

Предоставяне на квалифицирани удостоверителни услуги от
„Информационно обслужване“ АД

ПОЛИТИКА

**при предоставяне на квалифицирани удостоверения за
усъвършенстван електронен подпис и усъвършенстван
електронен печат (eIDAS-CP-AES)**

Версия: 2.0

Дата на публикуване: 07.06.2017 г.

Дата на последна корекция: 07.06.2017 г.

Съдържание

1. Въведение	10
1.1. Общ преглед на политиката	10
1.2. Наименование и идентификатор на политиката	11
1.3. Участници в инфраструктурата на публичния ключ, поддържана от „Информационно обслужване“ АД	11
1.3.1. Удостоверяващ орган	11
1.3.2. Регистриращи органи	11
1.3.3. Абонати	12
1.3.4. Доверяващи се страни	12
1.4. Приложимост и ограничения за употреба на издаваните квалифицирани удостоверения	13
1.4.1. Приложимост	13
1.4.2. Ограничения	13
1.5. Утвърждаване, управление на версиите и съдържанието на настоящата политика	13
2. Публични регистри и управление	14
2.1. Поддържани публични регистри	14
2.2. Честота на опресняване	14
2.3. Достъп	14
3. Идентификация и проверка на информацията за самоличност	14
3.1. Наименоване	14
3.2. Първоначална регистрация	16
3.2.1. Проверка за притежание на частен ключ	16
3.2.2. Проверка на юридическите лица	16
3.2.3. Проверка на физическите лица, юридическите лица, представители на юридическо лице	16
3.2.4. Проверка на физическите лица	16
3.2.5. Проверка от удостоверяващия орган	17
3.3. Подновяване на квалифицираното удостоверение	17
3.4. Временно спиране и прекратяване на действието на квалифицираното удостоверение	17
3.4.1. Заявка за временно спиране или прекратяване	18
3.4.2. Ефект от временното спиране или прекратяване	18
3.4.3. Уведомяване при спиране и прекратяване на квалифицирано удостоверение	18
3.5. Идентификация и проверка на самоличност след прекратяване на издадено квалифицирано удостоверение	18
4. Оперативни дейности	19
4.1. Валидна употреба на издаваните квалифицирани удостоверения	20
4.1.1. От страна на абонатите	20
4.1.2. От страна на доверяващите се страни	20
4.2. Подновяване и преиздаване на квалифицирани удостоверения	20
4.2.1. Процедура по подновяване на квалифицирани удостоверения	21

4.3.	Промяна на информация в квалифицираните удостоверения	21
4.4.	Спиране на квалифицираните удостоверения	22
4.4.1.	Основания за спиране	22
4.4.2.	Процедура за спиране	22
4.5.	Възобновяване на квалифицираните удостоверения	22
4.5.1.	Основания за възобновяване	23
4.5.2.	Процедура за възобновяване	23
4.6.	Прекратяване на квалифицираните удостоверения	23
4.6.1.	Основания за прекратяване	24
4.6.2.	Процедура за прекратяване	24
4.7.	Статус на издаваните квалифицирани удостоверения	24
4.7.1.	Автоматизирано, чрез Списъка със спрени и прекратени удостоверения (CRL)	25
4.7.2.	Автоматизирано, чрез Протокола за онлайн проверка на статуса на удостоверенията (OCSP)	25
4.7.3.	Ръчно, чрез Интернет страницата на StampIT	25
5.	Физическа и организационна сигурност	25
5.1.	Физическа сигурност	25
5.1.1.	Сигурни помещения	25
5.1.2.	Съхранение на данни	26
5.1.3.	Сигурно унищожаване на данни	26
5.2.	Организационна сигурност	26
5.3.	Сигурност на персонала	26
5.3.1.	Обучение на персонала	26
5.4.	Управление на записи и журнали	27
5.5.	Управление на архивите	27
5.6.	Прекратяване на дейността на Удостоверяващия орган	27
6.	Управление на техническата сигурност	28
6.1.	Генериране и привеждане в оперативен режим на ключовата двойка на Удостоверяващ орган	28
6.2.	Генериране на ключовата двойка на Абонат	28
6.2.1.	Изисквания към устройствата	29
6.2.2.	Предоставяне на ключовата двойка на Абоната	29
6.2.3.	Минимални дължини на ключовите двойки	29
6.2.4.	Параметри на публичния ключ	29
6.2.5.	Управление на частния ключ	30
6.2.5.1.	Съхранение на частния ключ	30
6.2.5.2.	Активиране на частния ключ	30
6.2.5.3.	Деактивиране на частния ключ	30
6.2.5.4.	Унищожаване на частния ключ	30
6.3.	Управление на ключовата двойка	30
6.3.1.	Архивиране на публичния ключ	30
6.3.2.	Валидност и употреба на издаваните удостоверения	30
6.4.	Активиране на частния ключ	31

6.4.1.	Генериране и предоставяне на данни за активиране	31
6.4.2.	Защита на данни за активиране	31
6.5.	Сигурност на използваните компютърни системи.....	31
6.6.	Управление на промените в системата на StampIT	31
6.7.	Управление на мрежовата сигурност	32
7.	Профили на удостоверенията	32
7.1.	Профил на StampIT базово (Root) удостоверение на „Информационно обслужване“ АД.....	32
7.2.	Профил на StampIT Оперативно (subordinate) удостоверение на „Информационно обслужване“ АД.....	33
7.3.	Профил на квалифицирано удостоверение за усъвършенстван електронен подпис StampIT Enterprise, което се издава на физическо лице /natural person/	34
7.4.	Профил на квалифицирано удостоверение за усъвършенстван електронен подпис за физическо лице, асоциирано с юридическо /legal person/ StampIT Enterprise Pro35	
7.5.	Профил на квалифицирано удостоверение за усъвършенстван електронен печат на юридическо лице /legal person/ StampIT Enterprise Seal	36
8.	Контрол на дейността на Доставчика.....	38
9.	Бизнес и правни въпроси	38
9.1.	Цени.....	38
9.1.1.	Отстраняване на неточности и възстановяване на извършено плащане	38
9.2.	Финансова отговорност	39
9.2.1.	Гаранции за плащане на обезщетенията.....	39
9.3.	Защита на личните данни	39
9.4.	Права върху интелектуалната собственост.....	39
9.4.1.	Собственост на ключовите двойки	39
9.5.	Задължения и отговорност на StampIT	40
9.5.1.	Отговорност пред Абоната.....	41
9.5.2.	Ограничения на отговорността на регистриращия орган	41
9.6.	Задължения на абоната	41
9.7.	Освобождаване от отговорност	42

„Информационно обслужване“ АД

София, ул. „Панайот Волов“ № 2

тел. 02/ 9420340

факс 02/ 943 6607

ЕИК 831641791

Авторското право върху настоящия документ принадлежи на
„Информационно обслужване“ АД.

ИЗПОЛЗВАНИ ТЕРМИНИ И СЪКРАЩЕНИЯ

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: а) създаването и проверката на електронни подписи, електронни печати и електронни времеви печати, както и удостоверения, свързани с тези услуги; 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: а) свързан е по уникален начин с титуляря на подписа; б) може да идентифицира титуляря на подписа; 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 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: а) свързан е по уникален начин със създателя на печата; б) може да идентифицира създателя на печата; 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 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: а) обвързва датата и часа с данните по начин, който до голяма степен изключва възможността за незабелязана промяна на данните; б) основава се на източник на точно време, свързан с координираното универсално време; и в) подписан е с усъвършенстван електронен подпис или е подпечатан с усъвършенстван електронен печат на доставчик на квалифицирани удостоверителни услуги или с друг равностоен метод.
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 автентичност на уебсайт	Удостоверение за автентичност на уебсайт, което се издава от доставчик на квалифицирани удостоверителни услуги и отговаря на изискванията, предвидени в приложение IV към

Доверяваща се страна	Регламент (ЕС) № 910/2014.
Национално право	Физическо или юридическо лице, което разчита на електронна идентификация или удостоверителна услуга
Надзорен орган	Действащото българско законодателство
ИО АД/Доставчик/ДКУУ	Надзорен орган по смисъла на член 17 от Регламент (ЕС) № 910/2014
Практика	„Информационно обслужване” АД в качеството му на доставчик на квалифицирани удостоверителни услуги, получил квалифицирания си статут от Надзорен орган.
Политика	Практика при предоставяне на квалифицирани удостоверителни услуги (Certification Practice Statement - CPS)
	Политика при предоставяне на квалифицирани удостоверения за квалифициран електронен подпис и квалифициран електронен печат (eIDAS-CP-QES)
	Политика при предоставяне на услуги за удостоверяване на време (eIDAS-CP-TS)
	Политика при предоставяне на квалифицирани удостоверения за усъвършенстван електронен подпис и усъвършенстван електронен печат (eIDAS-CP-AES);
	Политика при предоставяне на квалифицирани удостоверения за автентичност на уебсайт (eIDAS-CP-SSL).
PO	Регистриращ орган
YO	Удоверяващ орган
RSA Rivest-Shamir-Adelman	Криптографски алгоритъм (асиметричен)
SHA2 Secure Hash Algorithm	Хеш функция
SHA256/RSA Signature algorithm	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-I-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)	Удоверяващ орган
Common Name (CN)	Публично име
Certificate Policy (CP)	Политика за предоставяне на квалифицирано удостоверение за електронен подпис, електронен печат и автентичност на уебсайт
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 удостоверението
Enhanced key usage	Разширени цели за използването 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)
Public Key Infrastructure (PKI)
Registration Authority (RA/PO)

Серия стандарти в криптографията на публичния ключ
Инфраструктура на публичния ключ
Регистриращ орган

1. Въведение

Настоящият документ описва общите правила, прилагани от „Информационно обслужване“ АД при издаване и управление на квалифицирани удостоверения за усъвършенстван електронен подпис и за усъвършенстван електронен печат, както и приложимите за тях услуги и обхвата на приложимост

При издаване на квалифицирани удостоверения за усъвършенстван електронен подпис и за усъвършенстван електронен печат се прилагат процедури и практики, гарантиращи най-висока сигурност при издаване, публикуване и управление на издаваните квалифицирани удостоверения.

