1504 София, ул. Панайот Волов № 2
Тел.: 02/ 9420 340, факс: 02/ 943 66 07
office@is-bg.net www.is-bg.net
ЕИК: 831641791

Предоставяне на квалифицирани удостоверителни услуги от

„Информационно обслужване“ АД

ПРАКТИКА

ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРИТЕЛНИ УСЛУГИ

ОТ „ИНФОРМАЦИОННО ОБСЛУЖВАНЕ“АД (eIDAS-CPS)

Версия: 5.1.0

Дата на публикуване: 07.06.2017 г.

Дата на последна корекция: 07.06.2017 г.

Съдържание:

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 удостове-

	рение 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 ав-

	тентичността 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 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) 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).
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
	Устройство за създаване на квалифициран електронен под-

QSCD	Устройство за създаване на квалифициран електронен подпис/печат
NCP+	Разширена нормализирана удостоверителна политика, която изисква използване на квалифицирани удостоверения в съответствие с Регламент (ЕС) № 910/2014
Certification Authority (CA)	Удостоверяващ орган
Common Name (CN)	Публично име
Certificate Policy (CP)	Политика при предоставяне на квалифицирано удостоверение за квалифициран електронен подпис 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)	Уникално име на титуляра, вписано 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 на криптографията на публичния ключ
Public Key Infrastructure (PKI)	Инфраструктура на публичния ключ
Registration Authority (RA/PO)	Регистриращ орган

1 Въведение

„Информационно обслужване“АД е юридическо лице, което е търговско дружество, регистрирано съгласно българското законодателство. Дружеството е вписано в Търговския регистър, воден от Агенция по вписванията с ЕИК 831641791. Дружеството е със седалище и адрес на управление в гр.София, район Оборище, ул.“Панайот Волов“№2, телефон за контакт: +359 2 9420340, факс +359 2 943 6607. Интернет адрес: https://www.is-bg.net.

„Информационно обслужване“ АД е доставчик на квалифицирани удостоверителни услуги, които отговарят на изискванията, посочени в Регламент (ЕС) № 910/2014 и действащото национално право. При осъществяване на дейността си „Информационно обслужване“ АД прилага внедрената в дружеството Интегрирана система за управление, която е сертифицирана по стандартите ISO/IEC 9001:2013, ISO/IEC 27001:2013 и ISO/IEC 20000-1:2011. „Информационно обслужване“АД като доставчик на удостоверителни услуги използва запазената търговска марка StampIT.

1.1 Общ преглед на Практиката при предоставяне на квалифицирани удостоверителни услуги- (eIDAS-CPS)

“Практика при предоставяне на квалифицирани удостоверителни услуги”, наричана за по-кратко ППКУУ, е публично изявление за практиките на StampIT и за общите изисквания за предоставяне на предлаганите от „Информационно обслужване“АД квалифицирани удостоверителни услуги.

В този документ се съдържат и условията на издаване, временно спиране, прекратяване и възобновяване на действието на квалифицираните удостоверения и за издаване на КЕВП, издадени в йерархията на StampIT. Изброени са документите, които са необходими за предоставяне на квалифицирани услуги и условията, при които събраната информация се съхранява от StampIT. Посочени са мерките за сигурност, които се прилагат от Доставчика при предоставяне на квалифицираните удостоверителни услуги. В документа са уредени правата, задълженията и отговорностите както на персонала на Доставчика, ангажиран с предоставяне на квалифицираните удостоверителни услуги, така и на всички трети лица, овластени от Доставчика да изпълняват функции, свързани с предоставяне на тези услуги. Описват се правата, задълженията и отговорностите на титуляря на КУЕП/ създателя на КУЕПТ и на абоната при ползване на квалифицираните удостоверителни услуги, предоставяни от „Информационно обслужване“АД.

Документът съдържа описание на следните услуги, предоставяни от „Информационно обслужване“АД:

- Издаване и управление на квалифицирани удостоверения за електронни подписи (КУЕП): квалифицирани удостоверения за квалифицирани електронни подписи – КУЕП (квалифицирани) и квалифицирани удостоверения за усъвършенствани електронни подписи – КУЕП(усъвършенствани);
- Издаване и управление на квалифицирани удостоверения за електронни печати (КУЕПТ): квалифицирани удостоверения за квалифицирани електронни печати – КУЕПТ (квалифицирани) и квалифицирани удостоверения за усъвършенствани електронни печати – КУЕПТ(усъвършенствани);

- Издаване и управление на квалифицирани удостоверения за автентичност на уебсайт (КУАУ): квалифицирани удостоверения за автентичност на уебсайт - КУАУ (домейн) и квалифицирани удостоверения за автентичност на уебсайт - КУАУ (организация);
- Квалифицирана услуга за удостоверяване на време - издаване на квалифицирани електронни времеви печати (КЕВП).

Тази ППКУУ е разработена в съответствие с Регламент (ЕС) № 910/2014 и се позовава на изискванията на общоприетите и утвърдени международни стандарти, практики и спецификации:

- RFC 3647 - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework;
- RFC 3628 - Policy Requirements for Time-Stamping Authorities;
- RFC 2560 - X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP;
- ETSI EN 319 401 Electronic Signatures and Infrastructures(ESI); General Policy Requirements for Trust Service Providers;
- ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements;
- ETSI EN 319 411-2 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates;
- ETSI EN 319 412 Certificate Profiles;
- ETSI EN 319 421 Policy and Security Requirements for Trust Service Providers issuing Electronic Time-Stamps;
- ETSI EN 319 422 Time-stamping protocol and electronic time-stamp profiles;
- ETSI TS 102 176-1 - Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms;
- ETSI TS 102 176-2 - Electronic Signatures and Infrastructures (ESI);Algorithms and Parameters for Secure Electronic Signatures; Part 2: Secure channel protocols and algorithms for signature creation devices.

