



InfoNotary

**ПОЛИТИКА И ПРАКТИКА
ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНА
УСЛУГА ЗА ОТДАЛЕЧЕНО ПОДПИСВАНЕ И
ПОДПЕЧАТВАНЕ НА ЕЛЕКТРОННИ
ДОКУМЕНТИ**

НА
КВАЛИФИЦИРАНИЯ ДОСТАВЧИК НА
УДОСТОВЕРИТЕЛНИ УСЛУГИ
ИНФОНОТАРИ ЕАД

ВЕРСИЯ 1.2

В сила от 16.12.2024 г.

СЪДЪРЖАНИЕ

1.	ВЪВЕДЕНИЕ	5
1.1.	КОНЦЕПЦИЯ НА СЪЗДАВАНЕ НА ЕЛЕКТРОНЕН ПОДПИС/ПЕЧАТ ОТ РАЗСТОЯНИЕ (ОТДАЛЕЧЕНО ПОДПИСВАНЕ/ПОДПЕЧАТВАНЕ С ОБЛАЧЕН КЕП). ЗАКОНОСЪОБРАЗНОСТ И ПРАВНА СИЛА.	5
1.2.	ПРЕДМЕТ	5
1.3.	СЪОТВЕТСТВИЕ	6
2.	ОСНОВНИ ПОЛОЖЕНИЯ	7
2.1.	ДОСТАВЧИК НА УДОСТОВЕРИТЕЛНИ УСЛУГИ	7
2.2.	ИМЕНУВАНЕ И ИДЕНТИФИКАЦИЯ НА ДОКУМЕНТА	8
2.3.	УЧАСТНИЦИ В УСЛУГАТА ЗА ОТДАЛЕЧЕНО ПОДПИСВАНЕ	8
2.3.1.	Удостоверяващ орган	8
2.3.2.	Платформата за облачни квалифицирани удостоверения и отдалечено подписване и подпечатване на електронни документи - Infonotary QRSS	9
2.3.3.	Потребител	9
2.3.4.	Доверяващи се страни	10
2.3.5.	Трета страна	10
2.4.	УПОТРЕБА НА УДОСТОВЕРЕНИЯТА	11
2.4.1.	Типове удостоверения	11
2.4.2.	Приложимост, употреба и достъпност на услугата за отдалечено подписване/подпечатване на електронни документи	12
2.4.3.	Ограничения на удостоверителното действие	12
2.5.	УПРАВЛЕНИЕ НА УДОСТОВЕРИТЕЛНАТА ПОЛИТИКА НА ДОСТАВЧИКА	12
2.6.	ТЕРМИНИ И СЪКРАЩЕНИЯ	13
3.	ЗАДЪЛЖЕНИЯ ЗА ПУБЛИКУВАНЕ И ПОДДЪРЖАНЕ НА РЕГИСТРИ	17
4.	ИДЕНТИФИКАЦИЯ И АВТЕНТИКАЦИЯ	17
5.	ОПЕРАТИВНИ УСЛОВИЯ	17
5.1.	ИЗТЕГЛЯНЕ НА МОБИЛНОТО ПРИЛОЖЕНИЕ INFONOTARY SIGNZONE	17
5.2.	ИЗДАВАНЕ НА КВАЛИФИЦИРАНОТО УДОСТОВЕРЕНИЕ ЗА АУТЕНТИКАЦИЯ НА МОБИЛНО УСТРОЙСТВО	18
5.2.1.	Действия на удостоверяващия орган при издаване на Удостоверение	18
5.3.	ПРИЕМАНЕ И ПУБЛИКУВАНЕ НА УДОСТОВЕРЕНИЕ	18
5.3.1.	Приемане на удостоверението	18
5.3.2.	Публикуване на удостоверението	18
5.4.	ПОДНОВЯВАНЕ НА УДОСТОВЕРЕНИЕТО	18
5.5.	ПОДМЯНА НА КЛЮЧ В УДОСТОВЕРЕНИЕ И МОДИФИКАЦИЯ НА УДОСТОВЕРЕНИЕ	18
5.6.	ПРЕКРАТЯВАНЕ НА УДОСТОВЕРЕНИЕ	18
5.6.1.	Период, през който Удостоверяващият орган трябва да обслужи заявката за прекратяване	19
5.6.2.	Списък с прекратени удостоверения	19
5.7.	СПИРАНЕ И ВЪЗОБНОВЯВАНЕ НА УДОСТОВЕРЕНИЕ	19
6.	УСЛУГА ЗА ОТДАЛЕЧЕНО ПОДПИСВАНЕ	19
6.1.	ОБЩА ХАРАКТЕРИСТИКА И ОПИСАНИЕ	19
6.2.	ФУНКЦИОНАЛЕН МОДЕЛ ЗА СЪЗДАВАНЕ НА ПОДПИС	20
6.3.	АКТИВИРАНЕ НА УСЛУГАТА ЗА ОТДАЛЕЧЕНО ПОДПИСВАНЕ	21
6.4.	ИЗПОЛЗВАНЕ НА УСЛУГАТА ЗА ОТДАЛЕЧЕНО ПОДПИСВАНЕ	21
7.	КОНТРОЛ НА ОБОРУДВАНЕТО, ПРОЦЕДУРИТЕ И УПРАВЛЕНИЕТО	22
7.1.	ФИЗИЧЕСКИ КОНТРОЛ	22
7.1.1.	Разположение и конструкция на помещенията	22
7.1.2.	Физически достъп	22
7.1.3.	Електрическо захранване и климатични условия	23
7.1.4.	Наводнение	23
7.1.5.	Противопожарно известяване и защита	23
7.1.6.	Средства за съхранение на данни	23
7.1.7.	Извеждане от употреба на технически компоненти	23

7.1.8.	Дублиране на компоненти	23
7.2.	ПРОЦЕДУРЕН КОНТРОЛ	23
7.2.1.	Длъжности и функции	23
7.2.2.	Брой на служителите за определена задача.....	23
7.2.3.	Идентификация и автентификация за всяка длъжност	23
7.2.4.	Изисквания за разделяне на отговорностите при отделните функции	24
7.3.	КОНТРОЛ НА ПЕРСОНАЛА, КВАЛИФИКАЦИЯ И ОБУЧЕНИЕ	24
7.3.1.	Изисквания към независими доставчици	24
7.3.2.	Документация, предоставена на служителите.....	24
7.4.	ПРОЦЕДУРИ ПО ИЗГОТВЯНЕ И ПОДДЪРЖАНЕ НА ЖУРНАЛ НА ДАННИ ОТ ПРОВЕРКИ.....	24
7.4.1.	Честота на създаване на записи	24
7.4.2.	Период на съхранение на записите.....	24
7.4.3.	Защита на записите.....	24
7.4.4.	Процедура за създаване на резервни копия на записите.....	24
7.5.	АРХИВ	24
7.5.1.	Видове архиви.....	25
7.5.2.	Период на съхранение.....	25
7.5.3.	Защита на архива	25
7.5.4.	Процедури по възстановяване на архива	25
7.5.5.	Изисквания за удостоверяване на дата и час на записи	25
7.5.6.	Съхраняване на архива.....	25
7.5.7.	Процедури за придобиване и проверка на информация от архив	25
7.6.	ПРОМЯНА НА КЛЮЧ НА УДОСТОВЕРЕНИЕ	25
7.7.	КОМПРОМЕТИРАНЕ НА КЛЮЧОВЕ И ВЪЗСТАНОВЯВАНЕ СЛЕД БЕДСТВИЯ И НЕПРЕДВИДЕНИ СЛУЧАИ.....	25
7.8.	ПРОЦЕДУРИ ПО ПРЕКРАТЯВАНЕ ДЕЙНОСТТА НА ДОСТАВЧИКА	26
7.8.1.	Прекратяване на дейността	26
7.8.2.	Прехвърляне на дейността на друг квалифициран доставчик на квалифицирани удостоверителни услуги	26
7.8.3.	Отнемане на квалифицирания статут на Доставчика.....	26
8.	КОНТРОЛ НА ТЕХНИЧЕСКАТА СИГУРНОСТ	26
8.1.	ГЕНЕРИРАНЕ И ИНСТАЛАЦИЯ НА ДВОЙКА КЛЮЧОВЕ	26
8.1.1.	Генериране на двойка ключове	26
8.1.2.	Доставка на частния ключ	27
8.1.3.	Доставка на публичния ключ	27
8.1.4.	Доставка на Публичния ключ на Удостоверяващия орган до доверяващите се страни	27
8.1.5.	Дължина на ключовете.....	27
8.2.	ЗАЩИТА НА ЧАСТНИЯ КЛЮЧ И ТЕХНИЧЕСКИ КОНТРОЛ НА КРИПТОГРАФСКИЯ МОДУЛ.....	27
8.2.1.	Стандарти на криптографския модул	27
8.2.2.	Контрол на съхранението и ползването на частен ключ.....	27
8.2.3.	Съхранение на частните ключове	27
8.2.4.	Архивиране на частните ключове	27
8.2.5.	Прехвърляне на частните ключове в и от криптографския модул.....	27
8.2.6.	Активиране и деактивиране на частни ключове	28
8.2.7.	Унищожаване на Частните ключове.....	28
8.3.	ДРУГИ АСПЕКТИ ОТ УПРАВЛЕНИЕТО НА ДВОЙКАТА КЛЮЧОВЕ.....	29
8.3.1.	Архивиране на Публичен ключ	29
8.3.2.	Период на валидност на удостоверение и период на употреба на двойката ключове.....	29
8.4.	ДАННИ ЗА АКТИВИРАНЕ.....	29
8.5.	КОНТРОЛ НА КОМПЮТЪРНАТА СИГУРНОСТ	29
8.6.	ТЕХНИЧЕСКИ КОНТРОЛ И ЖИЗНЕН ЦИКЪЛ	29
8.7.	КОНТРОЛ НА СИГУРНОСТТА НА МРЕЖАТА	29
9.	ПРОФИЛИ	30
9.1.	Профил на удостоверение за аутентикация на мобилно устройство InfoNotary Mobile Device Authentication CP	30