1.1. Общ преглед на политиката

Настоящата политика се отнася до квалифицираните удостоверения за усъвършенстван електронен подпис и за усъвършенстван електронен печат, 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.

Документът е структуриран в съответствие с препоръките, дефинирани в IETF RFC 3647 „Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework“.

Политиката е съобразена със следните документи:

- ETSI EN 319 401: „Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers“;
- ETSI EN 319 411-2 v2.1.1 „Policy and security requirements for Trust Service Providers issuing certificates. Requirements for trust service providers issuing EU qualified certificates“;
- ETSI EN 319 412-5: „Electronic Signatures and Infrastructures (ESI); Certificate Profiles, Part 5: QCStatements“;
- ETSI TS 101 456: „Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates“.

Издаването на квалифицирани удостоверения за усъвършенствани електронни подписи и усъвършенствани електронни печати се свързва с:

- издаване на квалифицирано удостоверение на физическо лице (Титуляр) - има характер на квалифицирано удостоверение за усъвършенстван електронен подпис;
- издаване на квалифицирано удостоверение за усъвършенстван електронен печат на юридическо лице (Създател на печат) - има характер на квалифицирано удостоверение за усъвършенстван електронен печат.

Достъпът до настоящия документ е публичен, като неговата актуална версия е публикувана на Интернет страницата на StampIT <https://www.stampit.org>.

„Информационно обслужване“ АД си запазва правото да извършва промени в настоящия документ по всяко време, като всяка промяна се отразява в нова актуална версия на документа, публикувана по горепосочения начин.

1.2. Наименование и идентификатор на политиката

Издаваните удостоверения съдържат идентификатор на политика, издаден в съответствие с препоръка IETF RFC 3647 [1.4], 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:

QCP-n

itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112)
policy-identifiers(1) qcp-natural (0)

QCP-l

itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112)
policy-identifiers(1) qcp-legal (1)

Обектните идентификатори (OID) в съответствие с вида на издаваните удостоверения са както следва:

Вид удостоверение	StampIT Policy Identifier	ETSI Policy Identifier
StampIT Enterprise Certificate	1.3.6.1.4.1.11290.1.2.1.5	0.4.0.194112.1.0
StampIT Enterprise Pro Certificate	1.3.6.1.4.1.11290.1.2.1.6	0.4.0.194112.1.0
StampIT Enterprise Seal Certificate	1.3.6.1.4.1.11290.1.2.1.7	0.4.0.194112.1.1

1.3. Участници в инфраструктурата на публичния ключ, поддържана от „Информационно обслужване“ АД

„Информационно обслужване“ АД е квалифициран доставчик на квалифицирани удостоверителни услуги, които отговарят на изискванията, посочени в Регламент (ЕС) № 910/2014 и действащото национално право. „Информационно обслужване“ АД предоставя квалифицирани удостоверителни услуги посредством **удостоверяващ орган** и мрежа от **регистращи органи**. Удостоверяващият орган и регистриращите органи извършват дейностите си по предоставяне на квалифицирани удостоверителните услуги от името и за сметка на „Информационно обслужване“ АД.

1.3.1. Удостоверяващ орган

StampIT е Удостоверяващият орган на „Информационно обслужване“ АД, който издава квалифицирани удостоверения за усъвършенстван електронен подпис (КУЕП-усъвършенстван) на физически лица, квалифицирани удостоверения за усъвършенстван електронен подпис (КУЕПТ-усъвършенстван) на юридически лица и квалифицирани удостоверения за усъвършенстван електронен печат (КЕВП-усъвършенстван). Удостоверяващият орган извършва дейности, които включват издаване, подновяване, спиране, възобновяване и прекратяване на квалифицирани удостоверения, водене на регистри и осигуряване на достъп до тях.

1.3.2. Регистриращи органи

Удостоверяващият орган издава КУЕП-усъвършенстван и КУЕПТ-усъвършенстван след извършване на проверка на идентичността на абоната. В тази връзка „Информационно

обслужване“ АД предоставя услугите си на абонатите чрез мрежа от Регистриращи органи, които имат следните функции:

- приемат, проверяват, одобряват или отхвърлят исканията за издаване на квалифицирани удостоверения в съответствие с вътрешните правила на StampIT;
- регистрират подадените искания за квалифицирани удостоверителни услуги на StampIT;
- участват във всички етапи при идентифицирането на Абонатите, както е определено от StampIT, в зависимост от типа квалифицирано удостоверение, което издават;
- позовават се на официални, нотариално заверени или други посочени документи, за да проверят искането, подадено от заявителя;
- след одобрение на искането, уведомяват StampIT за инициране на издаването на квалифицирано удостоверение;
- регистрират подадените заявки за подновяване, прекратяване, временно спиране и възобновяване на действието на квалифицирано удостоверение.

Регистриращите органи действат с одобрение и след оторизиране от страна на „Информационно обслужване“ АД, в съответствие с неговите практики и процедури.

1.3.3.Абонати

Абонатите са физически или юридически лица, които са подали искане и след успешно завършване на процедурата, им е бил издадено квалифицирано удостоверение. Преди да бъде извършена проверка и да му бъде издадено квалифицирано удостоверение, абонатът е само заявител за квалифицираните услуги на StampIT.

Отношенията между „Информационно обслужване“ АД, като доставчик на квалифицирани удостоверителни услуги и абоната, се уреждат с писмен договор.

1.3.4.Доверяващи се страни

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

За да бъде потвърдена валидността на квалифицираното удостоверение, което получават, доверяващите се страни трябва да се обръщат към StampIT директорията, която включва Списъци със спрените и прекратените квалифицирани удостоверения, всеки път преди да вземат решение дали да се доверят на информацията, посочена в тях.

1.4. Приложимост и ограничения за употреба на издаваните квалифицирани удостоверения

1.4.1. Приложимост

Издаваните квалифицирани удостоверения за усъвършенстван електронен подпис и за усъвършенстван електронен печат могат да се използват за създаване на електронно подписани документи и/или трансакции в информационни системи, гарантиращ високо ниво на информационна сигурност.

1.4.2. Ограничения

Забранено е използването на издаваните квалифицирани удостоверения извън предвидените в настоящата политика начини и цели. Забранено е използването на издаваните квалифицирани удостоверения за извършване на дейности, попадащи под ограниченията на законите на Република България и приложимите регламенти и директиви на Европейския съюз.

1.5. Утвърждаване, управление на версиите и съдържанието на настоящата политика

Политиката се разработва от квалифицирани служители на „Информационно обслужване“ АД в съответствие с приложимите регламентиращи документи в областта. Всяка нова версия влиза в сила след съгласуване с отдел „Правен“, ресорен директор на техническа дирекция и след утвърждаването ѝ от Изпълнителния директор на „Информационно обслужване“ АД.

Подходът за управление на версиите включва инкрементиране на мажорна версия (при прилагане на мажорни промени в документа) и инкрементиране на минорна версия – point release – за отстраняване на технически грешки и несъответствия.

След утвърждаване на версия, тя се публикува незабавно на Интернет страницата на StampIT.

Потребителите (абонати и доверяващи се страни) са длъжни да се съобразяват с актуалната версия на настоящата политика към момента на използване на услугите на доставчика.

Информация за връзка със StampIT:

Ул. „Лъчезар Станчев“ 11, ж.к. Изгрев

1756 София, България

Тел.: + 359 2 9656 291

Факс: + 359 2 9656 212

Web: <https://www.stampit.org>

E-mail: support@mail.stampit.org

2. Публични регистри и управление

2.1. Поддържани публични регистри

StampIT публикува издадените квалифицирани удостоверения в регистъра на издадените удостоверения. StampIT може да публикува квалифицираните удостоверения и в други регистри, които смята за подходящи, но не носи отговорност за валидността, точността и наличността на директории, поддържани от трети страни. Абонатите от своя страна могат също да публикуват квалифицираните удостоверения, издадени от StampIT в други регистри. Абонатът може да потисне публикуването на издаденото удостоверение в поддържаните регистри и изрично волеизявление при сключване на договора за квалифицирани удостоверителни услуги.