1.2 Наименование, идентификация и управление на документа

Пълното наименование на документа е Практика при предоставяне на квалифицирани удостоверителни услуги от „Информационно обслужване“АД (eidas-cps).

Тази ППКУУ е публично достъпна в електронен вид на адрес:

http://www.stampit.org/repository/

ППКУУ се предоставя на всяко лице при искане, изпратено на електронен адрес: support@mail.stampit.org

Този документ може да бъде променян от „Информационно обслужване“АД по всяко време, като всяка промяна се отразява в нова актуална версия на документа, която влиза в сила след публикуването й на адрес: http://www.stampit.org/repository/.

В отношенията с Абонатите и третите лица е валидна само версията, която е актуална към момента на ползването на услугите на „Информационно обслужване“АД.

Новите версии се разработват от служители на „Информационно обслужване“АД и се публикува след одобрение от изпълнителния директор на „Информационно обслужване“АД.

ППКУУ е свързана със следните политики:

- 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).

ППКУУ изпълнява общите изисквания на удостоверителните политики, посочени в стандарта ETSI EN 319 411-1: NCP за QCP-l; NCP за QCP-l-qscd; NCP за QCP-n.

Квалифицираните удостоверенията, издадени от StampIT, съдържат идентификатори на политиките за издаването им, които могат да бъдат проверени в PolicyInformation и CertificatePolicies.

На всяка от политиките, в съответствие с които се издават квалифицираните удостоверения от StampIT се присвоява идентификатор на обект (OID - Object Identifier), със стойност както следва:

Стойности на идентификаторите на обекти

	Policy Identifier
Information Services Plc.	1.3.6.1.4.1.11290
StampIT	1.3.6.1.4.1.11290.1
StampIT Primary Root CA	1.3.6.1.4.1.11290.1.1
StampIT Qualified CA	1.3.6.1.4.1.11290.1.1.1
StampIT Time Stamping	1.3.6.1.4.1.11290.1.1.2
StampIT OCSP Validation	1.3.6.1.4.1.11290.1.1.3
StampIT DocPro Certificate	1.3.6.1.4.1.11290.1.1.1.1
StampIT Doc Certificate	1.3.6.1.4.1.11290.1.1.1.5
StampIT Global Root CA	1.3.6.1.4.1.11290.1.2
StampIT Global Qualified CA	1.3.6.1.4.1.11290.1.2.1

StampIT Global TSA	1.3.6.1.4.1.11290.1.2.1.1
StampIT DocPro Certificate	1.3.6.1.4.1.11290.1.2.1.2
StampIT Doc Certificate	1.3.6.1.4.1.11290.1.2.1.3
StampIT Seal Certificate	1.3.6.1.4.1.11290.1.2.1.4
StampIT Enterprise Certificate	1.3.6.1.4.1.11290.1.2.1.5
StampIT Enterprise Pro Certificate	1.3.6.1.4.1.11290.1.2.1.6
StampIT Enterprise Seal Certificate	1.3.6.1.4.1.11290.1.2.1.7
StampIT Server DVC	1.3.6.1.4.1.11290.1.2.1.8
StampIT Server OVC	1.3.6.1.4.1.11290.1.2.1.9
StampIT Global OCSP	1.3.6.1.4.1.11290.1.2.1.10
StampIT Global AES CA	1.3.6.1.4.1.11290.1.2.2

„Информационно обслужване“АД може да разширява поддържаните Политики на издавани удостоверения чрез оперативните удостоверяващи органи.

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 ***регистриращи органи***.

Удостоверяващият орган и регистриращите органи извършват дейностите си по предоставяне на квалифицирани удостоверителните услуги от името и за сметка на „Информационно обслужване“ АД.

В тази ПДКУУ се съдържат правила и процедури, които уреждат както отношенията между лицата в структурата на доставчика, така и отношенията между доставчика и потребителите на квалифицираните удостоверителни услуги (доверяващи се страни и абонати).

„Информационно обслужване“АД предоставя квалифицирани удостоверителни услуги на всички физически и юридически лица, които приемат правилата на този документ.

1.3.1 Удостоверяващ орган

StampIT е Удостоверяващият орган на „Информационно обслужване“ АД, който издава квалифицирани удостоверения за електронен подпис (КУЕП) на физически лица,квалифицирани удостоверения за електронен печат (КУЕПТ) на юридически лица и квалифицирани удостоверения за автентичност на уебсайт (КУАУ).

Удостоверяващият орган извършва дейности, които включват издаване, подновяване, спиране, възобновяване и прекратяване на КУЕП, КУЕПТ и КУАУ, водене на регистри и осигуряване на достъп до тях.

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=None		
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/		

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/		

1.3.2 Регистриращи органи

Удостоверяващият орган издава квалифицирано удостоверение (КУЕП/КУЕПТ/ КУАУ) 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;
- 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 иницииране 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/квалифицирани електронни подписи/ усъвършенствани/квалифицирани 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.

1.3.5 Други участници

1.3.5.1 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.