10. ПРОВЕРКА И КОНТРОЛ НА ДЕЙНОСТТА.....	31
10.1. РЕГУЛЯРНА ИЛИ ОБСТОЯТЕЛСТВЕНА ПРОВЕРКА	31
10.2. КВАЛИФИКАЦИЯ НА ПРОВЕРЯВАЩИТЕ ЛИЦА	31
10.3. ВРЪЗКА МЕЖДУ ПРОВЕРЯВАЩИТЕ ЛИЦА И ПРОВЕРЯВАНАТА ОРГАНИЗАЦИЯ	31
10.4. ОБХВАТ НА ПРОВЕРКАТА	32
10.5. ПРЕДПРИЕМАНЕ НА ДЕЙСТВИЯ ЗА ОТСТРАНЯВАНЕ НА НЕДОСТАТЪЦИТЕ	32
11. ДРУГИ БИЗНЕС И ПРАВНИ УСЛОВИЯ	32
11.1. ЦЕНИ И ТАКСИ	32
11.1.1. Възнаграждения по Договор за квалифицирани удостоверителни услуги	32
11.1.2. Фактуриране	32
11.1.3. Политика за връщане на удостоверението и възстановяване на плащането	32
11.2. ФИНАНСОВИ ОТГОВОРНОСТИ.....	32
11.3. ЗАСТРАХОВКА НА ДЕЙНОСТТА.....	32
11.4. Застрахователно покритие за крайните потребители	32
11.5. КОНФИДЕНЦИАЛНОСТ НА ИНФОРМАЦИЯТА.....	33
11.5.1. Обхват на конфиденциалната информация	33
11.5.2. Информация извън обхвата на конфиденциалната информация.....	33
11.5.3. Задължение за защита на конфиденциалната информация	33
11.6. ПОВЕРИТЕЛНОСТ НА ЛИЧНИТЕ ДАННИ.....	33
11.7. ПРАВА ВЪРХУ ИНТЕЛЕКТУАЛНАТА СОБСТВЕНОСТ	33
11.8. ЗАДЪЛЖЕНИЯ, ОТГОВОРНОСТ И ГАРАНЦИИ НА ДОСТАВЧИКА.....	34
11.8.1. Задължения, отговорност и гаранции на Доставчика.....	34
11.8.2. Гаранции и отговорност на Регистриращия орган.....	34
11.8.3. Задължения и отговорности на Титулярите на СЕИ	34
11.8.4. Задължения и отговорности на Третите страни.....	35
11.9. ОТКАЗ ОТ ОТГОВОРНОСТ	35
11.10. ОГРАНИЧЕНИЕ НА ОТГОВОРНОСТТА	35
11.11. КОМПЕНСАЦИИ ЗА ДОСТАВЧИКА	35
11.12. СРОК И ПРЕКРАТЯВАНЕ	36
11.12.1. Срок.....	36
11.12.2. Прекратяване	36
11.12.3. Ефект от прекратяването.....	36
11.13. ИНДИВИДУАЛНО УВЕДОМЯВАНЕ И КОМУНИКАЦИЯ МЕЖДУ УЧАСТНИЦИТЕ	36
11.14. ПРОМЕНИ.....	36
11.15. РЕШАВАНЕ НА СПОРОВЕ И ПОДСЪДНОСТ	36
11.16. ПРИЛОЖИМО ПРАВО	36
11.17. СЪОТВЕТСТВИЕ С ПРИЛОЖИМОТО ПРАВО	36
11.18. ДРУГИ РАЗПОРЕДБИ	37

1. ВЪВЕДЕНИЕ

1.1. КОНЦЕПЦИЯ НА СЪЗДАВАНЕ НА ЕЛЕКТРОНЕН ПОДПИС/ПЕЧАТ ОТ РАЗСТОЯНИЕ (ОТДАЛЕЧЕНО ПОДПИСВАНЕ/ПОДПЕЧАТВАНЕ С ОБЛАЧЕН КЕП). ЗАКОНОСЪОБРАЗНОСТ И ПРАВНА СИЛА.

Регламент (ЕС) № 910/2014 г. урежда възможността за създаване на квалифицирани електронни подписи от разстояние (отдалечено подписване), когато:

а) средата на създаване на квалифициран електронен подпис, т.е. устройството за създаване на квалифициран електронен подпис се управлява от Доставчик на квалифицирани удостоверителни услуги от името на Титуляря на електронния подпис/Създателя на електронния печат; б) при създаването му са изпълнени изискванията за криптографска сигурност за квалифициран електронен подпис; и в) Титуляря/Създателя на печат единствен има контрол („sole control“) върху използването на своите данни за създаване на квалифициран електронен подпис/печат, т.е. данните за активиране на частния си ключ. Създаденият квалифициран електронен подпис/печат по описания начин (чрез устройство за създаване на електронен подпис от разстояние) отговаря на изискванията на Регламент (ЕС) № 910/2014 г. за квалифициран електронен подпис, който има правната сила на саморъчния подпис.

В този смисъл „Инфонотари“ ЕАД (Инфонотари/Доставчик) като доставчик на квалифицирани удостоверителни услуги, предоставя услуга за отдалечено подписване/подпечатване на електронни документи (Услуга за отдалечено подписване/Услугата//Услуга за ОП), като изпълнява изискванията на Регламент (ЕС) № 910/2014г., приложимите към него европейски и международни стандарти и националното законодателство.

Доставчикът е внедрил и прилага специфични, сигурни и надеждни процедури за управление на физическата и административната сигурност, използва сигурни и надеждни системи и продукти, включително надеждна среда за създаване на квалифициран електронен подпис от разстояние и гарантира, че тази среда е използвана единствено под контрола на Титуляря на този подпис.

1.2. ПРЕДМЕТ

Основната цел на настоящия документ ПОЛИТИКА И ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА УСЛУГА ЗА ОТДАЛЕЧЕНО ПОДПИСВАНЕ И ПОДПЕЧАТВАНЕ НА ЕЛЕКТРОННИ ДОКУМЕНТИ на Доставчика на удостоверителни услуги ИНФОНОТАРИ ЕАД (ИНФОНОТАРИ/Доставчик) е да опише и направи публични:

- условията и правилата, които ИНФОНОТАРИ е въвело и изпълнява при предоставяне на услугата за отдалечено подписване/подпечатване на електронни документи;
- приложимостта и ограниченията при използването на Услугата.
- конкретните оперативни процедури, които ИНФОНОТАРИ следва, при

предоставяне на Услугата;

- средства за установяване на съответствието на дейността на Доставчика, включително нейната надеждност и сигурност, с разпоредбите и изискванията на Регламент (ЕС) 910/2014 и изискванията на приложимото българско законодателство.

Настоящият документ допълва и следва да се чете заедно с публикуваните актуални версии на документите на адрес: <https://www.infonotary.com> „Практика при предоставяне на квалифицирани удостоверителни услуги“, „Политика за предоставяне на квалифицирано удостоверение за квалифициран електронен подпис“, „Политика за предоставяне на квалифицирано удостоверение за квалифициран електронен печат“, „Политика и практика при предоставяне на услуга по отдалечена видео идентификация“ на ИНФОНОТАРИ ЕАД, които съдържат общите условия и изисквания към процедурите при идентификация, издаване, управление и използване на квалифицирани удостоверения за квалифициран електронен подпис/печат, изискванията за сигурност и генериране и съхранение на двойка ключове (частен и публичен) за тези удостоверения, както и тяхната приложимост.

В тази връзка, на някои места в текста, неизчерпателно са посочени референции към съответните части на цитираните в предходното изречение документи.

Настоящата „Политика и Практика при предоставяне на услуга за отдалечено подписване и подпечатване на електронни документи“ е публичен документ и може да бъде променян при необходимост, като всяка промяна в него е публично достъпна от всички заинтересувани лица на адрес: <https://www.infonotary.com> .