StampIT поддържа регистър на временно спрените и прекратени квалифицирани удостоверения – CRL.

StampIT поддържа интерфейс за статуса на издадените квалифицирани удостоверения – OCSP.

2.2. Честота на опресняване

Честотата на опресняване на публикуваните квалифицирани удостоверения е както следва:

	Адрес	Честота на публикуване
StampIT Global Root CA	http://www.stampit.org/crl/stampit_global.crl	365 дни
StampIT Global Qualified CA	http://www.stampit.org/crl/stampit_global_qualified.crl	Максимум 3 часа или незабавно при промяна
OCSP	http://ocsp.stampit.org	Реално време
Търсене в издадените удостоверения	https://stampit.org	Реално време

2.3. Достъп

StampIT осигурява HTTP/HTTPS(TLS) и OCSP базиран достъп до поддържаните регистри. Достъпът до публикуваната информацията не се ограничава, освен по искане на Титуляря/Създателя и само по отношение на негово валидно издадено квалифицирано удостоверение.

Информацията, публикувана в регистрите, е достъпна в режим 24x7, освен в случаите на събития, извън контрола на StampIT.

3. Идентификация и проверка на информацията за самоличност

3.1. Наименоване

В издаваните квалифицирани удостоверения се използват имената на Титуляря/Създателя и Абоната (когато е различен от Титуляря/ Създателя) според представени валидни официални документи и други идентификатори според типа на удостоверението. Включени са и обектни идентификатори в нотация ASN.1.

Имената в удостоверенията следват изискванията на ETSI EN 319 412, както и препоръките на RFC 5280. Допуска се и запис на DNS запис в съответствие с RFC 2247.

Полето „Subject“ съдържа наименованието на Титуляря/Създателя.

За всяко удостоверение се записва Distinguished Name (DN), формиращо се в съответствие с изискванията на X.520.

Издаването на квалифицирано удостоверение като използва „псевдоним“ се извършва само след като Регистриращия орган събере необходимата законово идентифицираща информация.

Използваната структура на DN е в съответствие с изискванията на X.520 и се състои минимум от следните елементи:

- C – двубуквено съкращение на името на страната според ISO 3166-1 alpha2
- CN – пълно име на физическото лице или на организацията
- GN – собствено име на физическото лице
- SN – фамилно име на физическото лице
- O – наименование на организацията, представлявана от лицето
- E – e-mail адрес на потребителя
- SerialNumber – уникален идентификатор на физическото лице
- Други полета, които се подробно описани в профилите на квалифицираните удостоверения

Титуляр/Създател с уникален DN може да има повече от едно издадено квалифицирано удостоверение в рамките на StampIT, но с различен SerialNumber. Комбинацията „Issuer“ и „SerialNumber“ гарантират уникалността на издаденото удостоверение в глобален мащаб.

Според вида на заявителя се извършват следните проверки:

- юридическо лице (Създател на печат), - осъществява се чрез проверка в съответните регистри по предоставен ЕИК, съответно БУЛСТАТ;
- упълномощен представител на юридическо лице (Титуляр) - осъществява се чрез проверка и заверка „Вярно с оригинала“ и саморъчен подпис върху изискуемите документи
- физическо лице (Титуляр) - осъществява се, чрез лично присъствие с документ за самоличност
- възможно е представяне на изискуемите документи неприсъствено (чрез упълномощено лице) - изисква се нотариална заверка на документите за упълномощаване;
- Проверката за валидност на представен документ за самоличност се извършва чрез регистъра на издадените лични документи, поддържан от Министерството на вътрешните работи
- Проверката на представителната власт на едно физическо лице спрямо юридическо лице се извършва чрез проверка в Търговския регистър/Регистър БУЛСТАТ към Агенцията по вписванията (за юридическите лица, регистрирани съгласно националното право)

3.2. Първоначална регистрация

Първоначалната регистрация се извършва по процедура, чиято цел е да се съберат всички необходими данни за идентификацията на лицето, преди да се пристъпи към фактическото издаване на квалифицираното удостоверение.

След проверка на предоставените данни и сключване на договор за квалифицирана удостоверителна услуга, лицето се включва като Потребител на услугите на StampIT.

3.2.1. Проверка за притежание на частен ключ

Услугите могат да се предоставят чрез локално или отдалечено генериране, в присъствието на специалист на StampIT на ключовата двойка.

За издаване или продължаване на действието на квалифицирано удостоверение е необходимо генерирането на електронно искане в PKCS#10 формат чрез системата на StampIT, подписано от Титуляря/Създателя, притежаващ частния ключ.

3.2.2. Проверка на юридическите лица

Представител на Регистриращия орган извършва по служебен път проверка в публичните регистри на юридическите лица – Търговски регистър/регистър БУЛСТАТ към Агенцията по вписванията.

При невъзможност за извършване на проверката, пред служител на РО следва да се представят:

- Удостоверение за актуално състояние, издадено от компетентен орган – оригинал или нотариално заверено копие;
- Уникален идентификатор, представящ юридическото лице пред органите на държавната власт.

3.2.3. Проверка на физическите лица, юридическите лица, представители на юридическо лице

С проверката на идентичността на юридическо лице се цели да се докаже, че по време на разглеждане на заявката юридическото лице съществува и че представляващото лице, което кандидатства за квалифицирано удостоверение притежава представителна власт да поиска издаването.

Пред служител на РО следва да се представят:

- Документ за самоличност на физическото лице, на което се издава КУЕП-усъвършенстван, което е асоциирано с юридическото лице – оригинал;
- Документ/пълномощно, от което произтича представителната власт на физическото лице спрямо юридическото лице – оригинал и копие, заверено от заявителя. Този документ е необходим в случай, че основанието за овластяване не е включено в другите документи за статуса на юридическото лице.

3.2.4. Проверка на физическите лица

Проверката на физическите лица се извършва от служители на РО чрез представяне пред РО на следните документи:

- Документ за самоличност (лична карта) на физическо лице – оригинал (при лично явяване на заявителя);
- Пълномощно с нотариална заверка на подписа (при заявяване чрез пълномощник);
- Документ за самоличност (лична карта) на физическото лице, упълномощено да представлява заявителя – оригинал.

3.2.5. Проверка от удостоверяващия орган

След успешното приключване на процесите по идентификация и проверка от Регистриращия орган на лицата и условията за издаване или управление на квалифицирано удостоверение, Удостоверяващият орган публикува незабавно издаденото квалифицирано удостоверение в Публичния регистър/Хранилището на издадените удостоверения, достъпно чрез OCSP или съответно в Списъка със спрени и прекратени удостоверения - CRL.

3.3. Подновяване на квалифицираното удостоверение

Периодът на валидност на квалифицираното удостоверение е отбелязан в съответното поле на удостоверението. Тъй като изискванията за подновяване могат да се различават от тези при първоначално издаване, StampIT публикува и актуализира условията за подновяване на квалифицираните удостоверения, издадени от него. Подновяване може да бъде извършено само ако квалифицираното удостоверение е издадено със срок на валидност 1 (една) година или 3 (три) години и всички данни в удостоверението останат непроменени, както са заявени в първоначалното искане.

Подновяването на квалифицирано удостоверение, издадено от StampIT се извършва в съответствие с условията, действащи към момента на подновяване и действащите нормативни изисквания.

Абонатът трябва постоянно да контролира верността и точността на информацията, публикувана в подновеното квалифицирано удостоверение. Искане за подновяване трябва да бъде получено от StampIT преди датата на изтичане на срока на валидност, вписан в удостоверението.

Когато има промени в заявените обстоятелства, вписани в квалифицираното удостоверение, задължително се генерира нова ключова двойка (rekey).

3.4. Временно спиране и прекратяване на действието на квалифицираното удостоверение

Временното спиране на квалифицирано удостоверение цели да бъде временно спряна неговата употреба.

Прекратяването на квалифицирано удостоверение спира за постоянно действието на удостоверението.

StampIT временно спира или прекратява действието на квалифицирано удостоверение при:

- наличие на основателни сведения и обстоятелства от които е видно, че има загуба, кражба, промяна, неоторизирано разкриване или друго компрометиране на частния ключ;

- Титулярят/Създателят, съответно Абонатът е нарушил задълженията си по настоящата политика и практиката на StampIT;
- Титулярят/Създателят, съответно абонатът е нарушил задълженията си по договора за предоставяне на квалифицирани удостоверителни услуги;
- изпълнението на някое задължение по настоящата политика и практиката на StampIT е било забавено или не е било изпълнено поради природно бедствие, повреда в компютрите или комуникациите или друга причина, която е извън човешкия контрол и като резултат информацията на друго лице е заплашена или компрометирана;
- има промяна в информацията, която се съдържа в квалифицираното удостоверение на Абоната;
- по искане на посочени в нормативен акт органи.

3.4.1. Заявка за временно спиране или прекратяване

Абонатът или орган, посочен в нормативен акт може да поиска временно спиране или прекратяване на действието на квалифицираното удостоверение.