Профил на StampIT удостоверение за издаване на квалифициран времеви печат на „Информационно обслужване“ АД

	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 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/
CRL Distribution Point/Non Critical/	[1]CRL Distribution Point Distribution Point Name: Full Name: 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** Хранилище = http://www.stampit.org/repository/

StampIT Global TSA приема искания за удостоверяване на време на предоставено съдържание на електронен документ от Абоната или Доверяващата се страна; използва технология за обвързване датата и часа с данните по начин, който до голяма степен изключва възможността за незабелязана промяна на данните; основава се на източник на точно време, свързан с координираното универсално време; подписва с квалифициран електронен подпис на StampIT; осигурява възможност за доказване в последващ период във времето (след изтичане периода на действие на КЕВП) на факта на подписване/ подпечатване на електронен документ/ друг обект.

1.4 Видове квалифицирани удостоверения. Употреба.

1.4.1 Видове квалифицирани удостоверения и приложимост.

1.4.1.1 Квалифицирани удостоверения за електронен подпис (КУЕП)

Квалифицираното удостоверение за електронен подпис дава възможност на дадено физическо лице, което участва в електронна транзакция, да се идентифицира пред другите участници в тази транзакция.

КУЕП могат да се ползват за дейности, които включват идентификация, подписване, автентификация и криптиране.

Видове:

1) **Квалифицирани удостоверения за квалифицирани електронни подписи – КУЕП (квалифицирани)**
   - **Квалифицирано удостоверение за квалифициран електронен подпис StampIT Doc, което се издава на физическо лице /natural person/;**

StampIT Doc КУЕП се издават на физически лица (титуляри на електронния подпис) и могат да бъдат използвани за идентифициране на абоната, защитено и криптирано изпращане на електронни съобщения и защитени и криптирани комуникации, достъп до информация и On-Line Интернет транзакции от всякакъв вид, като например Интернет абонаментни услуги.

StampIT Doc КУЕП осигуряват високо ниво на идентичност, като се изисква заявителят да докаже идентичност, като се яви лично или чрез представител, надлежно овластен с нотариално заверено пълномощно пред Регистриращ Орган. Валидността на тези КУЕП може да бъде 1 (една) или 3 (три)години, считано от датата на издаване и се определя в договора за квалифицирани удостоверителни услуги.

- **Квалифицирано удостоверение за квалифициран електронен подпис за физическо лице, асоциирано с юридическо /legal person/ StampIT DocPro**

StampIT DocPro КУЕП се издават на физически лица (титуляри на електронния подпис), които са асоциирани с юридически лица. Те могат да бъдат използвани за идентифициране на абоната, защитено и криптирано изпращане на електронни съобщения и защитени и криптирани комуникации, достъп до информация и On-Line Интернет транзакции.

StampIT DocPro КУЕП осигуряват високо ниво на идентичност, като се изисква заявителят да докаже своята идентичност, като се яви лично или чрез представител, надлежно овластен с нотариално заверено пълномощно пред Регистриращ Орган. Валидността на тези КУЕП може да бъде 1(една) или 3(три) години, считано от датата на издаване и се определя в договора за квалифицирани удостоверителни услуги.

2) **Квалифицирани удостоверения за усъвършенствани електронни подписи – КУЕП(усъвършенствани)**

- **Квалифицирано удостоверение за усъвършенстван електронен подпис StampIT Enterprise**

StampIT Enterprise КУЕП се издават на физически лица (титуляри на електронния подпис) и могат да бъдат използвани за идентифициране на абоната, защитено и криптирано изпращане на електронни съобщения и защитени и криптирани комуникации, достъп до информация и On-Line Интернет транзакции от всякакъв вид, като например Интернет абонаментни услуги. Приложими са във всички случаи, за които не се изисква квалифициран електронен подпис.

StampIT Enterprise КУЕП осигуряват високо ниво на идентичност, като се изисква заявителят да докаже идентичност, като се яви лично или чрез представител, надлежно овластен с нотариално заверено пълномощно пред Регистриращ Орган. Валидността на тези КУЕП може да бъде 1 (една) или 3 (три)години, считано от датата на издаване и се определя в договора за квалифицирани удостоверителни услуги.

- **Квалифицирано удостоверение за усъвършенстван електронен подпис StampIT EnterprisePro**

StampIT EnterprisePro се издават на физически лица (титуляри на електронния подпис), които са асоциирани с юридически лица. Те могат да бъдат използвани за идентифициране на абоната, защитено и криптирано изпращане на електронни съобщения и защитени и криптирани комуникации, достъп до информация и On-Line Интернет транзакции. Приложими са във всички случаи, за които не се изисква квалифициран електронен подпис.

StampIT EnterprisePro осигуряват високо ниво на идентичност, като се изисква заявителят да докаже своята идентичност, като се яви лично или чрез представител, надлежно овластен с нотариално заверено пълномощно пред Регистриращ Орган. Валидността на тези КУЕП може да бъде 1(една) или 3(три) години, считано от датата на издаване и се определя в договора за квалифицирани удостоверителни услуги.

1.4.1.2 Квалифицирани удостоверения за електронен печат (КУЕПТ)

Квалифицираното удостоверение за електронен печат дава възможност на да-дено юридическо лице, което участва в електронна транзакция, да се идентифицира пред другите участници в тази транзакция, като свързва данните за валидиране на електронния печат с юридическото лице и потвърждава името на това лице.

КУЕПТ могат да се ползват за да се гарантира произход и интегритет на изходящи от юридическото лице данни, като електронни документи, снимки, чертежи и софтуер.

Видове:

- **Квалифицирано удостоверение за квалифициран електронен печат на юридическо лице /legal person/ StampIT eSeal – КУЕПТ (квалифицирани)**

StampIT eSeal се издават на юридически лица (създатели на квалифициран електронен печат). Те могат да бъдат използвани за идентифициране на абоната/ създателя на квалифицирания електронен печат, защитено и криптирано изпращане на електронни съобщения и защитени и криптирани комуникации, достъп до информация и On-Line Интернет транзакции.

