСОНАЛА, КВАЛИФИКАЦИЯ И ОБУЧЕНИЕ	31
5.4.	ПРОЦЕДУРИ ПО ИЗГОТВЯНЕ И ПОДДЪРЖАНЕ НА ЖУРНАЛ НА ДАННИ ОТ ПРОВЕРКИ.....	32
5.5.	АРХИВ	33
5.6.	КОМПРОМЕТИРАНЕ НА КЛЮЧОВЕ И ВЪЗСТАНОВЯВАНЕ СЛЕД БЕДСТВИЯ И НЕПРЕДВИДЕНИ СЛУЧАИ.....	34
5.7.	ПРОЦЕДУРИ ПО ПРЕКРАТЯВАНЕ ДЕЙНОСТТА НА ДОСТАВЧИКА.....	35
6.	КОНТРОЛ НА ТЕХНИЧЕСКАТА СИГУРНОСТ	37
6.1.	ГЕНЕРИРАНЕ И ИНСТАЛАЦИЯ НА ДВОЙКА КЛЮЧОВЕ.....	37
6.2.	ЗАЩИТА НА ЧАСТНИЯ КЛЮЧ И ТЕХНИЧЕСКИ КОНТРОЛ НА КРИПТОГРАФСКИЯ МОДУЛ.....	38
6.3.	АРХИВИРАНЕ НА ПУБЛИЧЕН КЛЮЧ	41
6.4.	ДАНИИ ЗА АКТИВИРАНЕ	42
6.5.	КОНТРОЛ НА КОМПЮТЪРНАТА СИГУРНОСТ.....	42
6.6.	ТЕХНИЧЕСКИ КОНТРОЛ НА ЖИЗНЕН ЦИКЪЛ.....	42
6.7.	КОНТРОЛ НА СИГУРНОСТТА НА МРЕЖАТА.....	43

7.	ПРОФИЛИ НА УДОСТОВЕРЕНИЯТА	44
7.1.	ПРОФИЛ НА БАЗОВОТО УДОСТОВЕРЕНИЕ INFONOTARY TSP ROOT	44
7.1.	ПРОФИЛ НА ОПЕРАТИВНОТО УДОСТОВЕРЕНИЕ INFONOTARY QUALIFIED VALIDATED DOMAIN CA	45
7.2.	ПРОФИЛ НА КВАЛИФИЦИРАНОТО УДОСТОВЕРЕНИЕ ЗА АВТЕНТИЧНОСТ НА УЕБСАЙТ INFONOTARY QUALIFIED VALIDATED DOMAIN	48
7.3.	ПРОФИЛ НА КВАЛИФИЦИРАНОТО УДОСТОВЕРЕНИЕ ЗА АВТЕНТИЧНОСТ НА УЕБСАЙТ ЗА ОРГАНИЗАЦИЯ INFONOTARY QUALIFIED ORGANIZATION VALIDATED CERTIFICATE	51
7.4.	ПРОФИЛ НА КВАЛИФИЦИРАНОТО УДОСТОВЕРЕНИЕ ЗА АВТЕНТИЧНОСТ НА УЕБСАЙТ ПО PSD2 INFONOTARY QUALIFIED PSD2 WA CERTIFICATE	53
8.	ПРОВЕРКА И КОНТРОЛ НА ДЕЙНОСТТА.....	57
8.1.	ОБХВАТ НА ПРОВЕРКАТА.....	57
8.2.	ПРЕДПРИЕМАНЕ НА ДЕЙСТВИЯ ЗА ОТСТРАНЯВАНЕ НА НЕДОСТАТЪЦИТЕ	58
9.	ДРУГИ БИЗНЕС И ПРАВНИ УСЛОВИЯ.....	58
9.1.	ЦЕНИ И ТАКСИ	58
9.2.	ФИНАНСОВИ ОТГОВОРНОСТИ.....	59
9.3.	КОНФИДЕНЦИАЛНОСТ НА ИНФОРМАЦИЯТА	60
9.4.	ПОВЕРИТЕЛНОСТ НА ЛИЧНИТЕ ДАННИ	60
9.5.	ПРАВА ВЪРХУ ИНТЕЛЕКТУАЛНАТА СОБСТВЕНОСТ	61
9.6.	ЗАДЪЛЖЕНИЯ, ОТГОВОРНОСТ И ГАРАНЦИИ НА ДОСТАВЧИКА	61
9.7.	ОТКАЗ ОТ ОТГОВОРНОСТ	64
9.8.	ОГРАНИЧЕНИЕ НА ОТГОВОРНОСТТА НА ДОСТАВЧИКА.....	64
9.9.	КОМПЕНСАЦИИ ЗА ДОСТАВЧИКА.....	64
9.10.	СРОК И ПРЕКРАТЯВАНЕ.....	65
9.11.	ИНДИВИДУАЛНО УВЕДОМЯВАНЕ И КОМУНИКАЦИЯ МЕЖДУ УЧАСТНИЦИТЕ	65
9.12.	ПРОМЕНИ В ПОЛИТИКАТА ЗА ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ ЗА АВТЕНТИФИКАЦИЯ НА УЕБСАЙТ	66
9.13.	РЕШАВАНЕ НА СПОРОВЕ И ПОДСЪДНОСТ.....	66
9.14.	ПРИЛОЖИМО ПРАВО	66
9.15.	СЪОТВЕТСТВИЕ С ПРИЛОЖИМОТО ПРАВО.....	67
9.16.	ДРУГИ РАЗПОРЕДБИ	67