Идентичността на заявителя и представителната му власт ще бъде потвърдена, в зависимост от естеството на изисканото действие.

3.4.2. Ефект от временното спиране или прекратяване

За периода на временното спиране или при прекратяването на квалифицираното удостоверение валидността му незабавно се счита за прекратена.

Действието на удостоверението се възобновява с изтичане на срока на спиране, при отпадане на основанието за спиране или по искане на Абоната в съответствие с нормативната уредба.

Удостоверението се включва в CRL списъка със съответната причина (Reason) за спиране/прекратяване незабавно.

3.4.3. Уведомяване при спиране и прекратяване на квалифицирано удостоверение

StampIT уведомява абоната за прекратяване или спиране на квалифицирано удостоверение и за причините за прекратяване или спиране чрез средства за комуникация, които смята за подходящи.

3.5. Идентификация и проверка на самоличност след прекратяване на издадено квалифицирано удостоверение

Не се допуска подновяване или преиздаване на квалифицираното удостоверение след прекратяването му.

В случай на искане от страна на Титулярят/Създателят за издаване на ново квалифицирано удостоверение се спазва процедурата за първоначално създаване на квалифицирано удостоверение.

4. Оперативни дейности

Дейностите, свързани с предоставянето на удостоверителни услуги се изпълняват по следните процедури:

- регистрация и обработка на искане за издаване на квалифицирано удостоверение
- издаване на квалифицирано удостоверение
- предаване на Абоната на издаденото квалифицирано удостоверение
- подновяване на квалифицирано удостоверение чрез запазване (renew) или генериране на нова ключова двойка (rekey)
- спиране/възобновяване действие на квалифицирано удостоверение
- прекратяване на квалифицирано удостоверение

Регистрация

Искане за регистрация на Абонат на квалифицирани удостоверителни услуги се подава към Регистриращия орган от физически, юридически или упълномощени от тях лица и включва

следната информация:

- пълно наименование на Титуляря/Създателя или на упълномощен представител на юридическото лице
- пълно наименование на юридическото лице, асоциирано с Титуляря
- доказателства за представителна власт на Титуляря спрямо юридическото лице – където е приложимо
- идентификатори: ЕИК, ЕГН, БУЛСТАТ и др.;
- пълен пощенски адрес на лицето
- телефон за връзка
- e-mail адрес
- вид на исканото квалифицирано удостоверение
- идентификатор (OID) на политиката, въз основа на която се издава удостоверението
- частен ключ и съответстващ на публичен ключ
- допълнителна информация, заявена за включване в удостоверението
- подписване на Договор за квалифицирани удостоверителни услуги и съгласие с условията на тази Политика и Практиката при предоставяне на квалифицирани удостоверителни услуги

Подновяване

Подновяване може да се извърши само при налично валидно квалифицирано удостоверение от Титуляря/Създател, спазвайки тази Политика и Практиката на StampIT.

Подновяването на квалифицирано удостоверение запазва информацията за Титуляря/Създателя от текущото удостоверение, като в подновеното удостоверение се променя единствено периода на валидност.

Прекратяване

Искане за прекратяване от Абонат на квалифицирано удостоверение се подава към Регистриращия орган от физически, юридически или упълномощени от тях лица лично в РО.

StampIT може да извърши прекратяване на квалифицирано удостоверение в следните случаи:

- смърт/поставяне под запрещение на Титуляр/Създател
- прекратяване на представителната власт на Титуляря спрямо Абоната
- установяване на неверни данни при издаване на удостоверението
- установена невярна удостоверена информация;
- при промяна в удостоверена вече информация на Титуляр/Създател
- компрометиране на частен ключ
- забавяне в заплащането на дължимо възнаграждение
- искане за прекратяване от страна на Титуляр/Създател

Абонатът или негов законен представител е длъжен да информира StampIT при настъпване на някое от гореописаните събития.

Услугите по прекратяване на квалифицирани удостоверения са достъпни в режим 24x7.

4.1. Валидна употреба на издаваните квалифицирани удостоверения

4.1.1. От страна на абонатите

Абонатите са длъжни да използват издадените им квалифицирани удостоверения само в съответствие с Политиката според тяхното предназначение, в срока на тяхната валидност и в случай, че не са спрени/прекратени.

Отговорността за използването на частния ключ е на Титуляря/Създателя.

4.1.2. От страна на доверяващите се страни

Доверяващите се страни трябва да използват публичните ключове и съответните им удостоверения само в съответствие с тяхното предназначение, след извършването на следните проверки:

- проверка на статуса на удостоверението чрез OCSP или CRL
- проверка на електронния подпис на Удостоверяващия орган, включително и неговия статус чрез OCSP или ARL
- проверка на времевата валидност на удостоверението

4.2. Подновяване и преиздаване на квалифицирани удостоверения

Подновяване на квалифицирани удостоверения, издаден от StampIT, може да бъде извършено само, ако всички данни в удостоверението са непроменени, както в първоначалното искане за издаване. Съдържанието на подновеното квалифицирано удостоверение е идентично с това на текущото удостоверение с изключение на срока на валидност, който започва да тече от датата на подновяване, вписана в удостоверението.

В съответствие с изискванията за подновяване Регистриращия орган на StampIT може да изиска актуални документи, доказващи точността и верността на информацията, включена в съдържанието на квалифицираното удостоверение към текущия момент.

Заявителят декларира, че данните предоставени при първоначално издаване и тези, вписани в квалифицираното удостоверение са точни, верни и непроменени към настоящия момент.

При наличие на промени в данните и обстоятелствата, касаещи физическото и/или юридическото лице, заявителят следва да подаде искане за издаване на ново квалифицирано удостоверение.

Документите, необходими за подновяване на квалифицирани удостоверения са публикувани на Интернет страницата на StampIT: <https://www.stampit.org>.

4.2.1. Процедура по подновяване на квалифицирани удостоверения

Следните стъпки описват процеса по подновяване:

1. Заявителят подава "Искане за подновяване", придружено с документите за подновяване, като се явява лично, чрез надлежно овластен представител или по електронен път, като използва валидно квалифицирано удостоверение за електронен подпис.
2. Проверява се самоличността, съответно идентичността на заявителя и съответствието на данните и обстоятелствата, касаещи Абоната към момента на подновяване.
3. Операторът на Регистриращия орган на StampIT проверява представените документи и подава искането за подновяване на квалифицираното удостоверение до Удостоверяващия орган.
4. Удостоверяващият орган подновява квалифицираното удостоверение, което се изпраща обратно на Регистриращия орган на StampIT известява абоната относно наличието на подновеното квалифицирано удостоверение.
5. Квалифицираното удостоверение се записва на сигурно устройство за създаване на електронен подпис/ електронен печат.
6. Подновеното квалифицирано удостоверение се публикува в поддържания от StampIT публичен регистър.

Подновяване на квалифицирано удостоверение може да бъде извършено само за удостоверения, които са валидни към момента на подаване на заявката към Удостоверяващия орган. По тази причина искането за подновяване, както и необходимите документи, трябва да бъдат получени в Регистриращия орган преди изтичане на срока на валидност на квалифицираното удостоверение.

4.3. Промяна на информация в квалифицираните удостоверения

Не се допуска промяна в информацията за вече издадено и публикувано квалифицирано удостоверение.

При изявено желание от страна на Абоната, издаденото квалифицирано удостоверение може да бъде прекратено и да бъде издадено ново, с нова ключова двойка и срещу заплащане, спазвайки процедурата за първоначално издаване.

4.4. Спиране на квалифицираните удостоверения

Действието на квалифицирано удостоверение, издадено от StampIT, може да бъде спряно при наличие на съответните основания, за необходимия според обстоятелствата срок, но за не повече от 48 часа.

За периода на временно спиране на квалифицираното удостоверение, същото се счита за невалидно.

4.4.1. Основания за спиране

Действието на квалифицирано удостоверение, издадено от StampIT може да бъде спряно:

1. По искане на Абоната. Искането може да бъде подадено както в Регистрираш орган на доставчика, така и чрез други средства за комуникация, включително телефон, факс, електронна поща.
2. По искане на лице, за което според обстоятелствата е видно, че може да знае за нарушения на сигурността на частния ключ, като представител, съдружник, служител, член на семейството и др.
3. По разпореждане от страна на Надзорен орган – при непосредствена опасност за интересите на трети лица или при наличие на достатъчно данни за нарушение на закона.

4.4.2. Процедура за спиране

Следните стъпки описват процеса по спиране на действието на квалифицирано удостоверение:

1. Удостоверяващият орган получава искането за спиране.
2. Удостоверяващият орган спира действието на удостоверението, като го включва в списъка с прекратените квалифицирани удостоверения, който е публично достъпен.
3. Удостоверяващият орган незабавно уведомява абоната и титуляря/ създателя за спирането на действието на квалифицираното удостоверение.

4.5. Възобновяване на квалифицираните удостоверения

Действието на квалифицирано удостоверение се възобновява с изтичане на срока на спиране, при отпадане на основанията за спиране или по искане на абоната, след като StampIT, съответно Надзорният орган се увери, че той е узнал причината за спирането и искането за възобновяване е направено вследствие на узнаването.