StampIT eSeal осигуряват високо ниво на идентичност, като се изисква заявителят (законният представител на абоната/ създателя на квалифицирания електронен печат) да докаже своята идентичност, като се яви лично или чрез представител, надлежно овластен с нотариално заверено пълномощно пред Регистриращ Орган. Валидността на тези КУЕП може да бъде 1(една) или 3(три) години, считано от датата на издаване и се определя в договора за квалифицирани удостоверителни услуги.

- **Квалифицирано удостоверение за усъвършенстван електронен печат на юридическо лице /legal person/ StampIT EnterpriseSeal – КУЕПТ (усъвършенствани)**

StampIT EnterpriseSeal се издават на юридически лица (създатели на усъвършенстван електронен печат). Те могат да бъдат използвани за идентифициране на абоната/ създателя на квалифицирания електронен печат, защитено и криптирано изпращане на електронни съобщения и защитени и криптирани комуникации, достъп до информация и On-Line Интернет транзакции. Приложими са във всички случаи, за които не се изисква квалифициран електронен печат.

StampIT EnterpriseSeal осигуряват високо ниво на идентичност, като се изисква заявителят (законният представител на абоната/ създателя на усъвършенствания електронен печат) да докаже своята идентичност, като се яви лично или чрез представител, надлежно овластен с нотариално заверено пълномощно пред Регистриращ Орган. Валидността на тези КУЕП може да бъде 1(една) или 3(три) години, считано от датата на издаване и се определя в договора за квалифицирани удостоверителни услуги.

1.4.1.3 Квалифицирани удостоверения за автентичност на уебсайт (КУАУ)

Квалифицираното удостоверение за автентичност на уебсайт дава възможност да се установи автентичността на уебсайт, като го свързва с физическото или юридическото лице, на което ДКУУ е издал удостоверението в съответствие с изискванията на Регламент (ЕС) № 910/2014.

Видове:

- **StampIT Server DVC -** квалифицирано удостоверение за автентичност на уебсайт, Domain Validation - използва се за удостоверяване автентичността на уебсайт. Валидността на тези КУАУ може да бъде 1(една) или

3(три) години, считано от датата на издаване и се определя в договора за квалифицирани удостоверителни услуги.

- **StampIT Server OVC** - квалифицирано удостоверение за автентичност на уебсайт, Organization Validation - използва се за удостоверяване автентичността на уебсайт и връзката му с определено физическо или юридическо лице. Валидността на тези КУАУ може да бъде 1(една) или 3(три) години, считано от датата на издаване и се определя в договора за квалифицирани удостоверителни услуги.

1.4.1.4 Квалифициран електронен времеви печат (КЕВП)

Квалифицираният електронен времеви печат дава възможност да бъде установено, че определени данни са съществували в конкретен момент във времето. Квалифицираният електронен времеви печат се ползва от презумпцията за точност на указаните от него дата и час и за цялост на данните, с които са обвързани датата и часът.

Чрез електронните времеви печати Абонатите и Доверяващите се страни 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.

Квалифициран електронен времеви печат (КЕВП) се издава на физически и на юридически лица, които са титуляри или са доверяваща се страна. Квалифицираният електронен времеви печат (КЕВП) има официална удостоверителна сила след вписването му във водения от StampIT регистър, достъпен на адрес https://tsa.stampit.org.

1.5 Употреба. Достъпност на услугите

StampIT оказва съдействие на клиентите си за избор на подходяща квалифицирана удостоверителна услуга.

Абонатите трябва внимателно да определят изискванията си към специфичните приложения на квалифицираните удостоверителни услуги, както и нивата на сигурност за защитени и криптирани комуникации и др., преди да подадат искане за предоставяне на съответния тип квалифицирана удостоверителна услуга.

Квалифицираните удостоверения, издадени от StampIT не може да се използват по начин, несъвместим с обявената за тях приложимост, както и в приложения,които не отговарят на изискванията по т.1.4.

Забранено е използването на квалифицираните услуги за извършване на дейности, попадащи под ограниченията на националното право и приложимите регламенти и директиви на Европейския съюз.

Когато това е практически осъществимо, предоставяните квалифицирани удостоверителни услуги и продуктите, използвани при предоставянето им ще бъдат достъпни и за хора с увреждания.

2 Публични регистри и управление

2.1 Поддържани публични регистри

2.1.1 Регистър на издадените удостоверения

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.

2.1.2 Регистър на спрените и прекратени квалифицирани удостоверения

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

2.1.3 Проверка на статуса на издадените квалифицирани удостоверения

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

2.1.4 Проверка на статуса на издадените квалифицирани удостоверения за електронен времеви печат

StampIT поддържа регистър на издадените квалифицирани удостоверения за електронен времеви печат.

2.2 Друга публична информация

Актуални и предходни версии на всички документи, които подлежат на публикуване, включително:

- Практика при предоставяне на квалифицирани удостоверителни услуги от „Информационно обслужване“АД, Политики при предоставяне на квалифицирани удостоверителни услуги, Политика при предоставяне на услуги за удостоверяване на време, правила, процедури и документи, които са предназначени за Абонатите и Доверяващите страни;
- Доклади от одити, извършени от органи за оценка на съответствието и надзорни органи;
- Допълнителна информация, която доставчикът е длъжен да публикува

2.3 Честота на опресняване и публикуване

2.3.1 Честотата на опресняване на публикуваните квалифицирани удостоверения е както следва:

Наименование	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 квалифицирани удостоверения	https://www.stampit.org	Реално време

2.3.2 Практика при предоставяне на квалифицирани удостоверителни услуги от „Информационно обслужване“АД, Политики при предоставяне на квалифицирани удостоверителни услуги, Политика при предоставяне на услуги за удостоверяване на време – незабавно при всяка актуализация;

2.3.3 Доклади от одити, които подлежат на публикуване – незабавно след получаване.