1. ВЪВЕДЕНИЕ

Настоящия документ ПОЛИТИКА ЗА ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНО УДОСТОВЕРЕНИЕ ЗА АВТЕНТИЧНОСТ НА УЕБСАЙТ 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
- 319 411-2 v2.1.1: Requirements for trust service providers issuing EU qualified certificates;
- EN 319 412 Certificate Profiles
- 319 412-5 v2.1.1: QCStatements
- CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates
- TS 119 495 v1.2.1: Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive (EU) 2015/2366.

Основната цел на документа Политика за предоставяне на квалифицирано удостоверение за автентичност на уебсайт, 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 автентичност на уебсайт, да ги направи публични за потребителите и да предостави средства за всички заинтересувани страни за установяване на съответствието на дейността на Доставчика с разпоредбите и изискванията на Регламент (ЕС) 910/2014, приложимото законодателство на Република България, изискванията и насоките, дефинирани от CA/Browser Forum (<https://cabforum.org/>) 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 заинтересувани 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 Надзорен орган при предвидените в Регламент № (ЕС) 910/2014 условия и в съответствие със националното право.

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

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

Услуги по издаване на квалифицирани удостоверения за автентичност на уебсайт, включващи:

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

Услуги по управление на квалифицирани удостоверения за автентичност на уебсайт, включващи:

- отразяване на промените в статуса на валидност на издадено квалифицирано удостоверение;
- услуги по спиране, възобновяване и прекратяване действието на квалифицирано удостоверение;
- водене на регистър на издадените квалифицирани удостоверения;

- публикуване в регистъра на всяко издадено квалифицирано удостоверение;
- публикуване в регистъра на списък на спрените и прекратени квалифицирани удостоверения.

Услуги за достъп до квалифицирани удостоверения за автентичност на уебсайт, включващи:

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

Услуги за валидиране на квалифицирани удостоверения за автентичност на уебсайт, включващи:

- предоставяне на услуги за проверка в реално време на статуса на издадено квалифицирано удостоверение (OCSP).

При осъществяване на дейностите по издаване и управление на квалифицирани удостоверения за автентичност на уебсайт, 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 автентичност на уебсайт на ИНФОНОТАРИ ЕАД“ (Политиката), се именува “InfoNotary CP QWA” и се идентифицира посредством следния идентификатор на обект в издаваните удостоверения:

Policy name	Identifier (OID)
InfoNotary Qualified Validated Domain CP	1.3.6.1.4.1.22144.3.3.1

Политиката включва:

- описание на условията, които Доставчикът спазва и следва при издаване на квалифицирани удостоверения за автентичност на

- уебсайт, 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 автентичност на уебсайт, първоначалната идентификация и автентификация на Титулярите на удостоверения;
 - определя приложимостта и степента на доверие във включената в квалифицирани удостоверения за автентичност на уебсайт информация.

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 съдържашата се в различните типове удостоверения за крайни потребители индивидуализираща Титулярна 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 и други данни, в зависимост от типа на удостоверенията и в съответствие с удостоверителните политики на Доставчика;
- инициране на издаване на удостоверението след положителна проверка и одобряване на искането, като уведомяват Удостоверяващия орган;

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 документираните 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.

1.3.4. Доверяващи се страни

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

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

Доверяващите се страни са длъжни да извършват проверките на

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

1.3.5. Титуляр

„Титуляр“ е физическо или юридическо лице, което притежава издадено от Доставчика по негово искане квалифицирано удостоверение.

1.3.6. Представители

„Представител“ е надлежно овластено от Титуляря физическо лице, което извършва действия от негово име по издаване и управление на удостоверение за автентичност на уебсайт пред Доставчика.

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 автентичност на уебсайт, 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.

1.4.1.2. Оперативен удостоверяващ орган за издаване на удостоверения за автентичност на уебсайт (InfoNotary Qualified Validated Domain CA)

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

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

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

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

ИНФОНОТАРИ ЕАД издава квалифицирани удостоверения за автентичност на уебсайт в пълно съответствие с разпоредбите и изискванията на Регламент (ЕС) 910/2014 и изискванията и насоките на CA/Browser Forum (<https://cabforum.org/>).

1.4.1.3. Удостоверения за крайни потребители

InfoNotary Qualified Validated Domain Certificate Квалифицирано удостоверение за автентичност на уебсайт

Удостоверението се издава на Физическо или Юридическо лице (Титуляр) и може да бъде използвано за удостоверяване на

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

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

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

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

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

1.4.2. Ползване и достъпност на услугите

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

1.4.3. Ограничения на удостоверителното действие

Квалифицираните удостоверения за автентичност на уебсайт, които се издават от Доставчика, въз основа на настоящата Политика могат да бъдат с ограничено действие по отношение на целите и приложението. 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 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> и <https://repository.infonotary.com>.