Удостоверяващият орган възобновява действието на квалифицираното удостоверение, като го изважда от списъка с прекратените квалифицирани удостоверения.

4.5.1. Основания за възобновяване

1. По разпореждане на Надзорен орган – когато причината за спирането на действието е разпореждане на Надзорен орган.
2. След изтичане на срока на спиране на действието на удостоверението.
3. По искане от страна на Абоната.

4.5.2. Процедура за възобновяване

1. По разпореждане на Надзорен орган – StampIT получава разпореждането на Надзорния орган за възобновяване на действието на квалифицираното удостоверение. Удостоверяващият орган възобновява действието на удостоверението, като го изважда от списъка на спрените и прекратените квалифицирани удостоверения.
2. След изтичане на срока на спиране на действие на удостоверението – след изтичане на 48 часа от момента на спиране на действието на квалифицираното удостоверение, неговото действие се възобновява автоматично от Удостоверяващия орган, ако до този момент не е получена валидна заявка за прекратяване по реда за прекратяване на действието на квалифицираното удостоверение.
3. По искане от страна на абоната – след като StampIT се увери, че той е узнал причината за спирането и искането за възобновяване е направено вследствие на узнаването. Искането за възобновяване на действието на квалифицираното удостоверение от страна на абоната се реализира по следната процедура:
 - заявителят/ овластеният/ упълномощеният представител на заявителя се явява лично пред Регистриращия орган и подава “Искане за възобновяване”, придружено с документите, доказващи неговата самоличност и представителната му власт;
 - операторът на Регистриращия орган проверява представените документи и подава заявка за възобновяване на квалифицираното удостоверение до Удостоверяващия орган;
 - Удостоверяващият орган възобновява действието на квалифицираното удостоверение.

Ако в периода на спиране на квалифицираното удостоверение в Удостоверяващия орган се получи валидна заявка за прекратяване на действието му, то StampIT прекратява удостоверението в съответствие с утвърдените процедури.

4.6. Прекратяване на квалифицираните удостоверения

Прекратяване на действието на квалифицирано удостоверение се извършва от StampIT след подаване на заявка за прекратяване от страна на Регистриращия орган. За да направи тази заявка, операторът на Регистриращия орган е длъжен да се увери в самоличността на заявителя/ на овластения/упълномощения представител на заявителя, както и в представителната власт на овластения/упълномощения представител на заявителя. Искане за прекратяване може да бъде подадено към Регистриращ орган от Абоната.

4.6.1. Основания за прекратяване

Основанията за прекратяване на действието на квалифицирано удостоверение могат да бъдат, но не са ограничени до следните:

1. Налице са основателни сведения и обстоятелства от които е видно, че има загуба, кражба, промяна, неоторизирано разкриване или друго компрометиране на частния ключ.
2. Прекратяване на представителната власт на физическото лице спрямо юридическото лице, вписано в съдържанието на удостоверението.
3. Прекратяване на юридическото лице на абоната.
4. Смърт или поставяне под запрещение на физическото лице.
5. Установяване, че квалифицираното удостоверение е издадено въз основа на неверни данни.
6. При промяна в информацията, която е подадена първоначално и се съдържа в квалифицираното удостоверение на абоната.
7. При неизпълнение на задълженията на абоната по договора за квалифицирани удостоверителни услуги.
8. По искане на абоната, след проверка на самоличността и представителната власт на заявителя.

Действието на всички квалифицирани удостоверения, издадени от StampIT, се прекратява безусловно при прекратяване на дейността на StampIT.

Документите, необходими за прекратяване/спиране на квалифицирани удостоверения са публикувани на Интернет страницата на StampIT: <https://www.stampit.org>.

4.6.2. Процедура за прекратяване

Следните стъпки описват процеса по прекратяване на квалифицирано удостоверение:

1. Заявителят/ овластеният/ упълномощеният представител на заявителя се явява лично пред Регистриращия орган и подава "Искане за прекратяване", придружено с документите, доказващи неговата самоличност и представителната му власт.
2. Операторът на Регистриращия орган проверява идентичността на заявителя и представителната му власт към момента на подаване на "Искане за прекратяване".
3. Операторът на Регистриращия орган подава заявка за прекратяване до Удостоверяващия орган.
4. Удостоверяващият орган прекратява квалифицираното удостоверение.
5. Прекратеното удостоверение се включва в поддържащия от StampIT списък на спрените и прекратените квалифицирани удостоверения, който е публично достъпен.

4.7. Статус на издаваните квалифицирани удостоверения

Информацията за състоянието на издадените от StampIT квалифицирани удостоверения е достъпна в режим 24x7, както следва:

4.7.1. Автоматизирано, чрез Списъка със спрени и прекратени удостоверения (CRL)

StampIT поддържа списъци със спрените и прекратените удостоверения, достъпен на Интернет страницата на Доставчика, в съответствие с изискванията на RFC 6818. CRL списъците се опресняват минимум на 3 часа или незабавно, при настъпване на събитие. Конкретните адреси на CRL списъците са налични в CRL Distribution Point (CDP) атрибута на удостоверенията.

4.7.2. Автоматизирано, чрез Протокола за онлайн проверка на статуса на удостоверенията (OCSP)

StampIT поддържа автоматизирана услуга за проверка на статуса на издадените удостоверения (OCSP) в съответствие с изискванията на RFC 6960.

Адресът за проверка на статуса на издаваните удостоверения е описан в Authority Information Access (AIA) разширението на квалифицираните удостоверения.

4.7.3. Ръчно, чрез Интернет страницата на StampIT

StampIT поддържа web базиран интерфейс за ръчна проверка на състоянието на издаваните удостоверения, достъпен на адрес <https://www.stampit.org>.

5. Физическа и организационна сигурност

5.1. 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.

„Информационно обслужване“ АД е внедрило и 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.

5.1.1. Сигурни помещения

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.

5.1.2. Съхранение на данни

Изградено е специално оборудвано архивно помещение за съхранение на клиентските данни. Техническите носители се съхраняват в огнеупорни каси.

5.1.3. Сигурно унищожаване на данни

При унищожаване на данни се спазват политиките за сигурност на Дружеството. За хартиените носители се прилага нарязване чрез шредери с високо ниво на сигурност, а за техническите носители на данни се прилага DBAN метод и физическо унищожаване на носителя. Дейностите се документират по надлежен ред, като се регистрира одитна следа за извършените действия.

5.2. Организационна сигурност

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.

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.

5.3. 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.

5.3.1. Обучение на персонала

Служителите, работещи по управлението и оперирането (PO) на инфраструктурата на StampIT преминават на обучение по практиката и политиките за издаване на различните видове удостоверения и администриране на различните типове криптографски устройства. В обучението се включват и изискванията на Интегрираната система за управление, съответстващи на ролята на служителя.

Разработена е и специфична технологична документация, описваща технологичните параметри на специализирания софтуер за управление на инфраструктурата и необходимите клиентски инсталации.

Компанията разработва планове за технологично развитие и специализирани обучения на служителите. За всяко преминало обучение се извършва оценка на въздействието в работата и осъзнатостта на служителите.

5.4. Управление на записи и журнали

Управлението на събитията, записващи действията на потребители, изключителни случаи, грешки и събития, свързани със сигурността на информацията, се извършва според разработена работна инструкция „Управление на събитията“. Регистрираните събития могат да се използват при бъдещи анализи и наблюдение на механизмите за контрол на достъпа.

Одиторският екип в „Информационно обслужване“ АД извършва редовни проверки за спазване на въведените механизми, контроли и процедури съгласно „Практиката при предоставяне на квалифицирани удостоверителни услуги“, Регламент (ЕС) № 910/2014 и действащото национално законодателство. Одиторският екип оценява ефективността на съществуващите процедури за сигурност.

5.5. Управление на архивите

Информацията за значимите събития се архивира в електронен вид периодично, спрямо предварително утвърден „План за бекъп“.

„Информационно обслужване“ АД архивира всички данни и файлове, свързани с:

- информацията при регистрация
- със сигурността на системата
- всички искания, подадени от потребителите
- цялата информация за потребителите
- всички ключове, използвани от Удостоверяващите органи и от Регистриращия орган
- цялата кореспонденция между StampIT и абонатите
- всички документи и данни, използвани в процеса на проверка на самоличността

Дружеството съхранява архивите във формат, позволяващ възпроизвеждане и възстановяване.

5.6. Прекратяване на дейността на Удостоверяващия орган

В случай на прекратяване на дейността на Удостоверяващия орган, 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 Удостоверяващ орган, StampIT извършва следните действия:

- информира за намеренията си Надзорния орган и абонатите, които имат валидни квалифицирани удостоверения, най-късно четири месеца преди датата на прекратяване на дейността си;

- прекратява всички квалифицирани удостоверения, които все още не са прекратени или са все още валидни в края на четиримесечния период от време, без да иска съгласието на абонатите си - 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 удостоверителни услуги 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.

