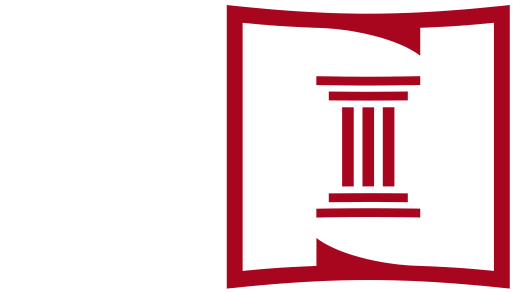

InfoNotary

ПОЛИТИКА ЗА

ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УСЛУГИ ЗА УДОСТОВЕРЯВАНЕ НА ВРЕМЕ (TIME STAMPS)

НА

КВАЛИФИЦИРАНИЯ ДОСТАВЧИК НА УДОСТОВЕРИТЕЛНИ УСЛУГИ

ИНФОНОТАРИ ЕАД

ВЕРСИЯ 1.4

В сила от 16.12.2024 г.

СЪДЪРЖАНИЕ

1. ВЪВЕДЕНИЕ

Настоящия документ ПОЛИТИКА ЗА ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УСЛУГИ ЗА УДОСТОВЕРЯВАНЕ НА ВРЕМЕ на Доставчика на удостоверителни услуги ИНФОНОТАРИ ЕАД (Политиката) е изготвен в съответствие с приложимото Европейско и национално законодателство на и се позовава на целите или на част от следните общоприети международни стандарти и спецификации:

- 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);
- РЕГЛАМЕНТ (ЕС) 2024/1183 НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА от 11 април 2024 година за изменение на Регламент (ЕС) № 910/2014 по отношение на създаването на европейска рамка за цифрова самоличност
- EN 319 401 v2.1.1 General Policy Requirements for Trust Service Providers;
- ETSI EN 319 421, Policy and Security Requirements for Trust Service Providers issuing Time-Stamps
- ETSI TS 102 023 v.1.2.1 Policy Requirements for time-stamping authorities
- EN 319 411 Policy and security requirements for Trust Service Providers issuing certificates
- 319 411-1 v1.1.1: General requiremenTS;
- IETF RFC 3161 (2001): "Internet X.509 Public Key Infrastructure: Time-Stamp Protocol (TSP)";
- IETF RFC 5816 ESSCertIDv2 Update for RFC 3161
- RFC 3647: Internet X.509 Public Key Infrastructure – Certificate Policies and Certification Practices Framework.

Основната цел на Политиката, е чрез описание на правилата и политиките, които ИНФОРНОТАРИ ЕАД е въвела и съблюдава при издаване и валидиране на квалифицирани електронни времеви печата, 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 и на надеждността и сигурността на осъществяваната удостоверителна дейност.

Политиката е публичен документ, разработен в съответствие ETSI

EN 319 421.

2. Управление на удостоверителната политика на Доставчика

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

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

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

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

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

3. ТЕРМИНИ И СЪКРАЩЕНИЯ

Валидиране	Процеса на проверка и потвърждаване на валидността на електронен подпис или печат.
Данни за валидиране	Данни, които се използват за валидиране на електронен подпис или електронен печат.
Данни за идентификация на лица	Набор от данни, които позволяват да се установи самоличността на физическо или юридическо лице, или на физическо лице, представляващо юридическо лице.
Данни за създаване на електронен печат	Уникални данни, които се използват от създателя на електронния печат за създаването на електронен печат
Доверяваща се страна	Физическо или юридическо лице, което разчита на електронна идентификация или удостоверителна услуга.
Доставчик на квалифицирани удостоверителни услуги	Доставчик на удостоверителни услуги, който предоставя една или повече квалифицирани удостоверителни услуги и е получил квалифицирания си статут от надзорен орган.
Електронен времеви печат	Данни в електронна форма, които свързват други данни в електронна форма с конкретен момент във времето и представляват доказателство, че последните данни са съществували в съответния момент.
Електронен документ	Всяко съдържание, съхранявано в електронна форма, по-специално текстови или звуков, визуален или аудио-визуален запис.
Квалифициран електронен времеви печат	Електронен времеви печат, който отговаря на следните изисквания: а) обвързва датата и часа с данните по начин, който до голяма степен изключва възможността за незабелязана промяна на

