ДОСТАВЧИК НА КВАЛИФИЦИРАНИ
УДОСТОВЕРИТЕЛНИ УСЛУГИ
Тел.: 0700 14 220
support@mail.stampit.org www.stampit.org

Предоставяне на квалифицирани удостоверителни услуги от
„Информационно обслужване“ АД

# ПОЛИТИКА
# при предоставяне на услуги за удостоверяване на време (eIDAS-CP-TS)

**Версия: 1.0**
Дата на публикуване: 07.06.2017 г.
Дата на последна корекция: 07.06.2017 г.

**Съдържание**

„Информационно обслужване“ АД
София, ул.”Панайот Волов” № 2
тел. 02/ 9420340
факс 02/ 943 6607
ЕИК 831641791

## 1. Въведение

Настоящият документ описва общите правила, прилагани от „Информационно обслужване“ АД при предоставяне на услуги за удостоверяване на време за издаване на квалифицирани времеви печати.

При издаване на квалифицирани времеви печати се прилагат процедури и практики, гарантиращи най-висока сигурност при издаване, публикуване и управление. Допълнителна и по-подробна информация за прилаганите правила е налична в „Практиката при предоставяне на квалифицирани удостоверителни услуги“, публикувана на Интернет страницата на StampIT https://www.stampit.org.

Квалифицираният електронен времеви печат изпълнява следните изисквания:

- обвързва датата и часа с подписаните данни по криптографски сигурен начин, който изключва възможността за последваща промяна на данните;
- основава се на сигурен източник на точно време;
- подписан е с квалифициран електронен подпис на StampIT, в ролята му на квалифициран доставчик на квалифицирани удостоверителни услуги.

Структурата и съдържанието на настоящия документ съответства на изискванията на техническа спецификация ETSI TS 102 023.

### 1.1. Обхват

Настоящата политика се отнася до квалифицираните електронни времеви печати, издавани от „Информационно обслужване“ АД в съответствие с Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета от 23 юли 2014 година относно електронната идентификация и удостоверителните услуги при електронни трансакции на вътрешния пазар и в съответствие с приложимото законодателство в Република България.

## 2. Референции

Политиката е съобразена със следните документи:

- ETSI EN 319 401: „Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers"
- ETSI EN 319 401: „Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers"
- ETSI EN 319 421: „Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Timestamps“
- ETSI EN 319 422: „Electronic Signatures and Infrastructures (ESI); Timestamping protocol and Timestamp token profiles"
- IETF RFC 3161 „Internet X.509 Public Key Infrastructure: Timestamp Protocol (TSP)"
- Практика за предоставяне на квалифицирани удостоверителни услуги(CPS) на StampIT

## 3. Определения и абревиатури

| | |
|---|---|
| **Регламент (ЕС) № 910/2014** | 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. |
| **Директива 95/46/ЕО** | Директива 95/46/ЕО на Европейския парламент и на Съвета от 24 октомври 1995 г. за защита на физическите лица при обработването на лични данни и за свободното движение на тези данни |
| **Удостоверителна услуга** | Електронна услуга, предоставяна от „Информационно обслужване“ АД срещу възнаграждение, която се състои в:<br>а) създаването и проверката на електронни подписи, електронни печати и електронни времеви печати, както и удостоверения, свързани с тези услуги;<br>б) създаването и проверката на удостоверения за автентичност на уебсайт. |
| **Квалифицирана удостоверителна услуга** | Удостоверителна услуга, която отговаря на приложимите изисквания, определени в Регламент (ЕС) № 910/2014. |
| **Титуляр на електронен подпис** | Физическо лице, което създава електронен подпис. |
| **Електронен подпис** | Данни в електронна форма, които се добавят към други данни в електронна форма или са логически свързани с тях и които титулярят на електронния подпис използва, за да се подписва. |
| **Усъвършенстван електронен подпис** | Електронен подпис, който отговаря на следните изисквания:<br>а) свързан е по уникален начин с титуляря на подписа;<br>б) може да идентифицира титуляря на подписа;<br>в) създаден е чрез данни за създаване на електронен подпис, които титулярят на електронния подпис може да използва с висока степен на доверие и единствено под свой контрол; и<br>г) свързан е с данните, които са подписани с него, по начин, позволяващ да бъде открита всяка последваща промяна в тях. |
| **Квалифициран електронен подпис** | Усъвършенстван електронен подпис, който е създаден от устройство за създаване на квалифициран електронен подпис и се основава на квалифицирано удостоверение за електронни подписи. |
| **Данни за създаване на електронен подпис** | Уникални данни, които се използват от титуляря на електронния подпис за създаването на електронен подпис. |
| **Удостоверение за електронен подпис** | Електронен атестат, който свързва данните за валидиране на електронен подпис с физическо лице и потвърждава най-малко името или псевдонима на това лице. |
| **Квалифицирано удостоверение за електронен подпис (КУЕП)** | Удостоверение за електронни подписи, което се издава от доставчик на квалифицирани удостоверителни услуги и отговаря на изискванията, предвидени в приложение I към Регламент (ЕС) № 910/2014. |
| **Устройство за създаване на електронен подпис** | Конфигуриран софтуер или хардуер, който се използва за създаването на електронен подпис |
| **Устройство за създаване на квалифициран електронен подпис** | Устройство за създаване на електронен подпис, което отговаря на изискванията, предвидени в приложение II към |