6. Управление на техническата сигурност

6.1. Генериране и привеждане в оперативен режим на ключовата двойка на Удостоверяващ орган

StampIT използва надежден процес за генериране, за да генерира частните си ключове. StampIT поделя частните си ключове на 3 (три) секретни части. StampIT е законният собственик и притежател на частните ключове, за които използва процедурата за разпределяне на секретни части. StampIT има правото да прехвърля такива секретни части на различни лица, които са изрично упълномощени.

StampIT генерира по сигурен начин и защитава собствените си частни ключове, 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.

StampIT използва тройно поделяне на секретни части и ги разпределя между упълномощени лица, които се грижат за съхраняването на секретните части, с цел да повиши доверието в Удостоверяващия орган при висока степен на сигурност и за да осигури възстановяване на ключовете.

6.2. Генериране на ключовата двойка на Абонат

Ключовата двойка на Абоната се генерира в сигурна среда, в съответствие с изискванията на Регламент (ЕС) № 910/2014 и ETSI спецификациите. Генерирането на ключовата двойка може да стане при Абоната, спазвайки горните изисквания, или при PO на StampIT, в присъствието на Абоната. Ключовата двойка може да се генерира и чрез устройство за създаване на усъвършенстван електронен подпис/печат (QSCD), проверено за ниво на сигурност и за оперативна съвместимост със системите на StampIT.

Контролът върху частния ключ се осъществява с код за достъп – ПИН код или еквивалентен.

Абонатът носи отговорност за защитата на управлението от него частен ключ.

6.2.1. Изисквания към устройствата

Удостоверяващият орган на StampIT одобрява директно или чрез оторизирани консултанти хардуера и софтуера, които той използва, за да предоставя квалифицирани удостоверителни услуги.

6.2.2. Предоставяне на ключовата двойка на Абоната

Титулярят/Създателят или упълномощено от него лице получава частния ключ и издаденото квалифицирано удостоверение върху устройство за създаване на електронен подпис/печат в Регистриращия орган на доставчика. При първоначално издаване на удостоверение върху устройство за създаване на електронен подпис/печат, след генериране на двойка ключове, устройството се инициализира и се създават следните кодове за достъп: Потребителски ("User") и Административен ("SO"). Потребителският код за достъп се:

- генерира от Титулярят/Създателят в Регистриращ офис на StampIT;
- предоставя първоначален случайно генериран ПИН код на Титуляря/Създателя или на упълномощеното от него лице в запечатан, непрозрачен хартиен плик. Титулярят/Създателят е задължен на смени своя първоначален Потребителски код за достъп до устройството посредством софтуера, който се предоставя с него. StampIT препоръчва Титуляря/Създателя да сменя периодично своя Потребителски ПИН код за достъп.

В случай на определен брой неуспешни опити за въвеждане на коректен код за достъп до частния ключ на Титуляря/Създателя, достъпът до него се блокира. В такива случаи Титулярят/Създателят или надлежно овластен пълномощник трябва да посети Регистриращ офис на StampIT, представи документ за самоличност и устройство за създаване на електронен подпис/печат. Оператор на StampIT предоставя възможност за ново генериране на ПИН код от страна на Титулярят/Създателят или предоставя нов случайно генериран ПИН код.

При желание от страна на Титуляря/Създателя, StampIT може да предостави Административен ("SO") за деблокиране на блокирано устройство за създаване на електронен подпис/печат.

6.2.3. Минимални дължини на ключовите двойки

Дължината на ключовата двойка за усъвършенстван електронен подпис и усъвършенстван електронен печат, генерирана чрез инфраструктурата на StampIT е минимум 2048 bits, с комбинация на хеш и асиметрични алгоритми sha256-with-RSA.

6.2.4. Параметри на публичния ключ

Абонатът е отговорен за проверката на качеството на параметрите на генерирания частен ключ. Той е длъжен да провери способността на ключа да създава валиден усъвършенстван електронен подпис/ усъвършенстван електронен печат и неговата последваща верификация.

Предоставяните от StampIT устройства са с ниво на сигурност CC EAL 4+ и FIPS 140-2 Level 3.

Всички устройства за създаване на усъвършенстван електронен подпис и усъвършенстван електронен печат (QSCD), използвани от Абоната извън инфраструктурата на StampIT трябва да са сертифицирани за ниво на сигурност CC EAL 4+ и по-високо.

6.2.5. Управление на частния ключ

6.2.5.1. Съхранение на частния ключ

Абонатът е длъжен да съхранява частния ключ в надеждна система, гарантираща неговата сигурност. Когато StampIT генерира ключовата двойка, при поискване от страна на Абоната, частният ключ се предава в защитен вид на Абоната.

StampIT не създава копия на частните ключове на Абоната.

6.2.5.2. Активиране на частния ключ

Активирането на частния ключ трябва да се извършва чрез въвеждане на валиден ПИН код, даващ достъп до функционалността за извършване на криптографски операции с частния ключ.

6.2.5.3. Деактивиране на частния ключ

Деактивирането се извършва чрез съответната функционалност на средата, в която се съхранява частния ключ.

6.2.5.4. Унищожаване на частния ключ

Извършва се чрез функционалността на средата, съхраняваща частния ключ. След изпълнението на тази операция използването на удостоверението трябва да бъде невъзможно.

6.3. Управление на ключовата двойка

6.3.1. Архивиране на публичния ключ

Публичните ключове на Абонатите са налични в регистрите на StampIT. Регистрите на доставчика се архивират по процедурите за управление на информационната сигурност, изпълнявани и наблюдавани от експертния състав на StampIT.

6.3.2. Валидност и употреба на издаваните удостоверения

Периода на употреба на публични ключове се определя от стойностите на полетата в удостоверението му, описващо валидността на публичния ключ – ValidFrom и ValidTo. Валидността на удостоверенията и съответните им частни ключове може да бъде и по-кратка в случай на прекратяване.

6.4. Активиране на частния ключ

При извършване на дейности в Регистриращия орган, данните за активиране на частен ключ се въвеждат от Потребителя по защитен начин, в присъствие на оператор.

Когато Абонатът генерира ключовата двойка за квалифицирано удостоверение е отговорност на Абоната управлението на данните за активиране.

6.4.1. Генериране и предоставяне на данни за активиране

Двойката ключове на Титуляр/Създател на квалифицирано удостоверение за усъвършенстван електронен подпис/печат се генерира в одобрено от StampIT устройство за създаване на усъвършенстван електронен подпис/печат (външно), проверено за ниво на сигурност и за успешна работа в инфраструктурата на StampIT за издаване и управление на квалифицирани удостоверения за усъвършенстван електронен подпис/печат. Когато генерирането се извършва в среда под контрола на Абоната, то той е отговорен за изпълнението на изискванията на изискванията на Регламент (ЕС) № 910/2014 и ESTI спецификациите в тази област.

6.4.2. Защита на данни за активиране

Титулярят/Създателят е задължен да съхранява и пази от компрометиране кодовете за достъп до устройствата и средите за създаване на усъвършенстван електронен подпис/печат.

Доставчикът препоръчва данните за активиране на устройството никога да не се съхраняват заедно със самото устройство или в средата.

6.5. Сигурност на използваните компютърни системи

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 заложили 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.

6.6. Управление на промените в системата на StampIT

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.

6.7. Управление на мрежовата сигурност

„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.

7. Профили на удостоверенията

7.1. Профил на StampIT базово (Root) удостоверение на „Информационно обслужване“ АД

StampIT Global Root CA			
Signature Algorithm	SHA256/RSA		
Issuer	CN	StampIT Global Root CA	Име
	C	BG	Държава
	O	Information Services JSC	Организация
	L	Sofia	
	2.5.4.97 (organizationIdentifier)	NTRBG-831641791	ЕИК
Validity	20 години		
Subject	CN	StampIT Global Root CA	Име
	C	BG	Държава
	O	Information Services JSC	Организация
	L	Sofia	Област
	2.5.4.97 (organizationIdentifier)	NTRBG-831641791	ЕИК
Public Key	RSA 4096 bits		
Key Usage (Critical)	Certificate Signing, Off-line CRL Signing, CRL Signing (06)		
Friendly Name	StampIT Global Root CA		
Basic constrains (Critical)	Subject Type=CA Path Length Constraint=0		
Certificate Policies (Non Critical)	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.11290.1.2 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.stampit.org/repository/		

7.2. Профил на StampIT Оперативно (subordinate) удостоверение на
„Информационно обслужване“ АД

StampIT Global Qualified CA			
Signature Algorithm	SHA256/RSA		
Issuer	CN	StampIT Global Root CA	Име
	C	BG	Държава
	O	Information Services JSC	Организация
	L	Sofia	
	2.5.4.97 (organizationidentifier)	NTRBG-831641791	ЕИК
Validity	20 години		
Subject	CN	StampIT Global Qualified CA	Име
	C	BG	Държава
	O	Information Services JSC	Организация
	L	Sofia	Област
	2.5.4.97 (organizationidentifier)	NTRBG-831641791	ЕИК
Public Key	RSA 4096 bits		
Key Usage (Critical)	Certificate Signing, Off-line CRL Signing, CRL Signing (06)		
Friendly Name	StampIT Global Qualified CA		
Basic constrains (Critical)	Subject Type=CA Path Length Constraint=0		
Authority Information Access	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://www.stampit.org/repository/stampit_global_root_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.stampit.org/		
CRL Distribution Point /Non Critical/	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.stampit.org/crl/stampit_global.crl		
Certificate Policies (Non Critical)	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.11290.1.2.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.stampit.org/repository/		