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

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

1.6. ТЕРМИНИ И СЪКРАЩЕНИЯ

Валидиране	Процеса на проверка и потвърждаване на валидността на електронен подпис или печат.
Данни за валидиране	Данни, които се използват за валидиране на електронен подпис или електронен печат.
Данни за идентификация на лица	Набор от данни, които позволяват да се установи самоличността на физическо или юридическо лице, или на физическо лице, представляващо юридическо лице.
Доверяваща се страна	Физическо или юридическо лице, което разчита на електронна идентификация или удостоверителна услуга.
Доставчик на квалифицирани удостоверителни услуги	Доставчик на удостоверителни услуги, който предоставя една или повече квалифицирани удостоверителни услуги и е получил квалифицирания си статут от надзорен орган.
Електронен документ	Всяко съдържание, съхранявано в електронна форма, по-специално текстови или звуков, визуален или аудио-визуален запис.
Квалифицирано удостоверение за автентичност на уебсайт	Удостоверение за автентичност на уебсайт, което се издава от доставчик на квалифицирани удостоверителни услуги и отговаря на изискванията, предвидени в приложение IV на Регламент (ЕС) 910/2014.
КРС	Комисия за регулиране на съобщенията
ПИН	Персонален Идентификационен Номер
Практика	Практика при предоставяне на квалифицирани удостоверителни услуги
Политика	InfoNotary Qualified CPS Политика за предоставяне на квалифицирано удостоверение за автентичност на уебсайт;
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.
Удостоверение за автентичност на уебсайт	Удостоверение, което позволява да се удостовери автентичността на уебсайт, като го свързва с физическото или

Удостоверяване на автентичност

юридическото лице, на което е издадено удостоверението.
Електронен процес, който позволява електронната идентификация на физическо или юридическо лице или потвърждаването на произхода и целостта на данни в електронна форма.
Електронна услуга, обикновено предоставяна срещу възнаграждение, която се състои в:

Удостоверителна услуга

- 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.

PSD2 Директива

Директива (ЕС) 2015/2366 на Европейския парламент и на Съвета от 25 ноември 2015 година за платежните услуги във вътрешния пазар, за изменение на директиви 2002/65/ЕО, 2009/110/ЕО и 2013/36/ЕС и Регламент (ЕС) № 1093/2010 и за отмяна на Директива 2007/64/ЕО Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните)

Регламент GDPR

СЪКРАЩЕНИЯ

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

PSD2	Payment Service Directive 2
PSP	Доставчик на платежна услуга
PSP_AI	Account Information Service Provider
PSP_AS	Account Servicing Payment Service Provider
PSP_IC	Payment Service Provider issuing Card-based payment instruments
PSP_AI	Payment Initiation Service Provider
RA	Registration Authority – Регистриращ орган
RSA	Rivest-Shamir-Adelman – Криптографски алгоритъм за създаване на подпис
SSCD	Secure Signature Creation Device – Устройство за сигурно създаване на подпис
QSCD	Qualified Seal Creation Device – Устройство за създаване на Квалифициран печат
SHA	Secure Hash Algorithm – Хеш-алгоритъм за извличане на хеш-идентификатор
SSL	Secure Socket Layer – Сигурен канал за предаване на данни
URL	Uniform Resource Locator – Единен ресурсен локатор

2. ЗАДЪЛЖЕНИЯ ЗА ПУБЛИКУВАНЕ И ПОДДЪРЖАНЕ НА РЕГИСТРИ

Доставчикът публикува информация за издадените квалифицирани удостоверения за автентичност на уебсайт, 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. 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 автентичност на уебсайт.

2.1. Публикуване на информация за удостоверенията

Издадените квалифицирани удостоверения за автентичност на уебсайт се публикуват в регистъра на удостоверенията своевременно след тяхното подписване от съответния удостоверяващия орган на Доставчика - InfoNotary Qualified Validated Domain 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.

2.1. 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 Инфотари ЕАД.

2.1. 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 Създателя на печат, Доставчикът ограничава достъпа за четене и изтегляне на квалифицираното му удостоверение за автентичност на уебсайт, 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 автентичност на уебсайт. Преди да бъде потвърдено издаването на удостоверение от Удостоверяващия орган на Доставчика, Регистриращият орган потвърждава идентификацията на Титуляря. Регистриращите органи на Доставчика съблюдают 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. Именуване

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

Полето "Subject" в квалифицираното удостоверение за автентичност на уебсайт съдържа наименованието на уебсайт.

Името и другите отличителни данни на Титуляря в съответните

полета за всеки тип удостоверение са в съответствие с DN (Distinguished Name), образувано съгласно стандартите X.500 и X.520.