| | |
|---|---|
| | Регламент (ЕС) № 910/2014 |
| **Създател на печат** | Юридическо лице, което създава електронен печат. |
| **Електронен печат** | Данни в електронна форма, които се добавят към други данни в електронна форма или са логически свързани с тях, за да се гарантират произходът и целостта на последните; |
| **Усъвършенстван електронен печат** | Електронен печат, който отговаря на следните изисквания:<br>а) свързан е по уникален начин със създателя на печата;<br>б) може да идентифицира създателя на печата;<br>в) създаден е чрез данни за създаване на електронен печат, които създателят на електронния печат може да използва с висока степен на доверие и единствено под свой контрол; и<br>г) е свързан с данните, за които се отнася, по начин, позволяващ да бъде открита всяка последваща промяна в тях. |
| **Квалифициран електронен печат** | Усъвършенстван електронен печат, който е създаден от устройство за създаване на квалифициран електронен печат и се основава на квалифицирано удостоверение за електронен печат |
| **Данни за създаване на електронен печат** | Уникални данни, които се използват от създателя на електронния печат за създаването на електронен печат |
| **Удостоверение за електронен печат** | Електронен атестат, който свързва данните за валидиране на електронен печат с юридическо лице и потвърждава името на това лице |
| **Квалифицирано удостоверение за електронен печат** | Удостоверение за електронен печат, което се издава от доставчик на квалифицирани удостоверителни услуги и отговаря на изискванията, предвидени в приложение III към Регламент (ЕС) № 910/2014. |
| **Устройство за създаване на електронен печат** | Конфигуриран софтуер или хардуер, който се използва за създаването на електронен печат |
| **Устройство за създаване на квалифициран електронен печат** | Устройство за създаване на електронен печат, което отговаря на приложимите изисквания, предвидени в приложение II към Регламент (ЕС) № 910/2014. |
| **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. |
| **Квалифициран електронен времеви печат** | Електронен времеви печат, който отговаря на следните изисквания:<br>а) обвързва датата и часа с данните по начин, който до голяма степен изключва възможността за незабелязана промяна на данните;<br>б) основава се на източник на точно време, свързан с координираното универсално време; и<br>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. |
| **Електронен документ** | Всяко съдържание, съхранявано в електронна форма, по-специално текстови или звуков, визуален или аудио-визуален запис |
| **Удостоверение за автентичност на уебсайт** | Удостоверение, което позволява да се удостовери автентичността на уебсайт, като го свързва с физическото или юридическото лице, на което е издадено удостоверението. |
| **Квалифицирано удостоверение за** | Удостоверение за автентичност на уебсайт, което се издава |