7.3. Профил на квалифицирано удостоверение за усъвършенстван електронен подпис StampIT Enterprise, което се издава на физическо лице /natural person/

Профил на StampIT Enterprise			
Signature Algorithm	SHA256withRSA		
Issuer	CN	StampIT Global Qualified CA	
	C	BG	
	O	Information Services JSC	
	L	Sofia	
	OrganizationIdentifier (2.5.4.97)	NTRBG-831641791	
Validity	срок, определен в договора за удостоверителна услуга (една или три)		
Subject	*C	Country	Държава
	L	Locality	Град/Област
	*CN	Common Name	Пълно име или Friendly name
	*G	Given	Име на физическото лице, изписано на латиница
	*Sn	SurName	Фамилия на физическото лице, изписано на латиница
	Pseudonym (2.5.4.65)	Pseudonym	Псевдоним
	*E	E-mail	Пощенски адрес
	*SerialNumber		Уникален идентификатор за физическото лице: За български гражданин: PNOBG-xxxxxxxx /ЕГН/ PASBG-xxxxxxxx /номер на паспорт/ TINBG-xxxxxxxx/ДДС номер/ За чуждестранно лице: PNOYY-xxxxxxxx /ЕГН/ PASYY-xxxxxxxx /номер на паспорт/ IDCYY-xxxxxxxx /национална карта/ YY- код на държава
	Public Key	RSA 2048 bits	
Key Usage (Critical)	Digital Signature Non-Repudiation Key Encipherment		
Authority Information Access	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://www.stampit.org/repository/stampit_global_qualified.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.stampit.org/		
Extended key usage (Non Critical)	Client Authentication E-Mail Protection Smart Card Logon Document Signing		
Qualified Certificate Statement (Non Critical)	id-etsi-qcs-semanticId-Natural(oid=0.4.0.194121.1.1)		
	id-etsi-qcs-QcCompliance (oid=0.4.0.1862.1.1)		

	id-etsi-qct-esign (oid=0.4.0.1862.1.6.1) id-etsi-qcs-QcPDS(oid=0.4.0.1862.1.5) PdsLocation=https://www.stampit.org/pds/pds_en.pdf language=en
Basic constrains (Critical)	End entity
CRL Distribution Point/Non Critical/	DP Name: http://www.stampit.org/crl/stampit_global_qualified.crl
Certificate Policies (Non Critical)	[1] Certificate Policy: Policy Identifier=0.4.0.194112.1.0 [2] Certificate Policy: Policy Identifier=1.3.6.1.4.1.11290.1.2.1.5 Policy Qualifier Id=CPS/1.3.6.1.5.5.2.7.1/ Qualifier=http://www.stampit.org/repository [3] Certificate Policy: Policy Identifier= 0.4.0.1456.1.2

7.4. Профил на квалифицирано удостоверение за усъвършенстван електронен подпис за физическо лице, асоциирано с юридическо /legal person/ StampIT Enterprise Pro

Профил на Enterprise Pro			
Signature Algorithm	SHA256withRSA		
Issuer	CN	StampIT Global Qualified CA	
	C	BG	
	O	Information Services JSC	
	L	Sofia	
	OrganizationIdentifier (2.5.4.97)	NTRBG-831641791	
Validity	срок, определен в договора за удостоверителна услуга (една или три години)		
Subject	*C	Country	Държава
	L	Locality	Град/Област
	*CN	Common Name	Пълно име или Friendly name
	*G	Given	Име на физическото лице, изписано на латиница
	*Sn	SurName	Фамилия на физическото лице, изписано на латиница
	Pseudonym (2.5.4.65)	Pseudonym	Псевдоним
	*E	E-mail	Пощенски адрес
	*SerialNumber		Уникален идентификатор за физическото лице: За български гражданин: PNOBG-xxxxxxxx /ЕГН/ PASBG-xxxxxxxx /номер на паспорт/ TINBG-xxxxxxxx/ДДС номер/ За чуждестранно лице: PNOYY-xxxxxxxx /ЕГН/ PASYY-xxxxxxxx /номер на паспорт/

			IDCYY-xxxxxxxx /национална карта/ YY- код на държава
	O	Organization	Име на юридическо лице
	*OrganizationIdentifier (2.5.4.97)	2.5.4.97	Идентификатор за юридическо лице NTRYY-xxxxxxxx /национален идентификационен код/ VATYY-xxxxxxxx /Данъчен номер/ YY – код на държава
Public Key	RSA 2048 bits		
Key Usage (Critical)	Digital Signature Non-Repudiation Key Encipherment		
Authority Information Access	<p>[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.stampit.org/</p> <p>[2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://stampit.org/repository/stampit_global_qualified.crt</p>		
Extended key usage (Non Critical)	Client Authentication E-Mail Protection Smart Card Logon Document Signing		
Qualified Certificate Statement (Non Critical)	<p>id-etsi-qcs-semanticId-Natural(oid=0.4.0.194121.1.1)</p> <p>id-etsi-qcs-QcCompliance (oid=0.4.0.1862.1.1)</p> <p>id-etsi-qct-esign (oid=0.4.0.1862.1.6.1)</p> <p>id-etsi-qcs-QcPDS(oid=0.4.0.1862.1.5)</p> <p>PdsLocation=https://www.stampit.org/pds/pds_en.pdf</p> <p>language=en</p>		
Basic constrains (Critical)	End entity		
CRL Distribution Point/Non Critical/	DP Name: http://www.stampit.org/crl/stampit_global_qualified.crl		
Certificate Policies (Non Critical)	<p>[1] Certificate Policy: Policy Identifier=1.3.6.1.4.1.11290.1.2.1.6 Policy Qualifier Id=CPS/1.3.6.1.5.5.2.7.1/ Qualifier=http://www.stampit.org/repository</p> <p>[2] Certificate Policy: Policy Identifier= 0.4.0.1456.1.2</p> <p>[3] Certificate Policy: Policy Identifier=0.4.0.194112.1.0</p>		

**7.5. Профил на квалифицирано удостоверение за усъвършенстван електронен
печат на юридическо лице /legal person/ StampIT Enterprise Seal**

Профил на StampIT Enterprise Seal

Signature Algorithm	SHA256withRSA		
Issuer	CN	StampIT Global Qualified CA	
	C	BG	
	O	Information Services JSC	
	L	Sofia	
	OrganizationIdentifier (2.5.4.97)	NTRBG-831641791	
Validity	срок, определен в договора за удостоверителна услуга (една или три години)		
Subject	*C	Country	Държава
	L	Locality	Град/Област
	*E	E-mail	Пощенски адрес
	*O	Organization	Име на юридическо лице
	*OrganizationIdentifier (2.5.4.97)	2.5.4.97	Идентификатор за юридическо лице NTRYY-xxxxxxxx /национален идентификационен код/ VATYY-xxxxxxxx /Данъчен номер/ YY – код на държава
Public Key	RSA 2048 bits		
Key Usage (Critical)	Digital Signature Non-Repudiation Key Encipherment		
Authority Information Access	<p>[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.stampit.org/</p> <p>[2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://stampit.org/repository/stampit_global_qualified.crt</p>		
Extended key usage (Non Critical)	Client Authentication E-Mail Protection Document Signing Code Signing		
Qualified Certificate Statement (Non Critical)	id-etsi-qcs-semanticId-Legal(oid=0.4.0.194121.1.2) id-etsi-qcs-QcCompliance (oid=0.4.0.1862.1.1) id-etsi-qct-eseal (oid=0.4.0.1862.1.6.2) id-etsi-qcs-QcPDS(oid=0.4.0.1862.1.5) PdsLocation=http://www.stampit.org/pds/pds_en.pdf language=en		
Basic constrains (Critical)	End entity		
CRL Distribution Point/Non Critical/	DP Name: http://www.stampit.org/crl/stampit_global_qualified.crl		
Certificate Policies (Non Critical)	<p>[1] Certificate Policy: Policy Identifier=1.3.6.1.4.1.11290.1.2.1.7 Policy Qualifier Id=CPS/1.3.6.1.5.5.2.7.1/ Qualifier=http://www.stampit.org/repository</p> <p>[2] Certificate Policy: Policy Identifier= 0.4.0.1456.1.2</p> <p>[3] Certificate Policy: Policy Identifier=0.4.0.194112.1.1</p>		

8. Контрол на дейността на Доставчика

Одитът е систематичен, независим и документиран процес за получаване на доказателства от одит и обективното им оценяване, за да се определи степента, до която са удовлетворени критериите за одит. Критериите за одит са съвкупност от Политики, Процедури или изисквания, използвани като база за сравнение, спрямо която се сравняват доказателствата от одита.