3.1.1. Типове имена

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

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

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

- C – международната абrevиатура на името на държавата (BG за България),
- CN – име на домейн (квалифицирано DNS име) или публичен IP адрес;
- GN – личното име на физическото лице (опционално)
- SN – фамилия на физическото лице (опционално)
- O – име на юридическото лице
- Organization Identifier – идентификатор на юридическото лице
- E – електронна поща,
- Serial Number – уникалният идентификатор на физическото лице,
- Други полета, които са детайлно описани профила на съответното квалифицирано удостоверение.

3.1.2. Псевдоними

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

3.1.3. Алтернативно име (Subject Alt Name)

Съдържа минимум CN записа, като в него могат да бъдат вписани и допълнителни домейни/публични IP адреси, под контрола на Титуляря на удостоверението.

3.1.4. Правила за интерпретиране на различните форми на имената

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

За идентификация на Титуляр – Физическо лице, на удостоверение се включват следните данни в GN – личното име на физическото лице и SN – фамилия на физическото лице.

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

- пълното име на юридическото лице по документи за регистрация

В квалифицираните удостоверения за автентичност на уебсайт уникалното име (DN) задължително съдържа информация за име на уебсайта (домейн), който се притежава от юридическото лице Титуляр.

3.1.5. Уникалност на имената

Доставчикът издава удостоверения с уникален номер в неговия регистър.

Комбинацията от името на Титуляря, заедно с типа на удостоверението са уникални за валидните удостоверения.

3.1.6. Признаване, автентичност и роля на търговските марки

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

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

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

Доставчикът не носи отговорност, ако включени в удостоверението

данни нарушават авторски права или права върху собственост на име, марка и др.

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

3.1. Първоначална идентификация и потвърждаване на самоличността

Процедурата е описана в Практика при предоставяне на квалифицирани удостоверителни услуги на ИНОФОНОТАРИ ЕАД.

3.1.1. Метод за потвърждаване на държането на частния ключ

Процедурата е описана в Практика при предоставяне на квалифицирани удостоверителни услуги на ИНОФОНОТАРИ ЕАД.

3.1.2. Установяване на самоличността на физическо лице

Процедурата е описана в Практика при предоставяне на квалифицирани удостоверителни услуги на ИНОФОНОТАРИ ЕАД.

3.1.3. Установяване на идентичността на Юридическо лице

Процедурата е описана в Практика при предоставяне на квалифицирани удостоверителни услуги на ИНОФОНОТАРИ ЕАД.

3.1.4. Автентификация на името на домейна (уебсайта)

Преди издаване на квалифицираното удостоверение за автентичност на уебсайт, Доставчика извършва проверка на заявеното за вписване име на домейн и и/или IP адреса. Проверката включва удостоверяване на собствеността на домейна от лицето, заявило издаване на удостоверението, както и че домейна и IP адреса са работоспособни и под негов контрол.

3.1.5. Непотвърдена информация

Процедурата е описана в Практика при предоставяне на квалифицирани удостоверителни услуги на ИНОФОНОТАРИ ЕАД.

3.2. Идентификация и автентификация при заявка за прекратяване на удостоверение

Процедурата е описана в Практика при предоставяне на квалифицирани удостоверителни услуги на ИНОФОНОТАРИ ЕАД.

3.3. Идентификация и автентификация при заявка за спиране на удостоверение

Процедурата е описана в Практика при предоставяне на квалифицирани удостоверителни услуги на ИНОФОНОТАРИ ЕАД.

4. ОПЕРАТИВНИ УСЛОВИЯ

4.1. Искане за издаване на удостоверение

Процедурата е описана в Практика при предоставяне на квалифицирани удостоверителни услуги на ИНОФОНОТАРИ ЕАД.

4.2. Процедура по заявяване на Удостоверение

Процедурата е описана в Практика при предоставяне на квалифицирани удостоверителни услуги на ИНОФОНОТАРИ ЕАД.

4.3. Издаване на удостоверение

4.3.1. Действия на Удостоверяващия орган при издаване на Удостоверение

Процедурата е описана в Практика при предоставяне на квалифицирани удостоверителни услуги на ИНОФОНОТАРИ ЕАД.

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

Процедурата е описана в Практика при предоставяне на квалифицирани удостоверителни услуги на ИНОФОНОТАРИ ЕАД.

4.5. Подновяване на Удостоверението

4.5.1. Условия за подновяване на удостоверение

Процедурата е описана в Практика при предоставяне на квалифицирани удостоверителни услуги на ИНОФОНОТАРИ ЕАД.

4.5.2. Процедура по заявяване на подновяване

Процедурата е описана в Практика при предоставяне на квалифицирани удостоверителни услуги на ИНОФОНОТАРИ ЕАД.

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:

- прекратяване на юридическото лице – Титуляр;
- 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 физическото лице, представляващо Титуляря.

4.6.2. Процедура за заявка за прекратяване

Процедурата е описана в Практика при предоставяне на квалифицирани удостоверителни услуги на ИНОФОНОТАРИ ЕАД.

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 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 му 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

Процедурата е описана в Практика при предоставяне на квалифицирани удостоверителни услуги на ИНОФОНОТАРИ ЕАД.