2.4 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 и другата публична информация е достъпна в режим 24x7, освен в случаите на събития, които са извън контрола на StampIT.

StampIT е препиел съответните мерки за защита срещу неоторизирани промени (включително премахване и добавяне) на информацията, както и за незабавно възстановяне при откриване на нарушения.

3 Идентификация и проверка на информацията за самоличност

Действията за идентификация и проверка на информацията за самоличността на заявителя, на титуляря/създателя и на абоната се извършват от Регистриращия орган след получаване на искане на издаване на квалифицирано удостоверение. Регистриращият орган събира и проверява както данните, които се включват в удостоверението, така и други данни за идентификация и самоличност, които StampIT е длъжен да събира, обработва и съхранява съгласно Регламент (ЕС) № 910/2014 и националното право. StampIT гарантира, че преди издаване на квалифицираното удостоверение физическите и юридическите лица са правилно идентифицирани, тяхната идентичност и самоличност е потвърден, както и че исканията за издаване са проверени и одобрени.

Когато информацията, предоставена от заявителя е потвърдена, Регистриращият орган изпраща искането на Удостоверяващия орган за издаване на исканото квалифицирано удостоверение.

3.1 Имена

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. Тази информация се предоставя от заявителя и следва да бъде потвърдена с представени документи. Регистриращият орган извършва проверки в първични държавни регистри (когато е приложимо), както и в други регистри при необходимост.

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

При издаване на квалифицирано удостоверение Абонатът може да поиска вписване на псевдоним. Издаването на квалифицирано удостоверение като използва „псевдоним" се извършва само след като Регистриращият орган събере необходимата идентифицираща информация съгласно националното право.

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 политиките за съответните профили 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.

StampIT гарантира, че няма да публикува квалифицирани удостоверения и други идентификационни данни, освен ако Абонатът изрично не заяви своето съгласие за това.

Когато предоставят и използват domain и distinguished name, както и всяка друга информация при подаване на искане за издаване на квалифицирано удостоверение) Абонатите са длъжни да не нарушават права на трети страни по отношение на техни търговски марки, търговски наименования или други права върху интелектуална собственост. Абонатите на StampIT са длъжни да не използват domain и distinguished names с незаконни цели, за нелоялна конкуренция и да не предоставят информация, объркваща или подвеждаща дадено лице, независимо дали то е физическо или юридическо. StampIT не носи отговорност за неизпълнение на тези задължения отстрана на Абонатите.

Ако е уведомен за възникнал спор за използване на имена, StampIT може да откаже да издаде квалифицирано удостоверение или едностранно да прекрати договора за квалифицирана удостоверителна услуга за издадено удостоверение.

3.2 Първоначална регистрация при издаване на квалифицирано удостоверение

Първоначалната регистрацията се извършва по процедури, които имат за цел е да се съберат всички необходими данни за идентификацията на заявителя и на Титуляря/ Създателя/ Абоната, преди да се пристъпи към фактическото издаване на квалифицираното удостоверение.

Данните за идентичност и самоличност подлежат на потвърждение с лично явяване пред Регистриращ орган, а в случаите на заявяване чрез пълномощник – лично явяване на упълномощителя пред Нотариус или длъжностно лице, изпълняващо нотариални функции.

Според вида на заявителя се извършват следните проверки:

- За юридическо лице, което е регистрирано по националното право - осъществява се чрез проверка в съответните регистри по предоставен ЕИК, съответно БУЛСТАТ;
- За упълномощен представител на юридическо лице - осъществява се чрез проверка и заверка „Вярно с оригинала“ и саморъчен подпис върху изискуемите документи;
- За физическо лице - осъществява се, чрез лично присъствие с документ за самоличност.
- В случай на представяне на изискуемите документи от 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 (когато са представени лични документи, издадени по националното право).
- 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).

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

3.2.1 Проверка за притежание на частен ключ

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

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. В този случай, след успешна проверка на валидността на електронния подпис/ електронния печат StampIT ще приеме, че заявителят притежава частния ключ, който съответства не техническите изисквания и кореспондира на публичния ключ, с който е подписано искането. Когато се издава квалифицирано удостоверение за квалифициран електронен подпис/ квалифициран електронен печат, двойката ключове, за която се издава квалифицираното удостоверение задължително се генерира в устройство за създаване на електронен подпис/ печат.

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 (когато юридическото лице е регистрирано по националното право).

При невъзможност за извършване на проверката, пред Регистриращия орган следва да се представят:

- Удостоверение за актуално състояние на юридическото лице, 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, представители на юридическо лице

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

Пред Регистриращия орган следва да се представят:

- Документ за самоличност на физическото лице, което е заявило издаването на квалифицираното удостоверение – оригинал;

- Документ/пълномощно, от което произтича представителната власт на физическото лице спрямо юридическото лице (когато в квалифицираното удостоверение се вписват данни за юридическо 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 Регистриращия орган след представяне 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 Включване на непотвърдена информация

Непотвърдена е всяка информация, която е заявена преди издаване на квалифицираното удостоверение, но не подлежи на задължителна проверка. Непотвърдена информация може да бъде включена в съдържанието на издаденото квалифицирано удостоверение, като в този случай StampIT не носи отговорност за тази информация.