	данните; б) основава се на източник на точно време, свързан с координираното универсално време; и в) подписан е с усъвършенстван електронен подпис или е подпечатан с усъвършенстван електронен печат на доставчик на квалифицирани удостоверителни услуги или с друг равностоен метод.
КРС	Комисия за регулиране на съобщенията
ПИН	Персонален Идентификационен Номер
Практика	Практика при предоставяне на квалифицирани удостоверителни услуги **InfoNotary Qualified CPS**
Политика	Политика за предоставяне на квалифицирани услуги за удостоверяване на време.
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.
Удостоверяване на автентичност	Електронен процес, който позволява електронната идентификация на физическо или юридическо лице или потвърждаването на произхода и целостта на данни в електронна форма.
Удостоверителна услуга	Електронна услуга, обикновено предоставяна срещу възнаграждение, която се състои в: - създаването, проверката и валидирането на електронни подписи, електронни печати или електронни времеви печати, услуги за електронна препоръчана поща, както и удостоверения, свързани с тези услуги; или - създаването, проверката и валидирането на удостоверения за

	автентичност на уебсайт; или - съхраняването на електронни подписи, печати или удостоверения, свързани с тези услуги.
Регламент GDPR	Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните)

СЪКРАЩЕНИЯ

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

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

4. ОСНОВНИ ПОЛОЖЕНИЯ

4.1.1. Доставчик на удостоверителни услуги

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

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

Като квалифициран доставчик ИНФОНОТАРИ ЕАД извършва удостоверителни дейности и предоставя квалифицирани удостоверителни услуги за удостоверяване на време чрез Орган за удостоверяване на време (InfoNotary Qualified TimeStamping Service).

Органа за удостоверяване на време на Доставчика издава квалифицирани електронни времеви печати, чрез които потребителите (Абонати на Доставчика и Трети доверяващи се страни) могат да удостоверят времето за представяне на електронен документ, подписване на документ или транзакция с електронен подпис и др.

При осъществяване на дейностите по издаване и управление на квалифицирани електронни времеви печати, 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.

4.1.2. Именуване и идентификация на документа

Документа **„Политика за предоставяне на квалифицирани услуги за удостоверяване на време на ИНФОНОТАРИ ЕАД" (Политиката),** се именува **"InfoNotary Qualified TimeStamping Service CP"** и се идентифицира посредством следния идентификатор на обект в издаваните удостоверения:

Policy name	Identifier (OID)
InfoNotary Qualified TimeStamping Service CP	1.3.6.1.4.1.22144.3.4.1

Политиката включва:

описание на условията, които Доставчикът спазва и следва при издаване на квалифицирани електронни времеви печати;

общите правила за издаване и управление на квалифицираните електронни времеви печати.

Издаваните удостоверения съдържат идентификатор на политика, издаден в съответствие с препоръка IETF RFC 3647 [I.4], т. 3.3, който може да бъде използван за разпознаването им от страна на Доверяващите се страни при използването им.

Идентификатора за политиките на квалифицираните електронни времеви печати, посочени в настоящия документ са както следва:

itu-t(0) identified-organization(4) etsi(0) time-stamp-policy(02023) policy-identifiers(1) baseline-ts-policy (1)

Обектния идентификатор (OID) в съответствие с вида на удостоверителната политика е:

	Име	InfoNotary Policy Identifier	ETSI Policy Identifier
Квалифициран електронен времеви печат	InfoNotary Qualified TimeStamping Service	1.3.6.1.4.1.22144.3.4.1	0.4.0.2023.1.1

4.2. Участници в удостоверителната инфраструктура

4.2.1. Удостоверяващ орган

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

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

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

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

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

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

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

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

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

Certificate Policies (Non Critical)	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.22144.3.4 [1.1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://repository.infonotary.com/cps/qualified-tsp.html Unotice: InfoNotary Qualified TimeStamping Service CA
Subject Key Identifier	SubjectKeyIdentifier
Authority Key Identifier	AuthorityKeyIdentifier

4.2.3. 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.