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

Процедурата е описана в Практика при предоставяне на квалифицирани удостоверителни услуги на ИНОФОНОТАРИ ЕАД.

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, пропускане 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 довереност и стабилност при изпълнение на всички поети от него

задължения и компетентност за извършване на дейността на Квалифициран Доставчик на удостоверителни услуги в съответствие с изискванията на Регламент (ЕС) 910/2014 и приложимото законодателство на България.

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

Всички лица от персонала на Доставчика подписват декларация за липсата на конфликт на интереси, спазване на конфиденциалност на информацията и защита на личните данни.

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

За определени дейности Доставчикът може да ползва и външни лица.

5.2.1. Длъжности и функции

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

5.2.2. Брой на служителите за определена задача

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

5.2.3. Идентификация и автентификация за всяка длъжност

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

5.2.4. Изисквания за разделяне на отговорностите при отделните функции

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

5.3. Контрол на персонала, квалификация и обучение

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

- технологии за сигурност, криптография, инфраструктура на публични ключове (PKI);
- технически норми за оценка на сигурността;
- информационни системи;
- администриране на големи бази данни;
- мрежова сигурност;
- 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 персоналят 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 РКІ 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 сървър 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, сринове 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 Създателя на печат, същият е задължен незабавно да уведоми Доставчикът за инициране 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 удостоверенията на удостоверяващите си органи, на всички издадени от него удостоверения и съхранява цялата документация, свързана с дейността му, ведно с всички архиви и всички издадени удостоверения (валидни, прекратени и спрени), за срок от 10 години.

Ако 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

Процедурата е описана в Практика при предоставяне на квалифицирани удостоверителни услуги на ИНОФОНОТАРИ ЕАД.

6.1.1. Генериране на двойка ключове

6.1.1.1. Генериране на частен ключ на Удостоверяващия орган на Доставчика

Процедурата е описана в Практика при предоставяне на квалифицирани удостоверителни услуги на ИНОФОНОТАРИ ЕАД.

6.1.1.2. Генериране на двойка ключове на Абонат

Процедурата е описана в Практика при предоставяне на квалифицирани удостоверителни услуги на ИНОФОНОТАРИ ЕАД.

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

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

Заявителя може да предостави електронната заявка:

- лично в Регистриращия орган или
- по електронен път и на адрес <http://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 автентичност на уебсайт частният ключ следва да е с дължина най-малко 2048 бита за алгоритмите RSA.

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

6.2.1. Стандарти на криптографския модул

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

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

Доставчика приема при издаване на квалифицирани удостоверения за квалифициран електронен подпис, устройството за създаване на квалифициран 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 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 Титуляря 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 електронен подпис съгласно изискванията на Регламент (ЕС) № 910/2014) и е достъпен посредством ПИН и не може да бъде съхранен на друго устройство или извън него.

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 на прави копия и не архивира частните ключове на Титуляря, които са генерирани на устройство за създаване на квалифициран електронен подпис. При дефект, загуба или унищожаване на устройството за създаване на квалифициран електронен подпис, Доставчика прекратява удостоверение, което 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.

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

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 квалифициран 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 унищожаване чрез изтриване на контейнера на устройството за създаване на квалифициран електронен подпис или чрез физическо унищожаване на самото устройство. Други аспекти от управлението на двойката ключове

6.3. 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.

6.3.1. 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 смарт карта за съхранение на частния си ключ е задължен да съхранява и пази от компрометиране персоналните данни за активиране на своята смарт карта или токън - ПИН или парола.

6.5. Контрол на 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.

Степента на надеждност на използваните от Доставчика техническо оборудване, технологии и системи покрива нормативните изисквания за извършване на дейност като Доставчик на удостоверителни услуги.

6.6. Технически 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		

7.1. Профил на оперативното удостоверение InfoNotary Qualified Validated Domain CA

InfoNotary Qualified Validated Domain CA	
Основни x509 атрибути:	
Атрибут	Стойност
Версия	3 (0x02)
Сериен номер	Уникален за регистъра на Доставчика; 16-байтово число
Начало на периода на валидност	Дата и час на подписване
Край на периода на валидност	Дата и час на подписване + 19 години
Алгоритъм на електронния подпис	SHA256/RSA
Атрибути на Издателя:	
Атрибут	Стойност

Common Name	Име	CN	InfoNotary TSP Root
Domain Component	Домейн компонент	DC	qualified-root-ca
Country Name	Държава	C	BG
Locality Name	Град	L	Sofia
Organization Name	Организация	O	InfoNotary PLC
Organizational Unit Name	Организационно звено	OU	Qualified TSP
Organization Identifier	Идентификатор на организацията (ЕИК)	2.5.4.97	NTRBG-131276827
Атрибути на Титуляря (x509 Subject DN):			
Атрибут		Стойност	
Common Name	Име	CN	InfoNotary Qualified Validated Domain CA
Domain Component	Домейн компонент	DC	qualified-domain-ca
Country Name	Държава	C	BG
Locality Name	Град	L	Sofia
Organization Name	Организация	O	InfoNotary PLC
Organizational Unit Name	Организационно звено	OU	Qualified TSP
Organization Identifier	Идентификатор на организацията (ЕИК)	2.5.4.97	NTRBG-131276827
Допълнителни атрибути на x509 разширения (x509v3 extensions):			
Атрибут		Стойност	
Basic Constraints (Critical)	Subject Type=CA		
Key Usage (Critical)	Certificate Signing, CRL Signing		
Public Key	RSA 3072 bits		
Authority information Access	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL= http://ocsp.infonotary.com/qualified		
CRL Distribution Point (Non Critical)	[1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl.infonotary.com/crl/qualified-root-ca.crl		