| | |
|---|---|
| **автентичност на уебсайт** | от доставчик на квалифицирани удостоверителни услуги и отговаря на изискванията, предвидени в приложение IV към Регламент (ЕС) № 910/2014. |
| **Доверяваща се страна** | Физическо или юридическо лице, което разчита на електронна идентификация или удостоверителна услуга |
| **Национално право** | Действащото българско законодателство |
| **Надзорен орган** | Надзорен орган по смисъла на член 17 от Регламент (ЕС) № 910/2014 |
| **ИО АД/Доставчик/ДКУУ** | „Информационно обслужване" АД в качеството му на доставчик на квалифицирани удостоверителни услуги, получил квалифицирания си статут от Надзорен орган. |
| **Практика** | Практика при предоставяне на квалифицирани удостоверителни услуги (Certification Practice Statement - CPS) |
| **Политика** | Политика при предоставяне на квалифицирани удостоверения за квалифициран електронен подпис и квалифициран електронен печат (eIDAS-CP-QES)<br>Политика при предоставяне на услуги за удостоверяване на време (eIDAS-CP-TS)<br>Политика при предоставяне на квалифицирани удостоверения за усъвършенстван електронен подпис и усъвършенстван електронен печат (eIDAS-CP-AES);<br>Политика при предоставяне на квалифицирани удостоверения за автентичност на уебсайт (eIDAS-CP-SSL). |
| **РО** | Регистриращ орган |
| **УО** | Удостоверяващ орган |
| **RSA Rivers-Shamir-Adelman** | Криптографски алгоритъм (асиметричен) |
| **SHA2 Secure Hash Algorithm** | Хеш функция |
| **SHA256/RSA Signature algoriithm** | Алгоритъм за създаване на квалифициран електронен подпис от ИО АД |
| **SSCD** | Устройство за сигурно създаване и проверка на електронен подпис |
| **URL Uniform Resource Locator** | Указател на ресурс/уеб адрес |
| **QCP-l-qscd** | Политика на квалифицирано удостоверение, издадено на юридическо лице, когато частния ключ на свързаното с него удостоверение е генериран на QSCD |
| **QCP-n-qscd** | Политика на квалифицирано удостоверение, издадено на физическо лице, когато частния ключ на свързаното с него удостоверение е генериран на QSCD |
| **QSCD** | Устройство за създаване на квалифициран електронен подпис или печат |
| **NCP+** | Засилена нормализирана удостоверителна политика, която включва допълнителни изисквания за квалифицирани удостоверения в съответствие с Регламент (ЕС) № 910/2014 |
| **Certification Authority (CA)** | Удостоверяващ орган |
| **Common Name (CN)** | Публично име |
| **Certificate Policy (CP)** | Политика за предоставяне на квалифицирано удостоверение за усъвършенстван електронен подпис и усъвършенстван електронен печат, квалифицирано удостоверение за автентичност на уебсайт и квалифициран електронен печат |
| **Certification Practice Statement (CPS)** | Практика при предоставяне на удостоверителни |

| | |
|---|---|
| | услуги |
| **Certificate Revocation List (CRL)** | Списък със спрени и прекратени удостоверения |
| **Distinguished Name (DN)** | Отличително име на субект, вписан в удостоверението |
| **Enhanced key usage** | Разширени цели за използване на ключа |
| **Federal Information Processing Standard (FIPS)** | Федерален стандарт за обработка на информация |
| **Hardware Security Module** | Хардуерен криптографски модул |
| **Object Identifier (OID)** | Обектен идентификатор |
| **Public Key Cryptography Standards (PKCS)** | Серия стандарти в криптографията на публичния ключ |
| **Public Key Infrastructure (PKI)** | Инфраструктура на публичния ключ |
| **Registration Authority (RA/PO)** | Регистриращ орган |

## 4. Общи понятия

### 4.1. Квалифицирана услуга за удостоверяване на време

Предоставянето на квалифицирана услуга за удостоверяване на време и управление на квалифицирани електронни времеви печати се състои от два компонента:

- Технологична система, която издава квалифицирани електронни времеви печати и поддържа архив на генерираните удостоверения за електронен времеви печат
- Управление на системата, чрез която се наблюдават и контролират операциите по предоставяне на услугата

Управлението на системата гарантира постоянна актуализация и синхронизация със сигурен източник на координирано универсално време(UTC) и надеждно управление на технологичната система.

### 4.2. Орган за удостоверяване на време

За издаване на удостоверенията за квалифицирани електронни времеви печати се използва орган за удостоверяване на време StampIT Global TSA, подписан с квалифициран електронен подпис на StampIT, в ролята му на квалифициран доставчик на квалифицирани удостоверителни услуги. Чрез електронните времеви печати Абонатите могат да удостоверят времето за представяне на електронни документи и електронни съобщения, като представлява доказателство, че подписаният обект от данни е съществувал към момента на поставяне на времевия печат.

StampIT е обект на одит от независим Орган за оценяване на съответствието най-малко веднъж на 24 месеца. Целта на одита е да потвърди, че „Информационно обслужване“ АД в качеството си на доставчик на удостоверителни услуги и предоставяните от Организацията удостоверителни услуги отговарят на изискванията на Регламент (ЕС) № 910/2014, ISO 9001, ISO/IEC 27001 и ISO/IEC 20000-1.

### 4.3. Абонати

Абонати са потребители на услугата, описани в „Практика при предоставяне на квалифицирани удостоверителни услуги“.

Абонатите могат да бъдат крайни клиенти или група потребители в рамките на една организация.

Когато потребителят е организация, някои от задълженията по настоящата политика ще бъдат прилагани и към крайните потребители. При всички положения организацията носи отговорност, ако задълженията на крайните потребители не са коректно изпълнени. Организацията е задължена да информира своите крайни потребители относно отговорността им във връзка с използването на настоящата удостоверителна услуга.

Когато потребителят е краен клиент, той носи отговорност за спазването на изискванията по настоящата политика.