1.3. СЪОТВЕТВИЕ

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

- Регламент 910/2014 на Европейския парламент и Съвет относно удостоверителните услуги и се позовава на информация, относно подготвяните в съответствие с този Регламент международни препоръки, спецификации и стандарти;
- РЕГЛАМЕНТ (ЕС) 2024/1183 на Европейския парламент и на Съвета за изменение на Регламент (ЕС) № 910/2014 по отношение на създаването на европейска рамка за цифрова самоличност;
- Закон за електронния документ и електронните удостоверителни услуги;
- 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);
- ETSI EN 319 401 v2.1.1 General Policy Requirements for Trust Service Providers;

- ETSI EN 319 411 Policy and security requirements for Trust Service Providers issuing certificates;
- CEN EN 419 241-1 „Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements“;
- CEN EN 419 241-2 „Trustworthy Systems Supporting Server Signing - Part 2: Protection profile for QSCD for Server Signing“;
- ETSI TS 119 431-1/2 - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers;
- Part 1: TSP service components operating a remote QSCD /SCDev;
- Part 2: TSP service components supporting AdES digital signature creation
- ETSI TS 119 432 - Electronic Signatures and Infrastructures (ESI); Protocols for remote digital signature creation
- IETF RFC 3647 „Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.

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

2. ОСНОВНИ ПОЛОЖЕНИЯ

2.1. 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 в съответствие с разпоредбите на Регламент № (ЕС) 910/2014 и националното право.

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

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

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

- Услуги по издаване и управление на квалифицирани удостоверения за квалифициран и усъвършенстват електронен подпис и печат;
- Услуги по издаване и управление на квалифицирани удостоверения автентичност на уебсайт;
- Услуги по издаване и управление на квалифицирани електронни времеви печати;

- Услуги по издаване и управление на квалифицирани PSD2 удостоверения;
- Услуги за валидиране на квалифицирани удостоверения, квалифициран електронен подпис и квалифициран електронен печат:
 - предоставяне на услуги за проверка в реално време на статуса на издадено от ИНФОНОТАРИ квалифицирано удостоверение (OCSP);
 - предоставяне на услуги за проверка в реално време на статуса на квалифицирано удостоверение, квалифициран електронен подпис и квалифициран електронен печат (InfoNotary Qualified Validation Service - IQVS).
- Услуги за квалифицирано отдалечено подписване на електронни документи;
- Квалифицирана на национално ниво услуга за отдалечена видео идентификация;
- Квалифицирана на национално ниво удостоверителна услуга за електронна идентификация, включваща услуга за издаване и управление на средства за електронна идентичност и услуга за динамично удостоверяване на автентичност на електронна идентичност.

При осъществяване на дейностите и предоставяне на квалифицирани удостоверителни услуги, ИНФОНОТАРИ ЕАД прилага внедрените в дружеството Система за управление, сертифицирана по стандарта ISO80/IEC 9001:2008 и Система за управление сертифицирана по стандарта ISO/IEC 27001:2013.

2.2. ИМЕНУВАНЕ И ИДЕНТИФИКАЦИЯ НА ДОКУМЕНТА

Документът „Политика и Практика при предоставяне на услуга за отдалечено подписване и подпечатване на електронни документи“, се именува **“InfoNotary Qualified Remote Signing Service (QRSS) CP_CPS”** и се идентифицира посредством следния идентификатор на обект (OID): **1.3.6.1.4.1.22144.3.10**, който отговаря на **EU SSASC Policy (OID 0.4.0.19431.1.1.3)**, в съответствие с ETSI TS 119 431-1.

2.3. УЧАСТНИЦИ В УСЛУГАТА ЗА ОТДАЛЕЧЕНО ПОДПИСВАНЕ

2.3.1. Удостоверяващ орган

В съответствие с т. 1.3.1. от документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги“.

Оперативните удостоверяващи органи имащи отношение към Услугата са:

- Оперативен удостоверяващ орган за издаване на квалифицирани удостоверения за квалифициран електронен подпис на физически лица **InfoNotary Qualified Personal Sign CA**;
- Оперативен удостоверяващ орган за издаване на удостоверения за квалифициран електронен печат за юридически лица **InfoNotary Qualified Legal Person Seal CA**;

- Оперативен удостоверяващ орган за издаване на оперативното удостоверение за аутентикация на устройства **InfoNotary Device Authentication CA.**

Оперативните условия и предназначението на споменатите удостоверяващи органи са в съответствие с т. 1.3.1, и т. 1.4.1. от „Практика при предоставяне на квалифицирани удостоверителни услуги“ и в съответствие със съответните удостоверителни политики на ИНФОНОТАРИ.

2.3.2. Платформата за облачни квалифицирани удостоверения и отдалечено подписване и подпечатване на електронни документи - Infonotary QRSS

Платформата за облачни квалифицирани удостоверения (Облачен КЕП/КЕПечат) и отдалечено подписване и подпечатване на електронни документи **Infonotary QRSS** (Платформа), която осигурява функционалностите по:

- генериране и сигурно съхранение по възлагане от Титуляр/Създател на печат на двойка публичен и частен ключ от асиметрична криptosистема посредством отдалечено устройство за създаване на подпис/печат InfoNotary Remote Qualified Signature Creation Device (RQSCD), което е обособена част от инфраструктурата на Доставчика;
- удостоверяване на Титуляря/Създателя на печат, за да му бъде разрешено използването на ключа за подписване;
- удостоверено управление и ползване на криптографските ключове в RQSCD, единствено под контрола на Титуляря/Създателя на печат за създаване на електронен подпис от разстояние или на електронен печат от разстояние към представен в Платформата електронен документ.

Платформата се състои от:

- отдалечена сървърна система, част от инфраструктурата на Доставчика, включваща и устройство за създаване на подпис от разстояние (SSA, SAM+HSM). ИНФОНОТАРИ използва сертифицирани в съответствие с изискванията на Регламент 910/2014 криптографски модули (SAM,HSM).
- Мобилно приложение InfoNotary SignZone или уеб интерфейс на информационна система на Доставчика или трета страна за активиране създаването Облачния КЕП/КЕПечат.

2.3.3. Потребител

Потребител свързан с ключа за подписване/подпечатване може да бъде:

- Физическо лице или физическо лице, в качеството му на упълномощен представител на друго физическо лице, на упълномощен представител на юридическо лице или организация или в качеството му на законен представител на юридическо лице или организация (Титуляр на електронен подпис/Създател на електронен печат);

- устройство или система, управлявана от или от името на физическо или юридическо лице.

Услугата за отдалечено подписване може да се ползва от Потребители, които:

- имат изтеглено и инсталирано мобилно приложение Infonotary SingZone/ мобилно приложение на трета страна с интегриран в него InfoNotary Mobile SDK на мобилно смарт устройство, което е единствено под техен контрол или използват уеб интерфейс на информационна система на Доставчика или трета страна;
- приемат условията на настоящия документ, Практиката за предоставяне на квалифицирани удостоверителни услуги на Доставчика, Общите условия за ползване на приложението и Политика за поверителност и защита на личните данни;
- използват и пазят от компрометиране частните и публичните ключове, както и средствата за достъп до тях и за тяхното активиране (ПИН кодове, пароли и др.), съгласно определеното в настоящия документ и „Практика при предоставяне на квалифицирани удостоверителни услуги“ на Доставчика.

2.3.4. Доверяващи се страни

Доверяваща се страна означава физическо или юридическо лице/организация, което разчита на предоставената от Доставчика удостоверителна услуга за отдалечено подписване с електронен подпис/печат.

Доверяващите се страни следва да имат умения да ползват удостоверения за електронен подпис/печат, като се доверяват на издадени от Доставчика квалифицирани удостоверения само след проверка на статуса и валидността на квалифицираните удостоверения, в регистрите на Доставчика.

Доверяващите се страни, могат да разчитат на надеждно, сигурно, лесно и удобно квалифицирано валидиране по автоматизиран начин на квалифицирани електронни подписи/печати, удостоверенията, които са издадени от ИНФОНОТАРИ.

2.3.5. Трета страна

Трета страна е отделно от Доставчика юридическо лице, организация, административен орган, орган на местно самоуправление, което се доверява на удостоверителните услуги на Инфонотари ЕАД и ползва за собствени цели услугата за отдалечено подписване.

Третите страни имат достъп до услугата за електронна идентификация след подписване на индивидуален договор с Доставчика, интеграция с Платформата за електронна идентификация на ИНФОНОТАРИ и определяне на данните за физическите лица, юридическите лица и организации, които ще се предоставят от ИНФОНОТАРИ, при ползване на съответните електронни услуги.

Третите страни следва да използват валидно квалифицирано удостоверение за автентичност на уеб сайт (SSL удостоверение), което ще се използва за автентикация

на Третата страна при използване на Услугата за електронна идентификация.

2.4. УПОТРЕБА НА УДОСТОВЕРЕНИЯТА

2.4.1. Типове удостоверения

В рамките на настоящата Политика и практика, издаваните от Доставчика, квалифицирани удостоверения на крайни потребители (Титуляри) имащи отношение към Услугата са: квалифицираното удостоверение за квалифициран електронен подпис (вкл. облачен квалифициран електронен подпис) на физическо лице **InfoNotary Qualified Natural Person Signature**, квалифицирано удостоверение за квалифициран електронен подпис на физическо лице с делегирани правомощия **InfoNotary Qualified Delegated Signature Certificate**, квалифицираното удостоверение за електронен печат (вкл. облачен квалифициран електронен печат) на юридическо лице **InfoNotary Qualified Legal Person Seal CP**, облачни квалифицирани удостоверения **InfoNotary Qualified eID CP** и **InfoNotary Qualified Company eID CP** за Титуляр на средство за електронна идентификация.