Certificate Policies (Non Critical)	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.22144.3.3 [1.1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://repository.infonotary.com/cps/qualified-tsp.html Unnotice:InfoNotary Qualified Validated Domain CA
Subject Key Identifier	subjectKeyIdentifier
Authority Key Identifier	authorityKeyIdentifier=keyid,issuer

7.2. Профил на квалифицираното удостоверение за автентичност на уебсайт InfoNotary Qualified Validated Domain

InfoNotary Qualified Validated Domain Certificate			
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 или 2 год.	
Алгоритъм на електронния подпис		SHA256/RSA	
Атрибути на Издателя:			
Атрибут		Стойност	
Domain Component	Домейн компонент	DC	qualified-domain-ca
Common Name	Име	CN	InfoNotary Qualified Validated Domain CA
Country Name	Държава	C	BG
Locality Name	Град	L	Sofia
Organization Name	Организация	O	InfoNotary PLC
Organizational Unit Name	Организационно звено	OU	Qualified TSP
Organization Identifier	Идентификатор на организацията (ЕИК)	2.5.4.97	NTRBG-131276827
Атрибути на Титуляря (x509 Subject DN):			
Атрибут		Стойност	
Common Name	Име на уебсайт(домейн)	CN	Domain name, IP, име на ресурс
Domain Component	Домейн компонент	DC	qualified-domain-ca
Country Name	Държава	C	
Locality Name	Град	L	

Email	Електронен адрес	E	
Organization	Име на юридическото лице, организация	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
Given Name	Лично име	G	Собствено име на по документ за самоличност (изписано на латиница)
Sur Name	Фамилия	Sn	Фамилно име по документ за самоличност (изписано на латиница)
Serial Number	Уникален идентификатор на физическото лице	2.5.4.5	PNOBG-XXXXXXXXXX (ЕГН) PASBG-XXXXXXXXXX (Номер на паспорт) IDCBG- XXXXXXXXXXXX (Номер на лична карта) TINBG-XXXXXXXXXX (ДДС идентификационен номер)
			PNOYY-XXXXXXXXXX (National Personal Number) PASYY-XXXXXXXXXX (Passport Number) IDCYY- XXXXXXXXXXXX (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, Key Encipherment		
Public Key	RSA 2048 bits		
Authority Key Identifier	AuthorityKeyIdentifier		
Subject Key Identifier	SubjectKeyIdentifier		

Authority information Access	<p>[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-domain-ca.crt</p> <p>[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</p>
CRL Distribution Point (Non Critical)	<p>[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.infonotary.com/crl/qualified-domain-ca.crl</p>
Certificate Policies (Non Critical)	<p>[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.22144.3.3.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://repository.infonotary.com/cps/qualified-tsp.html [1,2]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text=InfoNotary Qualified Domain Certificate</p> <p>[2]Certificate Policy: Policy Identifier=0.4.0.194112.1.4</p> <p>[3]Certificate Policy: Policy Identifier=0.4.0.2042.1.6</p>
Subject Alternative Name	DNS name [Domain name or IP]
Qualified Certificate Statement (Non Critical)	<p>id-etsi-qcs-semanticId-Legal (oid=0.4.0.194121.1.2)</p> <p>id-etsi-qcs-semanticId-Natural (oid=0.4.0.194121.1.1)*</p> <p>id-etsi-qcs-QcCompliance (oid=0.4.0.1862.1.1)</p> <p>id-etsi-qct-web (oid=0.4.0.1862.1.6.3)</p> <p>id-etsi-qcs-QcPDS (oid=0.4.0.1862.1.5) PDSLocation=https://repository.infonotary.com/pds/pds_bg.pdf Language=bg PDSLocation=http://repository.infonotary.com/pds/pds_en.pdf Language=en</p>
Extended Key Usage (Non Critical)	<p>Client Authentication Server Authentication</p>

7.3. Профил на квалифицираното удостоверение за автентичност на уебсайт за организация **InfoNotary Qualified Organization Validated Certificate**