### 4.4. Общ преглед

#### 4.4.1. Предназначение

Настоящият документ допълва „Практика при предоставяне на квалифицирани удостоверителни услуги“ със специфичните условия за предоставяне на квалифицирани услуги за удостоверяване на време.

#### 4.4.2. Ниво на детайлизация

Настоящата политика описва общия подход, процедури и правила при предоставяне на услугата за квалифицирано удостоверяване на време спрямо техническите, организационните и процедурни изисквания за поддържане на услугата.

Всички оперативни документи и записи, поддържани от StampIT са със съответното ниво на класификация относно достъпа до тях и са налични за преглед от надлежно оторизираните за това лица.

#### 4.4.3. Подход

Настоящия документ представя общата политика при предоставяне на услугите и не детайлизира техническите подходи за реализацията и управлението на инфраструктурата. В него са дефинирани условията и правилата, към които се придържа StampIT като квалифициран доставчик на квалифицирани удостоверителни услуги и квалифицирани електронни времеви печати.

## 5. Политика на органа за удостоверяване на време

### 5.1. Общи положения

Политиката на органа за удостоверяване на време представлява списък от правила и тяхното прилагане при издаването и управлението на удостоверения за време. StampIT гарантира минимална точност от под 1 секунда при издаването на тези удостоверения.

Използваният профил на издаваните квалифицирани удостоверения за време са в съответствие с изискванията на ETSI EN 319 422.

Издаването, верифицирането и търсенето в Публичния регистър на квалифицирани удостоверения за време се извършва чрез потребителски интерфейс, достъпен за Абонатите на адрес https://tsa.stampit.org.

Издаването може да се извърши и по https протокол в съответствие с RFC 3161, като издаваните удостоверения използват алгоритми RSA 2048 / SHA256.

Профилът на StampIT Global TSA удостоверението е следния:

| **StampIT Global TSA** | | | |
|---|---|---|---|
| Signature Algorithm | SHA256/RSA | | |
| Issuer | CN | StampIT Global Qualified CA | Име |
| | C | BG | Държава |
| | O | Information Services JSC | Организация |
| | L | Sofia | |
| | 2.5.4.97 (OrganizationIdentifier) | NTRBG-831641791 | ЕИК |
| Validity | 5 години | | |
| Subject | CN | StampIT Global TSA | Име |
| | C | BG | Държава |
| | O | Information Services JSC | Организация |
| | L | Sofia | Област |
| | 2.5.4.97 (OrganizationIdentifier) | NTRBG-831641791 | ЕИК |
| Public Key | RSA 2048 bits | | |
| Key Usage (Critical) | Digital Signature | | |
| Friendly Name | StampIT Global TSA | | |
| Extended key usage (Critical) | Time Stamping (1.3.6.1.5.5.7.3.8) | | |
| Basic constrains (Critical) | End entity | | |
| Authority Information Access | [1]Authority Info Access<br>Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)<br>Alternative Name:<br>URL=http://www.stampit.org/repository/stampit_global_qualified.crt<br>[2]Authority Info Access<br>Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)<br>Alternative Name:<br>URL=http://ocsp.stampit.org/ | | |
| CRL Distribution Point/Non Critical/ | [1]CRL Distribution Point<br>Distribution Point Name:<br>Full Name:<br>URL=http://www.stampit.org/crl/stampit_global_qualified.crl | | |
| Certificate Policies (Non Critical) | Идентификатор за политика = **1.3.6.1.4.1.11290.1.2.1.1**<br>Хранилище = http://www.stampit.org/repository/ | | |

### 5.2. Идентификация на политиката

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.

Идентификаторите за политиките на квалифицираните удостоверения, 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 издаваните удостоверения е както следва:

| Вид удостоверение | StampIT Policy Identifier | ETSI Policy Identifier |
|---|---|---|
| StampIT Global TSA | 1.3.6.1.4.1.11290.1.2.1.1 | 0.4.0.2023.1.1 |

### 5.3. Приложимост на електронния времеви печат

Настоящата политика е насочена към покриване на изискванията за квалифицирани електронни времеви печати (ETSI EN 319 122), но е приложима към всяка друга употреба на времеви печати с еквивалентни изисквания.

Квалифицираната услуга за удостоверяване на време, позволява за всеки подписан с обект да се удостовери датата и часа на представяне.