4.2.4. Доверяващи се лица

"Доверяващи се лица" са физически или юридически лица, които разчитат на удостоверителна услуга и които са адресати на подпечатани с електронен времеви печат електронни документи. Доверяващите се страни следва да имат умения да ползват заверките за електронен времеви печат и да се доверяват на издадени от Доставчика електронни времеви печати само след проверка на статуса на удостоверението на органа за време в Списъка на спрените и прекратени удостоверения (CRL) или на автоматичната информация, предоставена от Доставчика посредством OCSP протокол.

4.3. Приложимост на електронния времеви печат

Настоящата политика е насочена към покриване на изискванията за квалифицирани електронни времеви печати в съответствие с Регламент (ЕС) №910/2014 и ETSI EN 319 122.

Политиката не включва никакви ограничения в приложението на издаден от Доставчика и в съответствие с нея електронен времеви печат.

Политиката може да бъде приложена за удостоверяване на времето на създаване на електронен подпис/ електронен печат без ограничения.

5. ЗАДЪЛЖЕНИЯ, ОТГОВОРНОСТ И ГАРАНЦИИ

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

5.1. Задължения на Доставчика

Доставчикът се задължава да:

спазва своите вътрешни правила и процедури, практика за предоставяне на квалифицирани удостоверителни услуги и политики;

спазва Регламент (ЕС) № 910/2014 и разпоредбите на националното законодателство;

осигурява непрекъснато достъп до квалифицираната услуга за удостоверяване на време, освен при планирана профилактика и форсмажорни ситуации;

осигурява и ползва надеждно технологично оборудване при предоставяне на удостоверителната услуга;

предоставяните удостоверителни услуги са в съответствие с изискванията на общоприети международни стандарти и препоръки.

5.2. 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 настоящата политика.

Дейностите на Доставчика по предоставяне на квалифицираната услуга по удостоверяване на време подлежи на проверка от независим орган за оценяване на съответствието и националния надзорен орган.

Доставчикът отговаря пред Абонатите и пред Доверяващите се страни за вреди от:

от неизпълнение на задълженията на Доставчика, съгласно Регламент (ЕС) № 910/2014 и националното право, регламентиращи издаването, управлението и съдържанието на квалифицирания електронен времеви печат ;

от неверни или грешни данни в квалифицирания електронен времеви печат към момента на издаването му.

5.3. Задължения на Потребителите

Потребителите на квалифицираната услуга за удостоверяване на време са длъжни:

при подаване на заявки за издаване на електронен времеви печат да спазват изискванията на Доставчика за формата и начина на подаване на заявка;

при получаване на издадения електронен времеви печат да проверят валидността на електронния подпис на Органа за удостоверяване на време посредством проверка в поддържаните от Доставчика списъци с прекратени и спрени удостоверения и CRL и OCSP;

да изпълняват задълженията, описани в „Практика при предоставяне на квалифицирани удостоверителни услуги“.

5.4. Дължима грижа на Доверяващите се страни

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

имат технически умения да ползват квалифицираната услуга за удостоверяване на време;

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 електронни времеви печати посредством публикуваните данни за статуса на удостоверенията от Доставчика – Списъка на спрените и прекратени удостоверения;

се доверяват на издадени от Доставчика квалифицирани електронни времеви печати само ако резултатът от направените проверки за валидност е коректен и актуален;

да извършат проверка на приложимостта на използваните за създаване на времевия печат криптографски алгоритми;

5.5. 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 електронни времеви печати от страна на Абонатите или Доверяващите се страни.

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

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

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

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

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

Доставчикът не отговаря за сигурността, целостта и използването на

софтуерните продукти и хардуерни устройства, използвани от Абонати или Доверяващи се страни.

5.6. Ограничение на отговорността на Доставчика

В съответствие с т. 9.8 от документа ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги".

5.7. Компенсации за Доставчика

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

6. ИЗИСКВАНИЯ КЪМ ОРГАНА ЗА УДОСТОВЕРЯВАНЕ НА ВРЕМЕ

Доставчика гарантира, че осигурява механизми за контрол на дейността на Органа за удостоверяване на време, което позволява да се предоставя квалифицирана удостоверителна услуга в съответствие с разпоредбите на настоящата политика.

Всички събития в системата за удостоверяване на време се записват под формата на системни журнали, които се архивират и съхраняват по сигурен начин. Достъпа до журналите имат само оторизирани за това служители.