InfoNotary Qualified Organization Validated Certificate			
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 или 2 год.	
Алгоритъм на електронния подпис		SHA256/RSA	
Атрибути на Издателя:			
Атрибут		Стойност	
Domain Component	Домейн компонент	DC	qualified-domain-ca
Common Name	Име	CN	InfoNotary Qualified Validated Domain CA
Country Name	Държава	C	BG
Locality Name	Град	L	Sofia
Organization Name	Организация	O	InfoNotary PLC
Organizational Unit Name	Организационно звено	OU	Qualified TSP
Organization Identifier	Идентификатор на организацията (ЕИК)	2.5.4.97	NTRBG-131276827
Атрибути на Титуляря (x509 Subject DN):			
Атрибут		Стойност	
Common Name	Име на уебсайт(домейн)	CN	Domain name, IP
Domain Component	Домейн компонент	DC	qualified-domain-ca
Country Name	Държава	C	
Locality Name	Град	L	

Email	Електронен адрес	E	
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, Key Encipherment		
Public Key	RSA 2048 bits		
Authority Key Identifier	AuthorityKeyIdentifier		
Subject Key Identifier	SubjectKeyIdentifier		
Authority information Access	<p>[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-domain-ca.crt</p> <p>[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</p>		
CRL Distribution Point (Non Critical)	<p>[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.infonotary.com/crl/qualified-domain-ca.crl</p>		

Certificate Policies (Non Critical)	<p>[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.22144.3.3.2 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://repository.infonotary.com/cps/qualified-tsp.html [1,2]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text= InfoNotary Qualified Organization Validated Certificate</p> <p>[2]Certificate Policy: Policy Identifier=0.4.0.194112.1.4</p> <p>[3]Certificate Policy: Policy Identifier=0.4.0.2042.1.7</p>
Subject Alternative Name	DNS name [Domain name or IP]
Qualified Certificate Statement (Non Critical)	<p>id-etsi-qcs-semanticSId-Legal (oid=0.4.0.194121.1.2)</p> <p>id-etsi-qcs-QcCompliance (oid=0.4.0.1862.1.1)</p> <p>id-etsi-qct-web (oid=0.4.0.1862.1.6.3)</p> <p>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</p>
Extended Key Usage (Non Critical)	Client Authentication Server Authentication

7.4. Профил на квалифицираното удостоверение за автентичност на уебсайт по PSD2 InfoNotary Qualified PSD2 WA Certificate

InfoNotary Qualified PSD2 WA Certificate	
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 или 2 год.

Алгоритъм на електронния подпис			SHA256/RSA
Атрибути на Издателя:			
Атрибут			Стойност
Domain Component	Домейн компонент	DC	qualified-domain-ca
Common Name	Име	CN	InfoNotary Qualified Validated Domain CA
Country Name	Държава	C	BG
Locality Name	Град	L	Sofia
Organization Name	Организация	O	InfoNotary PLC
Organizational Unit Name	Организационно звено	OU	Qualified TSP
Organization Identifier	Идентификатор на организацията (ЕИК)	2.5.4.97	NTRBG-131276827
Атрибути на Титуляря (x509 Subject DN):			
Атрибут			Стойност
Common Name	Име на уебсайт(домейн)	CN	Domain name, IP
Domain Component	Домейн компонент	DC	qualified-domain-ca
Country Name	Държава	C	
Locality Name	Град	L	
Email	Електронен адрес	E	
Organization	Име на юридическото лице	O	
Organizational Unit Name	Организационно звено	OU	
Organization Identifier	Уникален идентификатор на юридическото лице	2.5.4.97	PSDYY-Z-XXXXXXXXXX YY – код на държавата Z – от 2 до 8 символа идентификатор на National Competent Authority (NCA) X - PSP identifier
Допълнителни атрибути на x509 разширения (x509v3 extensions):			
Атрибут			Стойност
Basic Constraints (Critical)	End entity		
Key Usage (Critical)	Digital Signature, Key Encipherment		

Public Key	RSA 2048 bits
Authority Key Identifier	AuthorityKeyIdentifier
Subject Key Identifier	SubjectKeyIdentifier
Authority information Access	<p>[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-domain-ca.crt</p> <p>[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</p>
CRL Distribution Point (Non Critical)	<p>[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.infonotary.com/crl/qualified-domain-ca.crl</p>
Certificate Policies (Non Critical)	<p>[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.22144.3.3.3 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://repository.infonotary.com/cps/qualified-tsp.html [1,2]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text= InfoNotary Qualified PSD2 WA Certificate</p> <p>[2]Certificate Policy: Policy Identifier=0.4.0.194112.1.4</p> <p>[3]Certificate Policy: Policy Identifier=0.4.0.2042.1.7</p>
Subject Alternative Name	DNS name [Domain name or IP]

<p>Qualified Certificate Statement (Non Critical)</p>	<p>id-etsi-qcs-semanticId-Legal (oid=0.4.0.194121.1.2)</p> <p>id-etsi-qcs-QcCompliance (oid=0.4.0.1862.1.1)</p> <p>id-etsi-qct-web (oid=0.4.0.1862.1.6.3)</p> <p>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</p> <p>id-etsi-psd2- qsStatement (oid=0.4.0.19495.2)</p> <p>RolesOfPSP (oid=0.4.0.19495.2) – една или повече от следните роли: roleOfPspName =PSP_AS roleOfPspOid (oid=0.4.0.19495.1.1), roleOfPspName =PSP_PI roleOfPspOid (oid=0.4.0.19495.1.2), roleOfPspName =PSP_AI roleOfPspOid (oid=0.4.0.19495.1.3) roleOfPspName =PSP_IC roleOfPspOid (oid=0.4.0.19495.1.4)</p> <p>nCAName = (име на National Competent Authority) nCAId = (Абривиатура на идентификатор на NCA – YY-Z) YY – код на държавата Z – от 2 до 8 символа идентификатор на National Competent Authority</p>
<p>Extended Key Usage (Non Critical)</p>	<p>Client Authentication Server Authentication</p>