Предназначението и оперативните условия за издаване и управление на споменатите квалифицирани удостоверения са в съответствие с т. 3 и т. 4 от „Политика за предоставяне на квалифицирано удостоверение за квалифициран електронен подпис“, „Политика за предоставяне на квалифицирано удостоверение за квалифициран електронен печат“ и т. 1.4.1.2.1, т. 3 и т. 4 от „Практика при предоставяне на квалифицирани удостоверителни услуги“ на ИНФОНОТАРИ.

За осигуряване на сигурност и надеждност на функционалностите и услугите, предоставяни отдалечено (през мобилното приложение InfoNotary SignZone, уеб интерфейс на Доставчика или интегрирани системи, мобилни приложения или уеб портал на трети страни), Доставчикът въвежда използване на квалифицирано удостоверение за автентикация на уебсайт и квалифицирано удостоверение за автентикация на мобилно устройство **InfoNotary Mobile Device Authentication Certificate**.

Доставчикът издава **InfoNotary Mobile Device Authentication Certificate** на удостоверен Потребител, с инсталирано мобилно приложение Infonotary SignZone. Удостоверението се издава на физическо лице, притежател/ползвател на мобилно устройство с уникален идентификатор, който е вписан в него и може да бъде използвано за удостоверяване на автентичността на мобилното устройство пред информационни системи, интернет приложения, при извършване на защитена и криптирана комуникация и извършване на дейности по гарантиране на произхода на електронни данни и информация, които са достъпни през мобилното приложение Infonotary SingZone, на Доставчика. Квалифицираното удостоверение може да съдържа и специфични атрибути, осигуряващи необходимата информация за идентификация на устройството.

2.4.2. Приложимост, употреба и достъпност на услугата за отдалечено подписване/подпечатване на електронни документи

Услугата може да се използва от потребители (физически лица в лично качество или като законни/упълномощени представители на юридическо лице), които са Титуляри/Създатели на печат на валидно облачно квалифицирано удостоверение за квалифициран електронен подпис/печат (облачен КЕП/облачен КЕПечат), издадено и поддържано от ИНФОНОТАРИ ЕАД.

Услугата за отдалечено подписване може да се използва чрез мобилното приложение на Доставчика – InfoNotary SignZone или чрез уеб интерфейс на информационна система на Доставчика или трета страна (например финансова, застрахователна институция и др.), която е сключила договор/споразумение с ИНФОНОТАРИ и има интеграция с Платформата за облачни квалифицирани удостоверения и отдалечено подписване и подпечатване на електронни документи на Доставчика.

Когато е практически осъществимо Доставчикът 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.

2.4.3. Ограничения на удостоверителното действие

Услугата за отдалечено подписване не трябва да се използва по начин, който нарушава поверителността и сигурността на личните данни.

Доставчикът не носи отговорност за вреди, настъпили в следствие на:

- ползването на Услугата за отдалечено подписване, извън разрешената употреба и съобразно ограниченията на приложение по отношение на нейното предназначение и ще доведе до анулиране на гаранциите, които ИНФОНОТАРИ дава на потребителите и на Доверяващите се страни.
- случайни събития, имащи характера на непреодолима сила, включително злоумишлени действия на трети лица.

2.5. 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, който е публично достъпен на адрес: <https://www.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
e-mail: legal@infonotary.com

2.6. ТЕРМИНИ И СЪКРАЩЕНИЯ

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.

Доставчик на услуга, прилагащ/използващ приложение за сървърно подписване/подписване от разстояние(SSASP)

Доставчик на квалифицирани удостоверителни услуги управляващ компонент на приложението за подписване на сървър/подписване от разстояние

Данни за идентификация на лица

Набор от данни, които позволяват да се установи самоличността на физическо или юридическо лице, или на физическо лице, представляващо юридическо лице

Данни за създаване на електронен подпис

Уникални данни, които се използват от Титуляря на електронния подпис за създаването на електронен подпис

Доверяваща се страна

Физическо или юридическо лице, което разчита на електронна идентификация или удостоверителна услуга

Достоверен източник

Всеки източник, независимо от неговата форма, на който може да се разчита за предоставяне на точни данни, информация и/или доказателства/факти, които могат да се използват, за да се докаже самоличността

Електронна идентификация

Процес на използване на данни в електронна форма за идентификация на лица, които данни представляват по уникален начин дадено физическо или юридическо лице, или физическо лице, представляващо юридическо лице

Електронна идентичност

Съвкупност от характеристики, записани в електронна форма, въз основа на които може да се направи еднозначно разграничаване на едно лице от други лица във виртуалната среда с цел осигуряване на достъп до информационни системи или осигуряване на възможност за извършване на електронни изявления.

Заявител/Потребител	Лице (юридическо или физическо), чиято самоличност трябва да бъде потвърдена
Квалифицирана удостоверителна услуга	Удостоверителна услуга, която отговаря на приложимите изисквания, определени в Регламент (ЕС) № 910/2014 г.
Компонент на услугата за подписване на сървър (SSASC)	Компонент на услугата на Доставчика, използващ приложение за подписване на сървър за създаване на стойност на цифров подпис от името на подписващ
Модул за активиране на подпис (SAM)	Сигурен софтуерен елемент разположен, в защитена от неправомерен достъп среда, в инфраструктурата на Доставчика, който осигурява едноличен контрол на Титуляря върху използването на данните за създаване на електронен подпис/печат при ползване на услуга отдалечено подписване, и който отговаря на изискванията на РЕГЛАМЕНТ (ЕС) № 910/2014.
Отдалечено устройство за създаване на подпис	Устройство за създаване на подпис, използвано дистанционно от гледна точка на подписващия и осигурява контрол на операцията по подписване от името на подписващия
Отдалечена видео идентификация/Онбординг процес	Процес на проверка на самоличността, при който заявителя/потребителя е физически отдалечен от местоположението, където се извършва проверката на самоличността
Платформа за облачни квалифицирани удостоверения и отдалечено подписване и подпечатване на електронни документи	Обособена част от удостоверителната инфраструктура на Доставчика, която отговаря на изискванията, предвидени в приложение II Регламент (ЕС) № 910/2014, и чрез която се генерират, съхраняват и управляват данните за създаване на облачен квалифициран електронен подпис/печат от Доставчика, по възлагане от Титуляря на електронния подпис или Създателя на електронния печат.
Регламент	РЕГЛАМЕНТ (ЕС) № 910/2014 НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА от 23 юли 2014 година относно електронната идентификация и удостоверителните услуги при електронни трансакции на вътрешния пазар и за отмяна на Директива 1999/93/ЕО.
Регламент GDPR	Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните)

Стойност на цифровия подпис	Резултат от криптографската трансформация на единица данни, която ги защитава срещу фалшифициране и позволява на получателя на единицата данни да докаже източника и целостта на тези данни
Средство за електронна идентификация	Материална и/или нематериална единица, която съдържа данни за идентификация на лица, която се използва за удостоверяване на автентичност за онлайн услуга.
Създател на електронен печат	Юридическо лице, което създава електронни печати и е вписано в удостоверението за електронен печат като такъв
Връзка/препратка към средство за електронна идентификация	Данни, използвани в SSASC като връзка/препратка към средство за електронна идентификация за удостоверяване на подписващия
Титуляр на електронен подпис	Означава физическо лице, което създава електронен подпис
Удостоверителна услуга	Електронна услуга, обикновено предоставяна срещу възнаграждение, която се състои в: <ul style="list-style-type: none">- създаването, проверката и валидирането на електронни подписи, електронни печати или електронни времеви печати, услуги за електронна препоръчана поща, както и удостоверения, свързани с тези услуги; или- създаването, проверката и валидирането на удостоверения за автентичност на уебсайт; или- съхраняването на електронни подписи, печати или удостоверения, свързани с тези услуги.
Устройство за създаване квалифициран на електронен подпис (SCDev)	Конфигуриран софтуер или хардуер, който се използва за създаването на електронен подпис, и който отговаря на изискванията, предвидени в приложение II на РЕГЛАМЕНТ (ЕС) № 910/2014

Отдалечено устройство за създаване на квалифициран електронен подпис/печат (RQSCD)

Устройство за създаване на електронен подпис/печат, което отговаря на изискванията, предвидени в приложение II Регламент (ЕС) № 910/2014, което е обособена част от инфраструктурата на Доставчика, използвано дистанционно от гледна точка на подписващия и осигуряващо контрол върху операцията по подписване от името на подписващия

Облачно удостоверение за квалифициран електронен подпис/електронен печат

Квалифицирано удостоверение за електронен подпис, което се издава от доставчик на квалифицирани удостоверителни услуги на отдалечено устройство за създаване на квалифициран електронен подпис/печат

СЪКРАЩЕНИЯ

ДКУУ	Доставчик на квалифицирани удостоверителни услуги
CP	Certificate Policy Политика за предоставяне на удостоверителни услуги
CPS	Certification Practice Statement Практика при предоставяне на удостоверителни услуги
ETSI	European Telecommunications Standards Institute Европейски институт за телекомуникационни стандарти
EU	European Union - Европейски съюз
ISO	International Standardization Organization Международна организация за стандартизация
OID	Object Identifier Идентификатор на обект
PKI	Public Key Infrastructure Инфраструктура на публичния ключ
eID	Electronic Identification
EUSCP	EU SSASC Policy
NCP	Normalized Certificate Policy
NSCP	Normalized SSASC Policy
SCDev	Signature Creation Device
SCP	SSASC Policy

SSASC	Server Signing Application Service Component
SSASP	Server Signing Application Service Provider
QSCD	Qualified electronic Signature/Seal Creation Device

3. ЗАДЪЛЖЕНИЯ ЗА ПУБЛИКУВАНЕ И ПОДДЪРЖАНЕ НА РЕГИСТРИ

В съответствие с т. 2 от документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги“.