### 5.4. Съответствие

Дейностите по издаване и управление на квалифицирани електронни времеви печати са в съответствие с изискванията на:

- Регламент (ЕС) № 910/2014
- ETSI TS 119 421
- RFC 3161
- RFC 5816

## 6. Задължения и отговорности

### 6.1. Задължения

#### 6.1.1. Общи

StampIT се задължава да:

- спазва своите вътрешни правила и публична практика, политики и процедури;
- спазва Регламент (ЕС) № 910/2014 и националното право;
- осигурява надеждни механизми, включително механизма за генерирането на ключовете, защитения механизъм за създаване на електронен подпис и

процедурите за разпределяне на секретните части по отношение на неговата собствена инфраструктура;

- уведомява страните в случай на компрометиране на частните си ключове;
- управлява жизнения цикъл на Stampit Global TSA удостоверението;
- издава квалифицирани електронни времеви печати в съответствие с политиката и практиката, като изпълнява задълженията си посочени в тях.

#### 6.1.2. Задължения към Абонатите

StampIT се задължава да:

- осигурява непрекъснато достъп до квалифицираната услуга за удостоверяване на време, освен при планирана профилактика и форсмажорни ситуации;
- осигурява квалифицирани електронни времеви печати с точност по-малка от 1 секунда;
- осигурява поддръжка на абонатите и доверяващите се страни;
- предоставя копия на практиката и политиките си, както и други действащи документи за публичен достъп.

### 6.2. Задължения на Абонатите

Абонатите се задължават да:

- верифицират издадените квалифицирани електронни удостоверения за време, включително и чрез проверка с CRL списъка или чрез OCSP интерфейса;
- да не злоупотребяват с предоставения интерфейс ;
- да изпълняват задълженията, описани в „Практика при предоставяне на квалифицирани удостоверителни услуги“.

### 6.3. Задължения на Доверяващите се страни

Доверяващите се страни се задължават да:

- верифицират издадените квалифицирани електронни удостоверения за време, включително и чрез проверка на StampIT Global TSA удостоверението в CRL списъка или чрез OCSP интерфейса;
- да извършат проверка на приложимостта на използваните за създаване на удостоверението криптографски алгоритми;
- да изпълняват задълженията, описани в „Практика при предоставяне на квалифицирани удостоверителни услуги“.

### 6.4. Отговорност

Във връзка с риска от отговорност за нанесени щети в съответствие с Регламент (ЕС) № 910/2014 StampIT поддържа достатъчни финансови ресурси и/или сключва подходяща застраховка за отговорност в съответствие с националното право.

Освен в случай на небрежност, StampIT не носи отговорност за:

- пропуснати ползи
- загуба на данни
- други косвени вреди, произтичащи от или във връзка с използването, действието или невъзможността за действие на квалифицираната услуга за удостоверяване на време
- използването на квалифицирано удостоверение за време, при което са надвишени определените ограничения, посочени в него или в тази политика
- сигурността, използването, целостта на продуктите, включително хардуера и софтуера, които абонатът използва

## 7. Изисквания към практиката на органа за удостоверяване на време

StampIT осъществява надежден и сигурен контрол върху изпълнението на изискванията на настоящата политика. Извършва се регистриране на всички събития в системата под формата на системни журнали, които се архивират и съхраняват по сигурен начин.

### 7.1. Практика и процедури на органа за удостоверяване на време

#### 7.1.1. Практика

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“, публикуван на https://www.stampit.org.

Дейностите по управление, поддържане и усъвършенстване на услугите, предоставяни от органа за удостоверяване на време (включително и процедурите за оценка на риска) се изпълняват в съответствие с изискванията на имплементираната в „Информационно обслужване“ АД Интегрирана система за управление, сертифицирана от външен сертифициращ орган по стандартите ISO 27001:2013 за управление на информационната сигурност, ISO 20000-1:2011 за управление на предоставяните ИТ услуги и ISO 9001:2015 за управление на качеството.

#### 7.1.2. Достъпност

Общите практики по предоставяне на квалифицираната услуга за удостоверяване на време са описани в документа „Практика при предоставяне на квалифицирани удостоверителни услуги“, публикуван на https://www.stampit.org.

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 ключовете на органа за удостоверяване на време

### 7.2.1. Генериране на ключовете на органа за удостоверяване на време

StampIT генерира по сигурен начин и защитава ключовата двойка, като използва надеждна система(HSM с ниво на сигурност FIPS 140-2, level 3+) и взема необходимите мерки, за да предотврати компрометирането или неоторизираното им използване. StampIT внедрява и документира процедурата по генериране на ключовете, в съответствие с настоящата политика. StampIT внедрява европейските и общопризнати в международната практика стандарти за надеждни системи, включително и стандартите за информационна сигурност и прави всичко възможно, за да ги съблюдава.

Изискванията за използваните алгоритми и дължината на подписващия частен ключ са съобразени с ETSI TS 119 312.

### 7.2.2. Защита на частния ключ на органа за удостоверяване на време

Частният ключ на органа за удостоверяване на време се съхранява и защитава единствено чрез HSM криптографски модул, сертифициран спрямо изискванията на FIPS 140-2, level 3+.