3.2.6 Проверка и последващи действия 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, Регистриращият орган потвърждава данните пред Удостоверяващия орган. 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.

3.2.7 Проверка за притежание на домейн

При издаването на удостоверението за автентичност на уебсайт, Регистриращия орган извършва необходимите справки за потвърждаването на автентичността на предоставените за удостоверяване домейни и/или публични IP адреси. Това става чрез извършването на проверки в релевантните бази данни, поддържани от трети страни - whois записите, поддържани от съответния регистратор, управляващ базовия домейн или RIPE за проверка на публичните IP адреси.

За Organization Validation квалифицирани удосотверения в допълнение се извършват и необходимте проверки за организацията, искаща издаването, в съответните регистри – Търговски регистър/Регистър БУЛСТАТ към Агенция по вписванията.

3.2.8 Съответствие с Регламент (ЕС) № 910/2014

Издадените от StampIT квалифицирани удостоверения отговарят на изискванията на Регламент (ЕС) № 910/2014 и се признават в Европейския съюз. С цел гарантиране на трансграничната оперативна съвместимост на квали-

фицираните електронни подписи и квалифицираните електронни печати, издадените от StampIT квалифицирани удостоверения не надвишават задължителните изисквания, поставени в Регламент (ЕС) № 910/2014. StampIT гарантира, че доколкото в квалифицираните удостоверения се съдържат спефични данни, включени на национално равнище, те не пречат на трансграничната оперативна съвместимост и признаването на квалифицираните удостоверения в Европейската общност.

3.3 Идентификация и проверка на информацията за самоличност при подновяване на квалифицирано удостоверение

Подновяване на квалифицирано удостоверение е допустимо в случаите, когато частният ключ е генериран в устройство за създаване на електронен подпис/ печат и удостоверението не е било прекратено в периода на валидност.

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 (renewal) може да бъде извършено само ако квалифицираното удостоверение е издадено със срок на валидност 1 (една) година 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, но не по-късно от 30 дни след тази дата. Подаването на искане за подновяване може да се извърши на място при Регистриращия орган или отдалечено – с електронно искане, подписано с квалифицирано удостоверение. При подаване на искане за подновяване пред Регистриращия орган се извършва идентификация и проверка на информацията за самоличност на заявителя.

При отдалеченото подаване на заявление за подновяване не се изисква допълнителна идентификация и проверка на информацията за самоличност.

Когато има промени в заявените обстоятелства, вписани в квалифицираното удостоверение или е изтекъл максималният срок на валидност на квалифицираното удостоверение според съответната Политика, задължително се генерира нова ключова двойка (rekey) с нов срок на валидност. В този случай се изисква лично явяване на заявителя пред Регистриращия орган и спазване на процедурите за идентификация и проверка на информацията за самоличност, които се прилагат при издаване на квалифицирано удостоверение от съответния вид.

3.4 Идентификация и проверка на информацията за самоличност при временно спиране на действието на квалифицирано удостоверение

Временното спиране на квалифицирано удостоверение цели да бъде временно спряна неговата употреба, като за периода на спирането квалифицираното удостоверение временно губи своята валидност.

Спирането се извършва от StampIT незабавно след получаване на искане за спиране, като за приемане и изпълнение на искането не се изисква идентификация и проверка на информацията за самоличност на заявителя. Удостоверението се включва незабавно в CRL списъка със съответната причина (Reason) за спиране.

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

3.5 Идентификация и проверка на информацията за самоличност при прекратяване на действието на квалифицирано удостоверение

Прекратяването на квалифицирано удостоверение спира за постоянно действието на удостоверението, като от момента на прекратяването квалифицираното удостоверение губи своята валидност и тя не може да бъде възстановена при никакви обстоятелства.

StampIT прекратява действието на квалифицирано удостоверение при следните обстоятелства:

- 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 съответната Политика и настоящата Практика на StampIT;
- Титулярят/Създателят, съответно Абонатът е нарушил задълженията си по договора за предоставяне на квалифицирани удостоверителни услуги;
- изпълнението на някое задължениепо съответната политика и настоящата Практика 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;
- прекратяване на договора за квалифицирани удостоверителни услуги.

Прекратяването се извършва по искане на Титуляря/Създателя или Абоната, както и по искане на посочени в нормативен акт органи, след идентификация и проверка на информацията за самоличност на лицето, заявило прекратяването и уточняване на причината за прекратяване. Удостоверението незабавно се включва в CRL списъка със съответната причина (Reason) за прекратяване.

StampIT съхранява надлежно информацията относно прекратяване на валидността на квалифицираните удостоверения и я предоставя на всяка доверяваща се страна.

StampIT не допуска подновяване или възобновяване на квалифицирано удостоверение след прекратяването му.

4 Жизнен цикъл на квалифицираните удостоверения. Оперативни изисквания.

Жизненият цикъл на квалифицираните удостоверения, издавани от StampIT въз основа на договор за квалифицирани удостоверителни услуги включва следните оперативни процедури по издаване и управление:

- Подаване на искане за издаване на квалифицирано удостоверение;
- Обработка на искане за издаване на квалифицирано удостоверение;
- Издаване на квалифицирано удостоверение;
- Предаване на квалифицирано удостоверение;
- Употреба на квалифицирано удостоверение и на двойка ключове;
- Подновяване на квалифицирано удостоверение (renewal);
- Подновяване на квалифицирано удостоверение (rekey);
- Спиране/ възобновяване на валидността на квалифицирано удостоверение;
- Прекратяване на квалифицирано удостоверение;
- Услуги за проверка на статуса на квалифицирано удостоверение.