4. ИДЕНТИФИКАЦИЯ И АВТЕНТИКАЦИЯ

При първоначалната идентификация и потвърждаване на самоличността потребителите, Титуляри на облачните квалифицирани удостоверения посочени в т.2.4.1, Доставчикът следва правилата и условията определени в т. 3 на документа „Практика при предоставяне на квалифицирани удостоверителни услуги“ и в т. 4.2.1 на документа „Политика и практика при предоставяне на квалифицирана на национално ниво услуга за отдалечена видео идентификация“ на ИНФОНОТАРИ.

5. ОПЕРАТИВНИ УСЛОВИЯ

Оперативните дейности при предоставяне на Услуга за отдалечено подписване/подпечатване включват: осигуряване на достъп за изтегляне на Мобилното приложение InfoNotary SignZone, удостоверяване на Потребителя (Титуляря/Създателя на печат) за активиране на частния ключ за създаване на квалифициран електронен подпис/печат, създаване на квалифициран електронен подпис от разстояние по заявка на Титуляря/Създателя на печат.

Доставчикът прилага оперативните правила и процедури за издаване и управление на облачните квалифицирани удостоверения по т.2.4.1, които са определени в т. 3 на документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги“. В настоящия документ са конкретизирани условията по отношение на издаването и управлението на квалифицираното удостоверение за аутентикация на мобилно устройство InfoNotary Mobile Device Authentication Certificate.

5.1. ИЗТЕГЛЯНЕ НА МОБИЛНОТО ПРИЛОЖЕНИЕ INFONOTARY SIGNZONE

Мобилното приложение InfoNotary SignZone е публикувано в електронните магазини App Store и Google Play и в зависимост от операционната система на ползваното от Потребителя смарт устройство, той може да го изтегли и инсталира.

5.2. ИЗДАВАНЕ НА КВАЛИФИЦИРАНОТО УДОСТОВЕРЕНИЕ ЗА АУТЕНТИКАЦИЯ НА МОБИЛНО УСТРОЙСТВО

5.2.1. Действия на удостоверяващия орган при издаване на Удостоверение

Оперативният удостоверяващият орган **InfoNotary Device Authentication CA** на Доставчика издава удостоверението, на база на получено искане за издаване от Регистриращия орган.

Доставчикът издава **InfoNotary Mobile Device Authentication Certificate** на всеки Потребител, с инсталирано мобилно приложение Infonotary SignZone, чиято самоличност е потвърдена успешно чрез отдалечена видео идентификация, съгласно т. 4.2. от „Политика и практика при предоставяне на отдалечена видео идентификация“.

5.3. ПРИЕМАНЕ И ПУБЛИКУВАНЕ НА УДОСТОВЕРЕНИЕ

5.3.1. Приемане на удостоверението

Квалифицираното удостоверение за аутентикация на мобилно устройство специфичен идентификатор и атрибути свързани с използваното от Потребителя мобилното устройство. В тази връзка удостоверението не подлежи на приемане от Потребителя.

5.3.2. Публикуване на удостоверението

В съответствие с т. 4.4.2 от документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги“.

5.4. ПОДНОВЯВАНЕ НА УДОСТОВЕРЕНИЕТО

Не се поддържа от Доставчика.

5.5. ПОДМЯНА НА КЛЮЧ В УДОСТОВЕРЕНИЕ И МОДИФИКАЦИЯ НА УДОСТОВЕРЕНИЕ

Не се поддържа от Доставчика.

5.6. ПРЕКРАТЯВАНЕ НА УДОСТОВЕРЕНИЕ

Квалифицираното удостоверение за аутентикация на мобилно устройство се прекратява:

- по искане на Титулярят с изтриване/деактивиране на потребителския профил или прекратяване на сключения договор за Услугата за отдалечено подписване.
- При всеки нов процес на отдалечена видео идентификация, извършен от Потребителя;
- При прекратяване на юридическото лице на Доставчика на квалифицирани

удостоверителни услуги.

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

В съответствие с т. 4.9.4 от документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги“.

5.6.2. Списък с прекратени удостоверения

В съответствие с т. 4.9.6, 4.9.7 и 4.9.8 от документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги“.

5.7. СПИРАНЕ И ВЪЗОБНОВЯВАНЕ НА УДОСТОВЕРЕНИЕ

Не се поддържа от Доставчика.

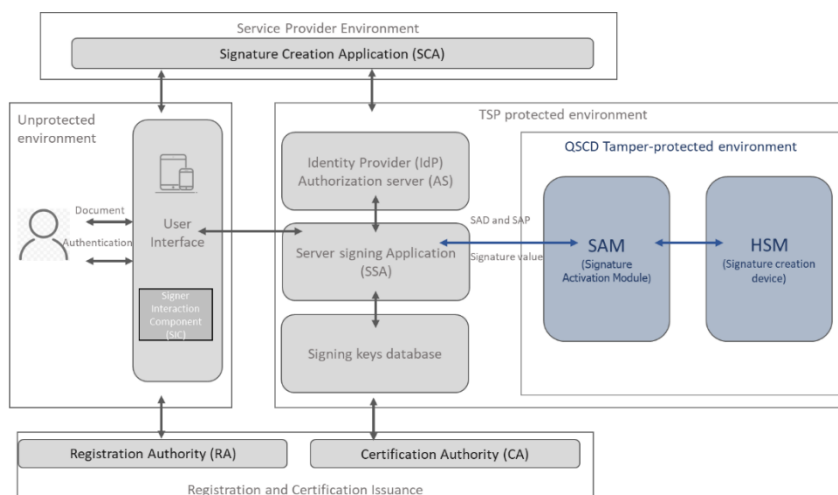
6. УСЛУГА ЗА ОТДАЛЕЧЕНО ПОДПИСВАНЕ

6.1. ОБЩА ХАРАКТЕРИСТИКА И ОПИСАНИЕ

Услугата за отдалечено подписване, предоставяна от ИНФОНОТАРИ, се реализира чрез Платформата **Infonotary QRSS** (Платформа), която отговаря на изисквания за сигурност на стандарт EN 419 241-1 и гарантира, че ключът за подписване/подпечатване на Титуляря/Създателя на печат се използват по предназначение единствено и само под негов контрол.

ИНФОНОТАРИ, в съответствие с ETSI TS 119 432, е реализирал, т.нар. SCAL 2 архитектура на услугата за отдалечено подписване с високо ниво на осигуряване на сигурност на персоналния контрол на ползване ключовете за подписване/подпечатване чрез използване на модул за активиране на подписа (SAM(Signature Activation Module)).

Общата схема на компонентите, интерфейсите и протоколите, осигуряващи специфичните функционалности като част от процеса за създаване на отдалечени квалифицирани електронни подписи/печати, която ИНФОНОТАРИ използва при реализация на услугата е представена на фиг. 1.



Фиг. 1

Схемата показва взаимодействието на основните компоненти SCA и SSA с останалите елементи, участващи в процеса на отдалечено подписване. SCA се състои от приложение за подписване и устройство за създаване на подпис от разстояние. SCA използва отдалеченото устройство за създаване на подпис, за да генерира, поддържа и използва ключовете за подписване под контрола на техните Титуляри/Създатели на печат. SCA е компонентът, който отговаря за създаването на подписа. SCA изпраща към SSA искане за създаване на подпис.

При този модел на реализация, защитената среда на Доставчика се допълва с т.нар. защитената от фалшифициране среда (QSCD Tamper-protected environment). Тя защитава използването на ключове за подписване/подпечатване и управлява активирането на подписа/печата, така че то да бъде единствено под контрола на Титуляря/Създателя на печат. Това се реализира от SAM модула, който осигурява сигурността, поверителността и целостта на ключа за подписване/подпечатване, който може да бъде активиран от SCA. SAM проверява данните за активиране на подписа, за да идентифицира Титуляря/Създателя на печат и да получи неговото разрешение да активира ключа за подписване/подпечатване. При успешна идентификация на Титуляря/Създателя на печат, съответният ключ може да се използва за подписване/подпечатване от името на Титуляря в рамките на определен период от време и/или определен брой подписи. Този процес осигурява висока степен на сигурност, че ключовете за подписване са под контрола единствено на Титуляря. Данните за активиране на подписа се предават в защитена форма директно от персонално устройство (PC, смартфон, таблет, др.) на подписващия до SAM, чрез сигурен/защитен канал, за да се гарантира персонален контрол на Титуляря/Създателя на печат върху ключа за подписа/печат и невъзможност за злоупотреба с този ключ.

Услугите CA/RA, OCSP и CRL, Time Stamp, автентикация и оторизация са външни за услугата.