В специално защитени огнеупорни каси се съхраняват разделени чрез key escrow ключове за възстановяване на частния ключ на органа за удостоверяване на време. Това се прави с цел възстановяване при настъпване на форсмажорни събития.

### 7.2.3. Разпространение на публичния ключ на органа за удостоверяване на време

Публичният ключ на удостоверението StampIT Global TSA е публикуван на Интернет страницата на StampIT https://www.stampit.org.

### 7.2.4. Преиздаване на ключовата двойка на органа за удостоверяване на време

StampIT Global TSA е издаден със срок на валидност 5 години. Ако в този период за използваните алгоритми има основателно съмнение, че са открити криптографски слабости или се променят изискванията се генерира нова ключова двойка. След изтичане на периода на валидност се генерира нова ключова двойка и се издава ново квалифицирано удостоверение.

### 7.2.5. Унищожаване на частния ключ на органа за удостоверяване на време

След изтичане срока на валидност или прекратяване частният ключ на удостоверението се съхранява за срок от 10 години. След изтичането на този срок частният ключ на такова удостоверение се унищожава по сигурен начин, гарантиращ, че няма да бъде използван повторно.

### 7.2.6. Управление на жизнения цикъл на подписващото криптографско оборудване

Криптографското оборудване се проверява от персонала на StampIT за наличие на цялост на опаковката при получаване и по време на съхранението.

Инсталацията, конфигурацията и активацията на устройството се извършва от служители със съответните роли съгласно процедурите на производителя в сигурните помещения на „Информационно обслужване“ АД.

Служителите изпълняват технологичните процедури за верификация на състоянието на оборудването.

При отпадане или замяна, служителите на StampIT изтриват по сигурен начин наличните в оборудването частни ключове в съответствие с предоставената от производителя документация.

## 7.3. Удостоверяване на време

Услугите по удостоверяване на време се извършват в съответствие с изискванията на ETSI

TS 101 861 Time Stamp Profile и RFC 3161.

Комуникацията с Абонатите се извършва по протоколите HTTP и HTTPS.

### 7.3.1. Token за електронен времеви печат (TST)

Профилите на заявките за издаване на TST и отговорите са следните:

| Time Stamp Query (TSQ) | | |
|---|---|---|
| Version | 1 | |
| MessageImprint | Hash Algorithm | OID SHA256 2.16.840.1.101.3.4.2.1 |
| | Hash Value | Стойност на хеша върху данните |
| RequestedPolicy | | OID StampIT Global TSA 1.3.6.1.4.1.11290.1.2.1.1 |
| Nonce | | Опция |
| CertReq | True/False | За включване на StampIT Global TSA удостоверението в TSR |

| Time Stamp Response (TSR) | | |
|---|---|---|
| Version | 1 | |
| MessageImprint | Hash Algorithm | OID SHA256 2.16.840.1.101.3.4.2.1 |
| | Hash Value | Стойност на хеша върху данните |
| Policy | | OID StampIT Global TSA 1.3.6.1.4.1.11290.1.2.1.1 |
| SerialNumber | | Сериен номер на TSR |
| GeneratedTime | | Удостоверено време по UTC |
| Accuracy | | min 999ms |
| Nonce | | Ако е присъствало в заявката |
| TSA | | Ако е било заявено |

### 7.3.2. Синхронизация на точно време с UTC

Синхронизацията на точното време се извършва по NTP/NTPS протокол чрез връзка към минимум два различни stratum-1 и в краен случай към stratum-2 сървъри. Синхронизацията се извършва минимум два пъти дневно автоматично, като се регистрират отклоненията.

Синхронизацията на точно време се наблюдава и регистрира, като са налични нотификации при наличие на отклонение от повече от 50 ms.

## 7.4. Управление и дейности на органа за удостоверяване на време

### 7.4.1. Управление на сигурността

Имплементираните организационни мерки за управление на информационната сигурност са в съответствие с изискванията на действащото законодателство, техническите стандарти и внедрената в Дружеството Интегрирана система за управление.

### 7.4.2. Класификация на активите и оценка на риска

„Информационно обслужване“ АД класифицира и поддържа регистри на всички активи в съответствие с изискванията на ISO/IEC 27001:2013. Съгласно разработената и внедрена Интегрирана система за управление се извършва анализ за оценката на уязвимост по всички вътрешни процедури, приложения и информационни системи. Изискванията за анализ могат, също така, да бъдат определени от външна институция, упълномощена да извършва одит от трета страна.

Анализът на риска се извършва най-малко веднъж годишно. Решението да се пристъпи към анализ се извършва от Съвета за управление.