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

Процедурата е описана в Практика при предоставяне на

квалифицирани удостоверителни услуги на ИНОФОНОТАРИ 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 карта, 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

Процедурата е описана в Практика при предоставяне на квалифицирани удостоверителни услуги на ИНОФОНОТАРИ ЕАД.

9.1.2. Фактуриране

Процедурата е описана в Практика при предоставяне на квалифицирани удостоверителни услуги на ИНОФОНОТАРИ ЕАД.

9.1.3. Политика за връщане на удостоверението и възстановяване на плащането

Процедурата е описана в Практика при предоставяне на квалифицирани удостоверителни услуги на ИНОФОНОТАРИ ЕАД.

9.2. Финансови отговорности

9.2.1. Финансова отговорност

ИНОФОНОТАРИ 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.

ИНОФОНОТАРИ 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.

Процедурата е описана в Практика при предоставяне на квалифицирани удостоверителни услуги на ИНОФОНОТАРИ ЕАД.

9.2.2. Застрахователно покритие за крайните потребители

Процедурата е описана в Практика при предоставяне на квалифицирани удостоверителни услуги на ИНОФОНОТАРИ ЕАД.

9.3. Конфиденциалност на информацията

Процедурата е описана в Практика при предоставяне на квалифицирани удостоверителни услуги на ИНОФОНОТАРИ ЕАД.

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

Процедурата е описана в Практика при предоставяне на квалифицирани удостоверителни услуги на ИНОФОНОТАРИ ЕАД.

9.6. Задължения, отговорност и гаранции на Доставчика

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

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

Доставчикът отговаря пред Титуляря/Създателя и пред всички

трети лица за вредите, причинени от:

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

9.6.1. Гаранции и отговорност на Регистриращия орган

Процедурата е описана в Практика при предоставяне на квалифицирани удостоверителни услуги на ИНОФОНОТАРИ ЕАД.

9.6.2. 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.

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

Титуляря 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 за вреди.

9.6.3. Дължимата 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 квалифицирани удостоверения от страна на Титуляри 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 отговаря 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/Създателя на печат/Абоната произтичащи от Практиката за

предоставяне на квалифицирани удостоверителни услуги и/или от Договора за квалифицирани удостоверителни услуги, Доставчикът ще ангажира отговорността на Титуляря, съответно Създателя за вреди.

9.10. Срок и прекратяване

9.10.1. Срок

Политиката влиза в сила от момента на нейното одобряване от Съвета на директорите на Инфонотари ЕАД и публикуването ѝ на адрес: <http://repository.infonotary.com>.

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

9.10.2. Прекратяване и недействителност

Действието на Политиката се прекратява с прекратяване на дейността на Доставчика.

В случай, че някоя от клаузите на настоящата Политика се окаже недействителна, това няма да влече други клаузи или части от Политиката или да доведе до недействителност на целия договор с Абонат. Недействителната клауза ще бъде заместена от повелителните норми на закона.

9.10.3. Ефект от прекратяването

След прекратяване на действието на Политиката за потребителя остават в сила разпоредбите за задълженията на Доставчика за поддържане на архив на документите и удостоверенията в обема и за периода.

9.11. Индивидуално уведомяване и комуникация между участниците

Всички заинтересувани страни могат да отправят съобщения до Доставчика във връзка с разпоредбите на Политиката и договорите посредством подписани електронни съобщения с квалифициран електронен подпис, писма с обратна разписка или писма, доставени от куриер до Доставчика.

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

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

9.12. Промени в Политиката за предоставяне на квалифицирано удостоверение за автентификация на уебсайт

Политиката може да бъде променяна по всяко време, като всяка промяна в нея се отразява след одобрение от Съвета на директорите на Инфонотари ЕАД и е публично достъпна от всички заинтересувани лица на адрес: <http://www.infonotary.com>.

Всяко лице може да отправя предложения за промени (структурни и съдържателни) и бележки за забелязани грешки на посочените в настоящия документ електронни и пощенски адреси за контакти с Доставчика.

9.13. Решаване на спорове и подсъдност

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

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

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

9.14. Приложимо право

За всички въпроси, неуредени в настоящата Политика, се прилагат разпоредбите на националното право.

9.15. Съответствие с приложимото право

Настоящата Политика е разработена в съответствие с изискванията на Регламент (ЕС) 910/2014 и националното законодателство.

9.16. Други разпоредби

Политиката не съдържа други разпоредби.