Допуска се прекратяване на договора за квалифицирани удостоверителни услуги от Титуляря/ Създателя, както и от Абоната.

Времето в системите, свързани със спиране и прекратяване на удостоверения се синхронизира спрямо UTC поне веднъж на 24 часа.

4.1 Подаване на искане за издаване на квалифицирано удостоверение

Подаването на искане за издаване на квалифицирано удостоверение е оперативна процедура, при която абонатът се обръща към Регистриращия орган с искане за издаване на квалифицирано удостоверение съобразно политиката за издаване на исканото удостоверение.

4.1.1 Лица, които могат да подадат искане за издаване на квалифицирано удостоверение

Квалифицираните удостоверения се издават по искане на титуляря/ създателя или абоната (ако не съвпада с титуляря/ създателя) или на надлежно овластено от него лице при спазване на съответната Политика. Искане за издаване може да бъде подадено и от служител на Доставчика, овластен с функции към Удостоверяващия орган.

Когато се иска вписване в КУЕП на юридическо лице, с което се асоциира титу-ляря, искането следва да изхожда от юридическото лице или от надлежно овластено от него лице.

Преди или по време на процеса по заявяване на квалифицирани удостоверителни услуги пред Регистриращия орган, заявителите извършват следните стъпки:

- подават искане за издаване и приемат условията на договора за квалифицирани удостоверителни услуги, на съответната Политика на ДКУУ, както и тази ПДПКУУ;
- предоставят доказателства за тяхната идентичност и самоличност (както се изисква според стандартно определените процедури на StampIT съгласно т.3), съобразно вида на искането квалифицирано удостоверение.

4.1.2 Съдържание на искането за издаване на квалифицирано удостоверение

Искането за издаване включва следните елементи за идентификация и съответни документи, в съответствие с типа на квалифицираното удостоверение и условията на неговото издаване:

4.1.2.1 За издаване на квалифицирано удостоверение за електронен подпис (КУЕП):

- име/ наименование на заявителя;
- пощенски адрес на заявителя
- псевдоним на заявителя (ако се иска вписване на псевдоним)
- единен граждански номер/ персонален идентификационен номер/ единен идентификационен код (ако заявителят има такъв);
- име на овластения/ упълномощения представител и номер на документ за овластяване;
- име на физическото лице, което е асоциирано с юридическото лице - заявител;
- псевдоним на физическото лице, което е асоциирано с юридическото лице - заявител (ако се иска вписване на псевдоним);
- град, държава;
- документ за плащане;
- документ за самоличност на заявителя (когато е приложимо);
- документ за самоличност на овластения/ упълномощения представител (когато е приложимо)
- документ за актуално състояние на заявителя (когато е приложимо);
- документ за овластяване (когато е приложимо);
- подписано искане за издаване на квалифицирано удостоверение с посочен вид на искането удостоверение;
- подписан договор за квалифицирани удостоверителни услуги;
- публичен ключ (в случаите, когато ключовата двойка е генерирана при Титуляря).

4.1.2.2 За издаване на квалифицирано удостоверение за електронен печат (КУЕПТ):

- наименование на заявителя;

- пощенски адрес на заявителя;
- единен идентификационен код (ако заявителят има такъв);
- име на овластения/ упълномощения представител и номер на документ за овластяване;
- град, държава;
- документ за плащане;
- документ за актуално състояние (когато е приложимо);
- документ за овластяване (когато е приложимо);
- документ за самоличност на овластения/ упълномощения представител;
- подписано искане за издаване на квалифицирано удостоверение с посочен вид на исканото удостоверение;
- подписан договор за квалифицирани удостоверителни услуги.
- публичен ключ (в случаите, когато ключовата двойка е генерирана при създателя).

4.1.2.3 За издаване на квалифицирано удостоверение за автентичност на уебсайт (КУАУ)

- наименование на заявителя;
- пощенски адрес на заявителя;
- единен граждански номер/ персонален идентификационен номер/ единен идентификационен код (ако заявителят има такъв)
- име на овластения/ упълномощения представител и номер на документ за овластяване;
- град, държава;
- наименование на домейна/ наименования на домейните, поддържани от заявителя, за които се иска издаването на квалифицирано удостоверение;
- документ за плащане;
- документ за актуално състояние (когато е приложимо);
- документ за овластяване (когато е приложимо);
- документ за самоличност на заявителя/ овластения/ упълномощения представител (когато е приложимо);
- подписано искане за издаване на квалифицирано удостоверение с посочен вид на исканото удостоверение;
- подписан договор за квалифицирани удостоверителни услуги.
- публичен ключ (в случаите, когато ключовата двойка е генерирана при Абоната).

StampIT може да модифицира изискванията към информацията, касаеща исканията на лицата, за да изпълни своите изисквания, бизнес контекста на употребата на квалифицираните удостоверения при спазване на препоръките на Регламент (ЕС) № 910/2014 и националното право.