В „Информационно обслужване“ АД се извършват вътрешни одити, за да се определи дали Интегрираната система за управление на качеството, информационната сигурност и услугите (ИСУ), целите по контрола, механизмите за контрол, процесите, документите и записите отговарят на изискванията на международните стандарти ISO 9001, ISO/IEC 27001, ISO/IEC 20000-1, Регламент (ЕС) № 910/2014, на нормативните актове, на изискванията за сигурност на информацията, на изискванията за ИТ услугите, дали са внедрени и поддържани ефективно и дали се изпълняват съгласно очакваното. Вътрешните одити обхващат всички регистриращи органи в структурата на Организацията. При подготовката на вътрешните одити и определяне на одиторския екип, се взема предвид условието за независимост на одиторите и осигуряване на тяхната обективност и безпристрастност към дейността, която следва да одитират.

„Информационно обслужване“ АД 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.

„Информационно обслужване“ АД представя на Надзорния орган докладите за оценка на съответствието, спрямо Регламент (ЕС) № 910/2014, ISO 9001, ISO/IEC 27001 и ISO/IEC 20000-1.

Надзорният орган може по всяко време да извърши одит или да поиска от независим Орган за оценяване на съответствието да направи оценка на съответствието на „Информационно обслужване“ АД.

Докладът от Органа за оценяване на съответствието се предава на Надзорния орган в рамките на 3 (три) работни дни след връчването му. Въз основа на одитните резултати се планират дейностите по отстраняване на евентуалните несъответствия и зони за подобрение, като се посочват конкретните задачи и времето им за изпълнение.

9. Бизнес и правни въпроси

9.1. Цени

StampIT определя цени за използване на продуктите и услугите на StampIT, които са публикувани на неговия уеб сайт. StampIT запазва правото си да променя тези цени.

9.1.1. Отстраняване на неточности и възстановяване на извършено плащане

Абонатът може да възрази относно неточност или непълнота в съдържанието на издадено удостоверение в 3-дневен срок след публикуването му в Публичния регистър.

Ако причина за невярното съдържание на квалифицирано удостоверение е техническа грешка, допусната от Регистриращ орган, StampIT прекратява удостоверението и издава

ново с вярно съдържание за своя сметка или възстановява направеното плащане за отмененото удостоверение с невярно съдържание.

Ако причината за невярното съдържание на квалифицирано удостоверение е по вина на Абоната, StampIT прекратява удостоверението и може да откаже възстановяване на извършеното плащане.

9.2. Финансова отговорност

StampIT носи отговорност пред Абонатите за предоставяните удостоверителни услуги, в случай, че са настъпили вреди, в следствие на неправилно прилагане на политиките и практиката на Доставчика от негови служители.

Ако бъде потвърдено и се приеме, че е настъпило такова събитие, то StampIT се ангажира да заплати обезвредата в рамките на указания в удостоверенията максимален размер, но без да се надвишава размера на вредите.

9.2.1. Гаранции за плащане на обезщетенията

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.

9.3. Защита на личните данни

„Информационно обслужване“ АД е администратор на лични данни, регистриран съгласно националното право и осигурява законосъобразна обработка на личните данни в съответствие с Директива 95/46/ЕО и националното право.

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.

9.4. Права върху интелектуалната собственост

StampIT притежава правата върху интелектуалната собственост, касаещи базата данни, уеб сайтовете, квалифицираните удостоверения на StampIT и всякакви други публикации, които са били извършени от StampIT, включително и разработените практика, политики и други съпътстващи документи.

9.4.1. Собственост на ключовите двойки

Квалифицираните удостоверения са собственост на StampIT. StampIT разрешава квалифицираните удостоверения да бъдат репродуцирани и разпространявани безплатно и без изключително право на това, при условие, че те са репродуцирани и разпространени изцяло. Това не се отнася до квалифицирани удостоверения, които не трябва да бъдат

публикувани в никакви публично достъпни хранилища или директории без категоричното писмено разрешение на StampIT.

Обхватът на това ограничение е с цел защита на абонатите от неоторизирано публикуване на лични данни, посочени в квалифицираното удостоверение.

Частните и публичните ключове са собственост на абонатите, които ги използват и съхраняват по правилен начин.

Секретните части на частните ключове на StampIT са собственост на StampIT.

9.5. Задължения и отговорност на StampIT

До нивото, определено в съответното поле в издаваното удостоверение, StampIT се задължава да:

- спазва своите вътрешни и публични практика, политики и процедури
- спазва Регламент (ЕС) № 910/2014 и националното право
- осигурява инфраструктура и удостоверителни услуги, включително изграждането и пускането в действие на хранилището и уеб сайта на StampIT за извършване на удостоверителните услуги
- 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
- публично предоставя процедурите за заявяване на различните типове квалифицирани удостоверения
- издава и подновява квалифицирани удостоверения в съответствие с политиката и практиката, като изпълнява задълженията си посочени в тях
- при получаване на искане от Регистриращия орган, издава и подновява квалифицирани удостоверения, в съответствие с практиката и политиките
- при получаване на искане за прекратяване на квалифицирано удостоверение от Регистриращия орган прекратява удостоверението, в съответствие с практиката и политиките
- публикува квалифицираното удостоверение, в съответствие с практиката и политиките
- осигурява поддръжка на абонатите и доверяващите се страни
- прекратява, спира и възобновява квалифицираните удостоверения в съответствие с практиката и политиките
- осигурява информация за изтичането на срока на валидност и подновяването на квалифицираното удостоверение в съответствие с практиката и политиките
- предоставя копия на практиката и политиките си, както и други действащи документи за публичен достъп

StampIT заявява, че няма други задължения по тази политика.

9.5.1. Отговорност пред Абоната

StampIT отговаря пред титуляря на електронен подпис / създателя на печат / съответно пред Абоната и пред всички трети лица за вредите, причинени от:

- Неизпълнение на законоустановените изисквания към дейността на квалифицирания доставчик на квалифицирани удостоверителни услуги
- Неизпълнение на законоустановените задължения на квалифицирания доставчик на квалифицирани удостоверителни услуги, регламентиращи издаването, управлението и съдържанието на квалифицираното удостоверение
- от неверни или липсващи данни в квалифицираното удостоверение към момента на издаването му
- от алгоритмичното несъответствие между частния ключ и публичния ключ, вписан в квалифицираното удостоверение

9.5.2. Ограничения на отговорността на регистриращия орган

Мрежата на StampIT може да включва Регистриращи органи, които оперират в съответствие с утвърдените практика и процедурите на StampIT.

StampIT гарантира целостта на всяко квалифицирано удостоверение, издадено от неговия собствен Удостоверяващ орган в рамките на условията, посочени в настоящата политика.

9.6. Задължения на абоната

Освен ако не е посочено друго, абонатите на StampIT носят пълна отговорност за следното:

- да имат познания за ползване на квалифицирани удостоверения
- да предоставят вярна, точна и пълна информация на StampIT
- да се запознаят и приемат сроковете и условията на тази политика на StampIT и свързаните с нея документи, публикувани в хранилището на StampIT
- да използват квалифицираните удостоверения, издадени от StampIT само за законни цели и в съответствие с тази политика
- да уведомяват StampIT или Регистриращия орган на StampIT за промени и непълноти в предоставената информация
- да преустановяват използването на квалифицираното удостоверение, ако някаква част от информацията се окаже, че е остаряла, променена, неточна или невярна
- да преустановяват използването на квалифицираното удостоверение, ако същото е с изтекъл срок и да го деинсталират от приложенията, устройствата или средите, в които то е било инсталирано
- да предотвратяват компрометиране, загуба, разкриване, модифициране или друго неоторизирано използване на частния ключ, който кореспондира на публичния ключ, публикуван в квалифицираното удостоверение чрез надеждна защита на персоналния идентификационен код (ПИН) за работа с ключовата двойка и/или физическия достъп до носителя или средата, съхраняващ ключовата двойка
- да заявят прекратяване на квалифицираното удостоверение в случай, че има съмнения относно целостта на издаденото удостоверение

- да заявят прекратяване на квалифицираното удостоверение в случай, че някаква част от информацията, включена в удостоверението се окаже остаряла, променена, неточна или невярна
- за действия и пропуски на трети лица, на които са предоставили неправомерно техния частен ключ
- да се въздържат от предоставяне пред StampIT на материали, с клеветнически, нецензурен, порнографски, обиден, фанатичен или расистки характер

9.7. Освобождение от отговорност

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 квалифицираното удостоверение.
- всякакви други вреди, освен тези, които са свързани с доверяване на информацията, посочена в даденото квалифицирано удостоверение, базирана на потвърдената информация в удостоверението
- грешка в потвърдената информация, която е в следствие на измама или умишлено невярно изявление на заявителя
- използването на квалифицирано удостоверение, което не е било издадено или използвано в съответствие с тази политика
- използването на квалифицирано удостоверение, което не е валидно
- използването на квалифицирано удостоверение, 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
- компрометиране на частния ключ на Абоната