6.2. ФУНКЦИОНАЛЕН МОДЕЛ ЗА СЪЗДАВАНЕ НА ПОДПИС

Целта на Услугата е създаване на квалифициран електронен подпис от разстояние, който обхваща: а) документа/данните, които ще бъдат изпратени и подписани от Потребителя (подписващия), б) удостоверението, с което се подписва, и в) атрибути в подкрепа на подписа, неговото валидиране и цел. Използваният от Доставчика функционален модел на среда за създаване на подпис от разстояние се състои от:

- Потребител (подписващ), който иска да създаде подпис;
- Мобилно устройство – под контрола на Титуляря/Създателя на печат и активен мобилен телефонен номер, с възможност за получаване на кратки текстови съобщения (SMS);
- Приложение за управление, което представлява средата (напр. мобилно приложение, информационна система), която подписващият използва за

достъп до функционалността за подписване; и

- Платформата **Infonotary QRSS**, която реализира функционалността за подписване.

Квалифицираната услуга за отдалечено подписване позволява създаване на следните формати и профили подписи:

Формат/Профил	BASELINE_B	BASELINE_T	BASELINE_LT	BASELINE_LTA
XAdES	✓	✓	✓	✓
PAdES	✓	✓	✓	✓
ASiCS/ ASiCE	✓	✓	✓	✓
JadES	✓	✓	✓	✓

6.3. АКТИВИРАНЕ НА УСЛУГАТА ЗА ОТДАЛЕЧЕНО ПОДПИСВАНЕ

Активирането на Услугата отдалечено подписване се извършва веднага след издаване на облачното удостоверение за квалифициран електронен подпис/печат.

За да използва Услугата за отдалечено подписване, Титуляря/Създателя на печат е необходимо да е инсталирал Мобилното приложение InfoNotary Mobile и да има създаден ПИН за достъп и подписване с частния ключ към валидно облачно удостоверение за квалифициран електронен подпис/печат.

6.4. ИЗПОЛЗВАНЕ НА УСЛУГАТА ЗА ОТДАЛЕЧЕНО ПОДПИСВАНЕ

Процедурата за създаване на отдалечено подписване/подпечатване на електронни документи е следната:

- Титулярят/Създателят на печат стартира мобилното приложение и въвежда потребителския си код за достъп (ПИН);
- Титулярят/Създателят на печат качва (upload) документи за подписване/изпраща заявка за подписване на електронен документ към Платформата на ИНФОНОТАРИ;
- Титулярят/Създателят на печат преглежда налични в Платформата документи за подписване от него, на които той е адресат и са му изпратени за подпис от трета страна, посредством Платформата;
- След проверка на коректността на потребителския код за достъп (ПИН), всички заявки за създаване на електронен подпис/документи се изтеглят/визуализират в приложението.
- Титулярят/Създателят на печат може да прегледа документа/документите в приложението;

- Ако, Титулярят/Създателят на печат реши да подпише съответните документи, той натиска бутона „Подпиши“ и въвежда персоналният си код за достъп/активиране на частния ключ.
- Ако, Титулярят/Създателят на печат е въвел правилен персонален код за достъп/активиране на частния ключ, тогава с помощта на частния ключ, съхраняван в защитено криптографско устройство RQSCD, Доставчика създава съответния квалифициран електронен подпис и връща/визуализира подписания документ в мобилното приложение.

При ползване на Услугата за отдалечено подписване от трета страна, която има интеграция с Платформата на Доставчика, тя изпраща заявка за подписване на електронен документ към Платформата на ИНФОНОТАРИ. Част от данните, съдържащи се в заявката са данни за идентификация на Титулярят/Създателят на печат, който трябва да подпише документа и самия документ или хеш стойност на документа и др.

Доставчикът уведомява Титуляря/Създателя на печат че има чакащи документи за подпис. За да извърши подписването Титуляря/Създателя на печат изпълнява горе описаните стъпки.

7. КОНТРОЛ НА ОБОРУДВАНЕТО, ПРОЦЕДУРИТЕ И УПРАВЛЕНИЕТО

Услугата за отдалечено подписване се изпълнява от Платформата за облачни квалифицирани удостоверения и отдалечено подписване и подпечатване на електронни документи на Доставчика, която е функционална част от изградената и одитирана, в съответствие с изискванията на Регламента, РКІ инфраструктурата на Доставчика, която се използва за предоставяне на квалифицирани удостоверителни услуги. В тази връзка за управление и оперативен контрол на оборудването, сигурността и дейността му се прилагат правилата и процедурите описани в документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги“. С настоящия документ, където е приложимо, са допълнени част от посочените правила и процедури.

7.1. ФИЗИЧЕСКИ КОНТРОЛ

В съответствие с т. 5.1. от документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги“.

7.1.1. Разположение и конструкция на помещенията

В съответствие с т. 5.1.1 от документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги“.

7.1.2. Физически достъп

В съответствие с т. 5.1.2 от документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги“.

7.1.3. Електрическо захранване и климатични условия

В съответствие с т. 5.1.3 от документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги“.

7.1.4. Наводнение

В съответствие с т. 5.1.4 от документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги“.

7.1.5. Противопожарно известяване и защита

В съответствие с т. 5.1.5 от документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги“.

7.1.6. Средства за съхранение на данни

В съответствие с т. 5.1.6 от документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги“.

7.1.7. Извеждане от употреба на технически компоненти

В съответствие с т. 5.1.7 от документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги“.

7.1.8. Дублиране на компоненти

В съответствие с т. 5.1.8 от документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги“.

7.2. ПРОЦЕДУРЕН КОНТРОЛ

В съответствие с т. 5.2 от документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги“.

7.2.1. Длъжности и функции

В съответствие с т. 5.2.1 от документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги“.

7.2.2. Брой на служителите за определена задача

В съответствие с т. 5.2.2 от документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги“.

7.2.3. Идентификация и автентификация за всяка длъжност

В съответствие с т. 5.2.3 от документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги“.

7.2.4. Изисквания за разделяне на отговорностите при отделните функции

В съответствие с т. 5.2.4 от документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги“.

7.3. КОНТРОЛ НА ПЕРСОНАЛА, КВАЛИФИКАЦИЯ И ОБУЧЕНИЕ

В съответствие с т.5.3 от документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги“.

7.3.1. Изисквания към независими доставчици

В съответствие с т. 5.3.1. от документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги“.

7.3.2. Документация, предоставена на служителите

В съответствие с т. 5.3.2 от документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги“.

7.4. ПРОЦЕДУРИ ПО ИЗГОТВЯНЕ И ПОДДЪРЖАНЕ НА ЖУРНАЛ НА ДАННИ ОТ ПРОВЕРКИ

В съответствие с т. 5.4 от документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги“.

7.4.1. Честота на създаване на записи

В съответствие с т. 5.4.1 от документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги“.

7.4.2. Период на съхранение на записите

В съответствие с т. 5.4.2 от документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги“.

7.4.3. Защита на записите

В съответствие с т. 5.4.3 от документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги“.

7.4.4. Процедура за създаване на резервни копия на записите

В съответствие с т. 5.4.4 от документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги“.

7.5. АРХИВ

В съответствие с т.5.5 от документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги“.

В допълнение, Доставчикът съхранява като вътрешен архив доказателствата от процеса на доказване на самоличността и идентичността на Титулярите и процеса по

удостоверяване на автентичност по начин, който: не позволява подправяне и промяна; гарантира поверителността на информацията; осигурява възможност за търсене, извличане и проверка.

7.5.1. Видове архиви

В съответствие с т.5.5.1. от документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги“.

7.5.2. Период на съхранение

В съответствие с т.5.5.2. от документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги“.

7.5.3. Защита на архива

В съответствие с т.5.5.3. от документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги“.

7.5.4. Процедури по възстановяване на архива

В съответствие с т.5.5.4. от документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги“.

7.5.5. Изисквания за удостоверяване на дата и час на записи

В съответствие с т.5.5.5. от документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги“.

7.5.6. Съхраняване на архива

В съответствие с т.5.5.6. от документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги“.

7.5.7. Процедури за придобиване и проверка на информация от архив

В съответствие с т.5.5.7. от документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги“.

7.6. ПРОМЯНА НА КЛЮЧ НА УДОСТОВЕРЕНИЕ

В съответствие с т.5.6 от документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги“.

7.7. КОМПРОМЕТИРАНЕ НА КЛЮЧОВЕ И ВЪЗСТАНОВЯВАНЕ СЛЕД БЕДСТВИЯ И НЕПРЕДВИДЕНИ СЛУЧАИ

В съответствие с т.5.7.1 и т. 5.7.2 от документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги“.

7.8. ПРОЦЕДУРИ ПО ПРЕКРАТЯВАНЕ ДЕЙНОСТТА НА ДОСТАВЧИКА

7.8.1. Прекратяване на дейността

В съответствие с т.5.8.1 от документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги“.

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

В съответствие с т.5.8.2 от документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги“.

7.8.3. Отнемане на квалифицирания статут на Доставчика

В съответствие с т.5.8.3 от документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги“.