Доставчикът съблюдава в своята дейност политика на управление и на управление на персонала, осигуряваща необходимата гаранция за доверието 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.

7. ПРАКТИКА И ПРОЦЕДУРИ НА ОРГАНА ЗА УДОСТОВЕРЯВАНЕ НА ВРЕМЕ

Процедурите и механизмите за контрол при предоставяне на квалифицираната услуга за удостоверяване на време са описани в документа „Практика при предоставяне на квалифицирани удостоверителни услуги" на Инфонотари ЕАД.

Дейностите по управление, поддържане и усъвършенстване на услугите, предоставяни от органа за удостоверяване на време се изпълняват в съответствие с изискванията на имплементираната в Инфонотари ЕАД система за сигурност на информацията по стандарта ISO 27001:2013

7.1. Достъпност на услугата

Общите практики по предоставяне на квалифицираната услуга за удостоверяване на време са описани в документа „Практика при предоставяне на квалифицирани удостоверителни услуги" на Инфонотари ЕАД.

За осигуряване на качествена и достъпна услуга, всички системни компоненти и комуникационна свързаност са минимум двойно резервирани. Изградени са инфраструктури за осигуряване на непрекъснато захранване, базирани на непрекъсваеми електрозахранващи устройства (UPS) и дизелови генератори на електрозахранване.

7.2. Управление на жизнения цикъл на двойката ключове на органа за удостоверяване на време

7.2.1. Генериране и инсталация на двойка ключове

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

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

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

7.2.2. Генериране на частен ключ на Удостоверяващия орган на Доставчика

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

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

Осъществяването на документираната процедура по генериране и инсталиране на базовата (root) двойка ключове на Удостоверяващия орган на Доставчика се извършва от оторизиран за това служител на Доставчика и в присъствието на членовете на Съвета на директорите на "ИНФОНОТАРИ" ЕАД.

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

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

до управлението на хардуерния модул посредством секретни данни, достъпни само за оторизирани лица;

контрол на достъпа за управление и ползване на частните оперативни ключове на Удостоверяващия орган посредством отделни секретни данни, достъпни само за оторизирани лица.

7.2.3. 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.

7.2.4. 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.

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

7.3.1. 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.

7.3.2. 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.

7.3.3. 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.

7.3.4. 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.

7.3.5. 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.

7.3.6. 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.

7.3.7. 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.

7.4. Други аспекти от управлението на двойката ключове

7.4.1. Архивиране на Публичен ключ

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

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

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

съдържанието на удостоверението.

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

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

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

7.5. 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.

7.6. Контрол на компютърната сигурност

7.6.1. Специфични изисквания към компютърната сигурност

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

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

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

7.6.2. Рейтинг на компютърната сигурност

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

7.7. Техническият контрол на жизнен цикъл

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

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

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

7.8. Контрол на сигурността на мрежата

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

8. КВАЛИФИЦИРАНА УДОСТОВЕРИТЕЛНА УСЛУГА ПО УДОСТОВЕРЯВАНЕ НА ВРЕМЕ

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

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

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

които са титуляри или са доверяваща се страна.

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

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

8.1.1. Процедура по предоставяне на услугата удостоверяване на време

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

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

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

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

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

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

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

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

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

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

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

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

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

8.1.2. Независим източник на точно време

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

- NTPv4 (RFC 5905)
- SNMPv1 (RFC 1157), SNMPv3 (RFC 3411-3415)

Системата се синхронизира за точност посредством GPS и синхронизация от други NTP сървъри.

9. Профили на TimeStamp

9.1.1. Профил на TimeStamp Заявката

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

9.1.2. Профил на TimeStamp Отговор

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

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

10. КОНТРОЛ НА ОБОРУДВАНЕТО,ПРОЦЕДУРИТЕ И УПРАВЛЕНИЕТО

10.1. 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.

10.1.1. 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.

10.1.2. Физически достъп

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

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

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

10.1.3. 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.

10.1.4. Наводнение

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

10.1.5. Противопожарно известяване и защита

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

10.1.6. 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.

10.1.7. Извеждане от употреба на технически компоненти

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

10.1.8. 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.

10.2. Процедурен контрол

Доставчикът съблюдава в своята дейност политика на управление и на управление на персонала, осигуряваща необходимата гаранция за доверието 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 национално законодателство.