Администраторът по сигурността е отговорен за извършване на вътрешните одити, в частта касаеща предоставянето на удостоверителни услуги. Той контролира опазване на записите по сигурността в журналите, коректното архивиране на резервните копия, дейностите, изпълнени в случай на заплахи и съответствието с настоящата политика.

### 7.4.3. Сигурност на персонала

Практиките за управление на персонала включват мерки, които дават гаранции за надеждност и компетентност на служителите и за изпълнение на техните задължения.

Всички служители, които имат достъп до информация, са длъжни да спазват стриктно изискванията за конфиденциалност и защита на личните данни.

Служителите на доставчика, които имат достъп до конфиденциална информация, подписват декларации за конфиденциалност и неразпространение на информация.

Служителите на доставчика, които имат достъп до лични данни, подписват декларации за неразгласяване на лични данни.

Дейностите се изпълняват от служители със съответна квалификация и роля в съответния процес, така, че да се минимизира възможността от компрометиране на заложените контроли, изтичане на конфиденциална информация и избягване на конфликт на интереси.

Ролите са регламентирани във вътрешните процедури на StampIT и длъжностните характеристики на всеки служител, имащ отношение към работата на Доставчика.

### 7.4.4. Физическа сигурност

Физическият достъп до защитената част на системите на StampIT е ограничен и до нея имат достъп само надлежно овластени служители, в зависимост от техните функционални задължения. Взети са мерки за защита от аварии или компрометиране на активите, водещи до прекратяване на бизнес дейностите, както и за откриване и предотвратяване на опитите за компрометиране на информация или кражба на информация и устройства, обработващи информация.

За нуждите на StampIT се поддържат специално изградени сигурни помещения, собственост на Дружеството, в които са разположени инфраструктурните компоненти на StampIT. В помещенията се следят в реално време базовите характеристики на средата (температура и влажност), като са разположени датчици за движение, сеизмична активност, видеонаблюдение и др.

Налична е 24x7 невъоръжена охрана, извършваща контрол и наблюдение на достъпа до помещенията. Сигурните помещения, използвани за инфраструктурата на доставчика разполагат с отделна алармена система, в допълнение към основната, използвана за достъпа до сградите на Дружеството.

Достъпът до помещенията е организиран чрез двуфакторна оторизация и се регистрира всяко влизане и напускане на помещенията.

### 7.4.5. Управление на оперативните дейности

StampIT използва надеждни и резервирани системи при предоставяне на своите услуги. Надеждната система представлява компютърен хардуер, софтуер и процедури, които осигуряват приемливо ниво на защита срещу рискове, свързани със сигурността, предоставя разумно ниво на работоспособност, надеждност, правилно опериране и изпълнение на изискванията за сигурност.

Комплексът от софтуер и хардуер, използван за дейността на StampIT е изграден от високонадеждни и сигурни компоненти. Прилага се концепцията Security by design, като за всеки компонент са заложени и включени наличните фактори и конфигурации за сигурност.

StampIT прилага процедурите и политиките за управление на информационната сигурност, част от Интегрираната система за управление, поддържана от „Информационно обслужване“ АД.

При управление на промените в системата на StampIT се прилагат процедурите и политиките за управление на информационната сигурност, част от Интегрираната система за управление, поддържана от „Информационно обслужване“ АД.

Всички промени се управляват от съответните оторизирани служители на Дружеството. При добавяне на нови компоненти към системата (хардуерни или софтуерни), към тях задължително се прилага необходимата техническа и експлоатационна документация.

При отпадане на компоненти от системата се гарантира сигурното унищожаване на наличните на тях данни на Доставчика.

„Информационно обслужване“ АД разполага с високо развита мрежова инфраструктура, компонентите на която предлагат възможности за защита от различни видове мрежови

атаки. Разположени са устройства за защита от DDoS, защитни стени от ново поколение (ng-firewalls) и високопроизводителни активни мрежови устройства.

Наличен е Център за управление на мрежата (NOC), който работи в режим 24x7, в който се извършва наблюдение и ранно известяване при настъпили събития, които могат да повлияят върху дейността на StampIT.

Допълнителна и по-подробна информация за прилаганите оперативни правила е налична в „Практиката при предоставяне на квалифицирани удостоверителни услуги“, налична на Интернет страницата на StampIT https://www.stampit.org.

### 7.4.6. Управление на достъпа

При управление на сигурността на квалифицираната услуга за удостоверяване на време се прилагат редица технически и административни контроли за управление на достъпа. Техническите контроли се прилагат на мрежово (правила на ng-firewall устройства и ср.), системно и локално ниво.

Администрирането на потребителите се извършва от служители със съответните оторизирани роли, както е описано в политиките за сигурност, част от Интегрираната система за управление на Дружеството.