8. КОНТРОЛ НА ТЕХНИЧЕСКАТА СИГУРНОСТ

8.1. ГЕНЕРИРАНЕ И ИНСТАЛАЦИЯ НА ДВОЙКА КЛЮЧОВЕ

В съответствие с т.6.1. от документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги“.

8.1.1. Генериране на двойка ключове

8.1.1.1. Генериране на частен ключ на Удостоверяващия орган на Доставчика

В съответствие с т.6.1.1.1 от документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги“.

8.1.1.2. Генериране на двойка ключове на Абонат

В съответствие с т.6.1.1.2 от документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги“.

Доставчикът винаги генерира двойката ключове на Титуляря/Създателя на печат след успешна идентификация и потвърждаване на неговата самоличност.

Всяка генерирана двойка ключове е уникално свързана с удостоверен клиентския профил на Титуляря/Създателя на печат ползван от услугата за отдалечено подписване.

Когато Доставчикът по възлагане от Титуляря/Създателя на печат генерира двойката ключове, частният ключ от тази двойка се генерира и съхранява в криптиран вид в RQSCD на Доставчика и достъпът до него се осъществява чрез личен код за достъп (ПИН), парола или ключ под контрола на Титуляря/Създателя на печат.

Частният ключ на облачно удостоверение за квалифициран електронен подпис/печат е достъпен отдалечено и се активира единствено от Титуляря/Създателя на печат чрез личен код за достъп (ПИН), парола или ключ под контрола на Титуляря/

Създателя на печат.

8.1.2. Доставка на частния ключ

В съответствие с т.6.1.2 от документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги“.

8.1.3. Доставка на публичния ключ

В съответствие с т.6.1.3 от документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги“.

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

В съответствие с т.6.1.4 от документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги“.

8.1.5. Дължина на ключовете

В съответствие с т.6.1.5 от документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги“.

8.2. ЗАЩИТА НА ЧАСТНИЯ КЛЮЧ И ТЕХНИЧЕСКИ КОНТРОЛ НА КРИПТОГРАФСКИЯ МОДУЛ

8.2.1. Стандарти на криптографския модул

В съответствие с т.6.2.1 от документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги“.

8.2.2. Контрол на съхранението и ползването на частен ключ

В съответствие с т.6.2.2 от документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги“.

8.2.3. Съхранение на частните ключове

В съответствие с т.6.2.3 от документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги“.

8.2.4. Архивиране на частните ключове

В съответствие с т.6.2.4 от документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги“.

8.2.5. Прехвърляне на частните ключове в и от криптографския модул

В съответствие с т.6.2.5 от документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги“.

8.2.6. Активирание и деактивирание на частни ключове

В съответствие с т.6.2.6 от документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги“.

В допълнение, създаването на отдалечени квалифицирани електронни подписи/печати изисква идентификация и удостоверяване на Титуляря/Създателя на печат с цел активирание на издаденото му облачно удостоверение и съответния частен ключ.

Удостоверяването на Титуляря/Създателя на печат се осъществява посредством двуфакторната му автентикация пред Платформата посредством Мобилното приложение InfoNotary Mobile: а) притежаване на уникално мобилно устройство с активиран потребителски профил в Мобилното приложение InfoNotary Mobile, чрез валидиране на издаденото удостоверение за автентикация на мобилното устройство и б) валидиране на създадения от и известен само на Титуляря/Създателя на печат персонален идентификационен код (ПИН).

Проверката и потвърждаването на посочените атрибути се извършва от посочените в т.6.1. (фиг. 1) компоненти Identity Provider и SAM в Платформата за облачни квалифицирани удостоверения и отдалечено подписване и подпечатване на електронни документи на Доставчика.

При успешно удостоверяване на Титуляря/Създателя на печат, Доставчикът активира частния ключ на Титуляря/Създателя на печат за извършване на конкретната криптографска операция, т.е. отдалечено създаване на квалифицирани електронни подписи/печати/отдалечено подписване/подпечатване на електронен документ по възлагане от Титуляря/Създателя на печат.

При неуспешно удостоверяване на Титуляря/Създателя на печат, Доставчикът отказва извършването на извършването на съответната криптографска операция.

Доставчикът винаги проверява валидността на съответното облачно удостоверение, преди да използва частния ключ и отказва да използва ключ към облачно квалифицирано удостоверение с изтекъл срок на валидност

Частен ключ на Титуляр на облачно удостоверение за електронен подпис се деактивира автоматично, след извършване на криптографската операция (отдалеченото подписване на електронен документ), за която е бил активиран и посредством преустановяване на логическия достъп до защитения потребителски профил в RQSCD на платформата за облачен подпис.

8.2.7. Унищожаване на Частните ключове

Частен ключ на Титуляр на облачно удостоверение електронен подпис се унищожава чрез изтриването му от защитения потребителски профил в RQSCD на платформата за облачен подпис, при:

- Изтичане на срока на валидност на издаденото облачно удостоверение за квалифициран електронен подпис/печат;

- Прекратяване на издаденото облачно удостоверение за квалифициран електронен подпис/печат;
- Прекратяване на договора за предоставяне на удостоверителни услуги;
- Подадено искане от страна на Титуляря/Създателя на печат или Изтриване на клиентския профил в системите на Доставчика;
- Прекратяване/унищожаване на логическия път/достъп между приложението за управление (напр. мобилно приложение, информационна система) и защитения потребителски профил в RQSCD на Платформата за облачен подпис.

8.3. ДРУГИ АСПЕКТИ ОТ УПРАВЛЕНИЕТО НА ДВОЙКАТА КЛЮЧОВЕ

8.3.1. Архивиране на Публичен ключ

В съответствие с т.6.3.1 от документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги“.

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

В съответствие с т.6.3.2 от документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги“.

8.4. ДАННИ ЗА АКТИВИРАНЕ

В съответствие с т.6.4 от документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги“.

8.5. КОНТРОЛ НА КОМПЮТЪРНАТА СИГУРНОСТ

В съответствие с т.6.5 от документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги“.

8.6. ТЕХНИЧЕСКИ КОНТРОЛ И ЖИЗНЕН ЦИКЪЛ

В съответствие с т.6.6 от документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги“.

8.7. КОНТРОЛ НА СИГУРНОСТТА НА МРЕЖАТА

В съответствие с т.6.7 от документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги“.

9. ПРОФИЛИ

9.1. Профил на удостоверение за аутентикация на мобилно устройство InfoNotary Mobile Device Authentication CP

InfoNotary Mobile Device Authentication 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 + 5 год.	
Алгоритъм на електронния подпис		SHA256/RSA	
Атрибути на Издателя:			
Атрибут		Стойност	
Domain Component	Домейн компонент	DC	deviceauth-ca
Common Name	Име	CN	InfoNotary Device Authentication CA
Country Name	Държава	C	BG
Locality Name	Град	L	Sofia
Organization Name	Организация	O	InfoNotary PLC
Organizational Unit Name	Организационно звено	OU	TSP CA
Organization Identifier	Идентификатор на организацията (ЕИК)	2.5.4.97	NTRBG-131276827
Атрибути на Титуляря (x509 Subject DN):			
Атрибут		Стойност	
Common Name	Уникално име на мобилното устройство	CN	Unique mobile device ID
Domain Component	Домейн компонент	DC	deviceauth-ca
Organizational Unit Name	Организационно звено	OU	*опционално
Допълнителни атрибути на x509 разширения (x509v3 extensions):			
Атрибут		Стойност	

Basic Constraints (Critical)	End entity
Key Usage (Critical)	Digital Signature, Key Encipherment, Key agreement
Public Key	RSA 2048 bits, ECDSA 256
Authority Key Identifier	AuthorityKeyIdentifier
Subject Key Identifier	SubjectKeyIdentifier
Authority information Access	[1] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= https://repository.infonotary.com/device-ca.crt [2] Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL= http://ocsp.infonotary.com/qualified
CRL Distribution Point (Non Critical)	[1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl.infonotary.com/crl/deviceauth-ca.crl
Certificate Policies (Non Critical)	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.22144.3.9.1 Qualifier: Notice Text= InfoNotary Mobile Device Authentication Certificate
Extended Key Usage (Non Critical)	Client Authentication3

10. ПРОВЕРКА И КОНТРОЛ НА ДЕЙНОСТТА

В съответствие с т. 8 от документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги“.

10.1. РЕГУЛЯРНА ИЛИ ОБСТОЯТЕЛСТВЕНА ПРОВЕРКА

В съответствие с т. 8.1. от документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги“.

10.2. КВАЛИФИКАЦИЯ НА ПРОВЕРЯВАЩИТЕ ЛИЦА

В съответствие с т. 8.2. от документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги“.

10.3. ВРЪЗКА МЕЖДУ ПРОВЕРЯВАЩИТЕ ЛИЦА И ПРОВЕРЯВАНАТА ОРГАНИЗАЦИЯ

В съответствие с т. 8.3. от документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги“.

10.4. ОБХВАТ НА ПРОВЕРКАТА

В съответствие с т. 8.4. от документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги“.