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

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

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

За определени дейности Доставчикът може да ползва и външни лица.

10.2.1. 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.

10.2.2. Брой на служителите за определена задача

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

10.2.3. Идентификация и автентификация за всяка длъжност

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

10.2.4. Изисквания за разделяне на отговорностите при отделните функции

Длъжностите по т.10.2.1 се изпълняват от различни лица от персонала на Доставчика.

10.3. 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.

10.3.1. Изисквания към независими доставчици

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

10.3.2. 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.

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

Процедурите по изготвяне и поддържане на журнал на данни от проверки включва документиране на събития и документиране на проверки на системите, имплементирани за целите на поддържане на защитена среда. Доставчикът записва всички събития, свързани с дейностите на Удостоверяващия орган, включващи, но не ограничени само до:

- издаване на удостоверение;
- подписване на удостоверение;
- прекратяване на удостоверение;
- спиране на удостоверение;
- публикуване на удостоверение;
- публикуване на Списък на спрените и прекратени удостоверения.

Записите съдържат следната информация:

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

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

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

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

Записите се създават автоматично и се съхраняват на дискретни интервали за различните модули. Оторизиран персонал на Доставчика на регулярни интервали проверява записите и логовете и установява и рапортува за аномалии.

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

Всички записи и логове, които се генерират от компонентите в удостоверителната инфраструктура, се съхраняват електронно. Единствено квалифицирани овластени лица от персонала на Доставчика имат право на достъп и работа с тези записи и логове.

Резервни копия на записите и логовете се създават на дискретни интервали от няколко часа до едно денонощие за различните модули. Резервните копия се записват на физически носители и се съхраняват в помещение с високо ниво на защита на контрола на достъпа.

10.5. Архив

Доставчикът съхранява като вътрешен архив следните документи:

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

Доставчикът съхранява архива във формат, възможен за възстановяване. Доставчикът осигурява целостта на физическите носители и осъществява механизъм за копирането им като превенция на загубата на данни. Архивът е достъпен само от оторизиран персонал на Доставчика и Регистриращите органи, ако е необходимо.

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

удостоверителните услуги.

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

Обезпечаването на сигурността на архива включва:

само персоналът, оторизиран да води архива, да има достъп до него;

защита от модификация на архива, като записването на данните върху средства за еднократен запис;

защита от изтриване на архива;

защита за сигурно унищожаване на носителите, на които архивът е бил записан, след изпълнение на действие по периодично прехвърляне на данните на нов носител.

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

Архивната информация се съхранява в помещение с висока степен на физическа защита и при условия, позволяващи безопасното и дългосрочно съхранение на хартиени, магнитни, оптични и други носители. Архивната информация, която е публична, се публикува и е достъпна в Публичните електронни регистри на Доставчика в четим вид.

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

За да поддържа непрекъсваемостта и целостта на услугите си, Доставчикът внедрява, документира и периодично тества подходящи планове и процедури за непредвидени случаи и възстановяване след бедствия. Доставчикът полага необходимите усилия да гарантира пълно и автоматично възобновяване на услугите си в случай на бедствие, сривове в компютърните ресурси, в софтуера или в информацията. Приоритетно Доставчикът осигурява възстановяването на поддържането и публичния достъп до регистъра на удостоверенията и списъка на спрените и прекратени удостоверения.

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

удостоверението за електронния подпис на Доставчика се прекратява незабавно;

уведомява се Надзорния орган за прекратяването на Удостоверението на Доставчика;

уведомяват се потребителите на удостоверителните услуги на Доставчика, чрез публикуване на информация на публичния сайт и по електронна поща;

Удостоверяващият орган на Доставчика се спира;

инициира се процедура по генериране на нова двойка криптографски ключове;

издава се ново удостоверение за електронния подпис на Доставчика;

всички издадени и валидни удостоверения преди компрометиране на ключа се преиздават.

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

10.6.1. 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.

10.7. 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.

11. ДРУГИ БИЗНЕС И ПРАВНИ УСЛОВИЯ

11.1. Цени и такси

Доставчикът определя цени и абонаментни такси за ползване на предоставяните от него квалифицирани удостоверителни услуги 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.