Всички действия, извършвани в рамките на инфраструктурата на StampIT се допускат единствено след надлежна оторизация на служителите, за което се съхранява надлежна информация в системните журнали.

За всяко нарушение на сигурността, което има значително влияние върху предлаганата услуга, се информира Органа по надзор.

### 7.4.7. Използване на сигурни устройства

Издаването на квалифицирани удостоверения за време се извършва чрез HSM криптографски модул с ниво на сигурност FIPS 140-2, level 3+. В него са заложени редица технически контроли срещу неоторизиран достъп и модифициране на физическо и логическо ниво.

### 7.4.8. Компрометиране на частния ключ

StampIT генерира по сигурен начин и защитава частния ключ на StampIT Global TSA, като използва надеждна система и взема необходимите мерки, за да предотврати компрометирането или неоторизираното им използване. StampIT внедрява и документира процедурата по генериране на ключовете, в съответствие с настоящата политика. StampIT внедрява европейските и общопризнати в международната практика стандарти за надеждни системи, включително и стандартите за информационна сигурност и прави всичко възможно, за да ги съблюдава.

В случай на компрометиране на частния ключ на Органа за удостоверяване на време се предприемат следните действия:

- прекратява се удостоверението на StampIT Global TSA, като се включва в CRL списъка;

- преиздава се удостоверение с нова ключова двойка;
- информират се Абонатите и Доверяващите се страни, които биха могли да бъдат засегнати;
- извършва се детайлен одит на сигурността на StampIT с оглед идентифициране на евентуални съпътстващи щети и анализиране на причините за компрометирането;
- предприемат се коригиращи действия, които се документират, изпълняват и се валидират.

### 7.4.9. Прекратяване на дейността на органа за удостоверяване на време

В случай на прекратяване на дейността на Органа за удостоверяване на време, независимо поради какви причини, StampIT трябва навреме да уведоми и да прехвърли отговорностите си по поддръжката на архивите на приемните страни.

Преди да прекрати своята дейност като орган за удостоверяване на време, StampIT извършва следните действия:

- информира за намеренията си Надзорния орган и Абонатите на услугата, най-късно четири месеца преди датата на прекратяване на дейността си;
- прекратява удостоверението на Органа за удостоверяване на време - ако дейността няма да бъде прехвърлена на друг доставчик;
- извършва необходимите действия за съхранение на архивите в съответствие с тази настоящата политика и нормативните изисквания - ако дейността няма да бъде прехвърлена на друг доставчик;
- в случай, че прехвърля дейността си на друг доставчик, StampIT ще предаде на приемната страна цялата документация, свързана с дейността му на доставчик на услуги за удостоверяване на време и правото да използва инфраструктурата на публичния ключ на StampIT, с оглед управление на вече издадените квалифицирани удостоверения, за срок не по-дълъг от шест месеца.

### 7.4.10. Спазване на правни изисквания

За всички въпроси, неуредени в настоящата политика се прилагат разпоредбите на Регламент (ЕС) № 910/2014 и действащото национално право. Всички изисквания за предоставяне на квалифицирани електронни времеви печати, произтичащи от настоящия документ, са в съответствие с изискванията на стандартите и техническите изисквания на ETSI.

### 7.4.11. Регистриране на събития, свързани с органа за удостоверяване на време

Всички събития, свързани с работата на Органа за удостоверяване на време се регистрират по надлежен и сигурен начин. Това включва и съхранение на заявките за издаване на TST (TSQ) и отговорите (TSR). За записите се осигурява контрол на конфиденциалността и интегритета по време на целия им жизнен цикъл – по време на опериране на системите (data in use), по време на трансфер/преместване (data in transit) и

при архивиране (data at rest). Информация от тези записи може да бъде искана от компетентните органи по надлежния ред.

Освен системните записи се извършват и:

- записи по управление на ключовете на Органа за удостоверяване на време;
- записи, свързани със синхронизирането на точно време.

Журналите се съхраняват за период от минимум 2 година.

Издадените квалифицирани електронни времеви печати се съхраняват за период от минимум 10 години.

### 7.5. Организация на дейността

За организация на дейността на Органа за удостоверяване на време „Информационно обслужване“ АД поддържа Интегрирана система за управление, сертифицирана от външен сертифициращ орган по стандартите ISO 27001:2013 за управление на информационната сигурност, ISO 20000-1:2011 за управление на предоставяните ИТ услуги и ISO 9001:2015 за управление на качеството.

Документите, управлявани от ИСУ, както и политиките и практиките съдържат всички оперативни контроли и процедури.

Дейността подлежи на контрол за съответствие от външен Орган за оценяване на съответствието съгласно изискванията на техническа спецификация ETSI TS 119 421.