10.5. ПРЕДПРИЕМАНЕ НА ДЕЙСТВИЯ ЗА ОТСТРАНЯВАНЕ НА НЕДОСТАТЪЦИТЕ

В съответствие с т. 8.5. от документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги“.

11. ДРУГИ БИЗНЕС И ПРАВНИ УСЛОВИЯ

11.1. ЦЕНИ И ТАКСИ

В съответствие с т. 9.1 от документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги“.

11.1.1. Възнаграждения по Договор за квалифицирани удостоверителни услуги

В съответствие с т. 9.1.1 от документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги“.

11.1.2. Фактуриране

В съответствие с т. 9.1.2 от документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги“.

11.1.3. Политика за връщане на удостоверението и възстановяване на плащането

В съответствие с т. 9.1.3 от документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги“.

11.2. ФИНАНСОВИ ОТГОВОРНОСТИ

В съответствие с т. 9.2.1 от документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги“.

11.3. ЗАСТРАХОВКА НА ДЕЙНОСТТА

В съответствие с т. 9.2.2 от документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги“.

11.4. Застрахователно покритие за крайните потребители

В съответствие с т. 9.2.3 от документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги“.

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

- неспазване на задълженията на Потребителите/Доверяващата се страна/Третите страни на Услугата за отдалечено подписване произтичащи от условията на настоящия документ, Практиката за предоставяне на квалифицирани удостоверителни услуги на Доставчика, Общите условия за ползване на приложението InfoNotary SignZone и сключения индивидуален договор;
- загуба мобилно устройство или компрометиране на създадения секретен код (ПИН код) за вход в приложението от потребителя, поради неполагане на дължимата грижа за опазването или ползването му;
- злоумишлени действия на трети лица (хакерски атаки, отнемане на мобилно устройство, достъп до начина на идентифициране и др.);
- незаконни действия от страна на Потребители и доверяващи се страни;
- форсмажор, аварии и други събития, които са извън контрола на Доставчика.

11.5. КОНФИДЕНЦИАЛНОСТ НА ИНФОРМАЦИЯТА

В съответствие с т. 9.3 от документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги“.

11.5.1. Обхват на конфиденциалната информация

В съответствие с т. 9.3.1. от документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги“.

В допълнение, Доставчикът приема за конфиденциална информацията, за документи изпратени за подписване или подписани през SingZone и данни, ползвани за адресиране на електронни документи, които са изпратени за подписване чрез SingZone.

11.5.2. Информация извън обхвата на конфиденциалната информация

В съответствие с т. 9.3.2 от документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги“.

11.5.3. Задължение за защита на конфиденциалната информация

В съответствие с т. 9.3.3 от документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги“.

11.6. ПОВЕРИТЕЛНОСТ НА ЛИЧНИТЕ ДАННИ

В съответствие с т. 9.4 от документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги“.

11.7. ПРАВА ВЪРХУ ИНТЕЛЕКТУАЛНАТА СОБСТВЕНОСТ

В съответствие с т. 9.5 от документа на ИНФОНОТАРИ „Практика при

предоставяне на квалифицирани удостоверителни услуги”.

11.8. ЗАДЪЛЖЕНИЯ, ОТГОВОРНОСТ И ГАРАНЦИИ НА ДОСТАВЧИКА

В съответствие с т. 9.6 от документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги”.

11.8.1. Задължения, отговорност и гаранции на Доставчика

В съответствие с т. 9.6.1 от документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги”.

11.8.2. Гаранции и отговорност на Регистриращия орган

В съответствие с т. 9.6.2 от документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги”.

11.8.3. Задължения и отговорности на Потребителите на Услугата за отдалечено подписване

В съответствие с т. 9.6.3 от документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги”.

В допълнение, Потребителят при ползване на Услугата за електронна идентификация има следните задължения и отговорности:

- да спазва условията на настоящия документ, Практиката за предоставяне на квалифицирани удостоверителни услуги, Общите условия за ползване на Мобилното приложение и Политика за поверителност и защита на личните данни;
- да предоставя вярна, точна и пълна информация, която Доставчикът изисква, в съответствие с нормативните изисквания и приложимите Политики и Практики;
- да не извършва неверни изявления или предоставят неистински документи, пред Регистриращия орган, които имат отношение към предоставяната услуга;
- да изпълнява точно изискванията за сигурност, определени от Доставчика;
- да пази създадения секретен код (ПИН код) от разкриване или неоторизирано използване;
- да поиска своевременно от Доставчика спиране или прекратяване на достъпа до мобилното приложение, когато е узнал, че създадения ПИН е компрометиран, бил е използван неправомерно или съществува опасност от неправомерното му използване.

Потребителят отговаря пред ИНФОНОТАРИ във всички случаи на неизпълнение на посочените задължения, произтичащи настоящия документ, Практиката за предоставяне на квалифицирани удостоверителни услуги на Доставчика, Общите условия за ползване на Мобилното приложение, като Доставчикът ще ангажира

отговорността на потребителя за вреди.

11.8.4. Задължения и отговорности на Третите страни

Задълженията, отговорностите и начина на интеграция на Доверяващите се страни/Третите страни с Платформата за отдалечено подписване на ИНФОНОТАРИ се уреждат в сключения индивидуален договор с Доставчика.

11.9. ОТКАЗ ОТ ОТГОВОРНОСТ

В съответствие с т. 9.7 от документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги“.

ИНФОНОТАРИ не носи отговорност в случаи на вреди причинени от:

- неспазване на задълженията на Потребителите на Услугата за отдалечено подписване произтичащи от условията на настоящия документ, Практиката за предоставяне на квалифицирани удостоверителни услуги на Доставчика, Общите условия за ползване на приложението InfoNotary SignZone;
- загуба на мобилно устройство или компрометиране на създадения секретен код (ПИН код) за вход в приложението от потребителя, поради не полагане на дължимата грижа за опазването или ползването му;
- злоумишлени действия на трети лица (хакерски атаки, отнемане на мобилно устройство, достъп до начина на идентифициране и др.);
- незаконни действия от страна на Потребители и Доверяващи се страни;
- форсмажор, аварии и други събития, които са извън контрола на Доставчика.

Доставчикът не носи отговорност за настъпили вреди за Доверяваща се страна/Трета страна, които са в резултат от неизпълнение на задълженията и неполагане на дължимата грижа, определени в сключения договор.

11.10. ОГРАНИЧЕНИЕ НА ОТГОВОРНОСТТА

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

11.11. КОМПЕНСАЦИИ ЗА ДОСТАВЧИКА

Във всички случаи на неизпълнение на задълженията от страна на Потребителите на Услугата за отдалечено подписване и на Третите страни, произтичащи от условията на настоящия документ, Практиката за предоставяне на квалифицирани удостоверителни услуги на Доставчика и Общите условия за ползване на квалифицирани удостоверителни услуги през мобилно приложение, Доставчикът ще ангажира отговорността на Потребителите на Услугата за отдалечено подписване и на Третите страни, за вреди.

11.12. СРОК И ПРЕКРАТЯВАНЕ

11.12.1. Срок

Настоящата „Политика и практика при предоставяне на квалифицирана услуга за отдалечено подписване и подпечатване на електронни документи“ влиза в сила от момента на нейното одобряване от Съвета на директорите на Инфонотари ЕАД и публикуването ѝ на адрес: <https://www.infonotary.com>.

Настоящия документ е валиден до неговата промяна или публикуване в Документния регистър и в интернет портала на Доставчика на информация за невалидността ѝ.

11.12.2. Прекратяване

Действието на „Политика и практика при предоставяне на квалифицирана услуга за отдалечено подписване и подпечатване на електронни документи“ се прекратява с прекратяване на дейността на Доставчика.

11.12.3. Ефект от прекратяването

В съответствие с т. 9.10.3 от документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги“.

11.13. ИНДИВИДУАЛНО УВЕДОМЯВАНЕ И КОМУНИКАЦИЯ МЕЖДУ УЧАСТНИЦИТЕ

В съответствие с т. 9.11 от документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги“.

11.14. ПРОМЕНИ

Настоящата „Политика и практика при предоставяне на квалифицирана услуга за отдалечено подписване и подпечатване на електронни документи“ може да бъде променяна по всяко време, като всяка промяна в нея се отразява след одобрение от Съвета на директорите на Инфонотари ЕАД и е публично достъпна от всички заинтересовани лица на адрес: <https://www.infonotary.com>.

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.

11.15. РЕШАВАНЕ НА СПОРОВЕ И ПОДСЪДНОСТ

В съответствие с т. 9.13 от документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги“.

11.16. ПРИЛОЖИМО ПРАВО

В съответствие с т. 9.14 от документа на ИНФОНОТАРИ „Практика при предоставяне на квалифицирани удостоверителни услуги“.

11.17. СЪОТВЕТСТВИЕ С ПРИЛОЖИМОТО ПРАВО

Настоящата „Политика и практика при предоставяне на квалифицирана услуга за отдалечено подписване и подпечатване на електронни документи“ е разработена в съответствие с изискванията на Регламент (ЕС) 910/2014 и националното законодателство.

11.18. ДРУГИ РАЗПОРЕДБИ

Настоящият документ не съдържа други разпоредби.