4.1.3 Обработка на искането и издаване на квалифицирано удостоверение

4.1.3.1 Издаване на потребителски удостоверения

Обработката на искането се извършва след проверка на искането за издаване и сключване на договор за квалифицирани удостоверителни услуги и включва следните стъпки:

- **регистриране на искането за издаване**. Регистрирането включва въвеждане на цялата информация, която се съдържа в искането за издаване, включително и непотвърдената информация по т.3.2.5.;
- **генериране на ключова двойка**. Регистриращите органи на StampIT носят цялата отговорност за безопасното генериране на ключова двойка на абоната. Когато се генерира ключова двойка за квалифицирани удостоверения за квалифициран електронен подпис/ квалифициран електронен печат, във всички случаи се използва устройство за сигурно създаване на електронен подпис/ електронен печат със съответното изисквано ниво на сигурност съгласно Регламент (ЕС) № 910/2014; В случаите, когато ключовата двойка е генерирана при Титуляра/ Създателя или Абоната, Регистриращият орган извършва проверка на изискванията за нивото за сигурност на устройството за създаване на електронен подпис/ печат и проверка за съответствие с криптографските изисквания.
- **генериране на заявка за издаване, подписана с частния ключ от генерираната/предоставената ключова двойка**;
- **изпращане на заявката за издаване на Удостоверяващия орган**;
- **издаване на квалифицирано удостоверение от Удостоверяващия орган чрез подписване на заявката за издаване с частния ключ на Удостоверяващия орган. Незабавно публикуване на издаденото удостоверение в Регистъра на издадените удостоверения.**
- **записване на удостоверението и ключовата двойка в устройство за сигурно създаване на електронен подпис/печат**.
- **предаване на квалифицираното удостоверение от Регистриращия орган на Абоната/ упълномощеното лице, заедно с код за достъп до частния ключ**.
- **приемане на квалифицираното удостоверение от Абоната**.

4.1.3.2 Издаване на удостоверения на Удостоверяващ орган и на Регистриращ орган

Ключовете и удостоверенията на Удостоверяващия орган на StampIT могат да бъдат генерирани само при изпълнение на церемония за генериране на ключове, в която участват само лица, изрично оправомощени от StampIT.

Удостоверения на външни Регистриращи органи могат да бъдат издавани само след сключване на договор със StampIT, в който е предвиден ред за определяне на лицата, които ще изпълняват функции на Регистриращи орга-

ни и изискване за потвърждаване на тяхното съгласие да представляват и двете страни при изпълнение на договора.

4.1.4 Подновяване и промяна на квалифицирано удостоверение

Титулярят/ Създателят или Абонатът може да заяви подновяване на квалифицирано удостоверение, издадено от StampIT при спазване на съответната Политика и тази Практика и съобразно условията и нормативните изисквания, действащи към момента на подновяване.

Подновяване на квалифицирано удостоверение е допустимо в случаите, когато частният ключ е генериран в устройство за създаване на електронен подпис/ печат и удостоверението не е било прекратено в периода на валидност.

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.

4.1.4.1 Подновяване (renewal)

Може да бъде извършено само ако квалифицираното удостоверение е издадено със срок на валидност 1 (една) година и всички данни в удостоверението останат непроменени, както са заявени в първоначалното искане. Квалифицираното удостоверение може да бъде подновявано до достигане на максималния срок на валидност 3 (три) години.

Абонатът трябва постоянно да контролира верността и точността на информацията, публикувана в подновеното квалифицирано удостоверение.

За подновяване е необходимо да бъде подадено Искане за подновяване, което да бъде получено от StampIT преди датата на изтичане на срока на валидност, вписан в удостоверението. Подаването на искане за подновяване може да се извърши на място при Регистриращия орган или отдалечено – с електронно искане, подписано с квалифицирано удостоверение.

Искане за подновяване може да бъде подадено не по-късно от 30 (тридесет) дни след изтичане на срока на валидност, вписан в удостоверението. В този случай искане за подновяване може да се извърши само на място при Регистриращия орган.

4.1.4.2 Подновяване (rekey)

Извършва се когато има промени в заявените обстоятелства, вписани в квалифицираното удостоверение или е изтекъл максималният срок на валидност на квалифицираното удостоверение според съответната Политика. В тези случаи задължително се генерира нова ключова двойка (rekey) с нов срок на валидност.

За подновяване е необходимо да бъде подадено Искане за подновяване, което да бъде получено от StampIT преди датата на изтичане на срока на валидност, вписан в удостоверението, но не по-късно по-късно от 30 (тридесет) дни след изтичане на срока на валидност, вписан в удостоверението.

Подаването на искане за подновяване (rekey) може да се извърши само на място при Регистриращия орган.

4.1.4.3 Информация и документи за подновяване на квалифицирано удостоверение

- име/ наименование на заявителя;
- единен граждански номер/ персонален идентификационен номер/ единен идентификационен код (ако заявителят има такъв);
- име на овластения/ упълномощения представител и номер на документ за овластяване;
- име на физическото лице, което е асоциирано с юридическото лице - заявител;
- документ за плащане;
- документ за самоличност на заявителя (когато е приложимо);
- документ за самоличност на овластения/ упълномощения представител (когато е приложимо)
- документ за актуално състояние на заявителя (когато е приложимо);
- документ за овластяване (когато е приложимо);
- подписано искане за подновяване на квалифицирано удостоверение с посочен вид на удостоверението;
- квалифицираното удостоверение, за което се иска подновавяне – при подновяване (renewal);
- нова ключова двойка - в случаите, когато се иска подновяване(rekey) и ключовата двойка е генерирана при Титуляра/ Създателя или Абоната.

4.1.4.4 Промяна в съдържанието на квалифицирано удостоверение, издадено от StampIT

StampIT не допуска други промени в съдържанието на квалифицираните удостоверения, освен продължаване на срока на валидност при подновяване (renewal).

4.1.5 Подаване на искане за спиране, възобновяване и прекратяване на валидността на квалифицирано удостоверение

Спирането на квалифицирано удостоверение цели да бъде временно спряна неговата употреба, като за периода на спирането квалифицираното удостоверение временно губи своята валидност.

Спирането се извършва от StampIT незабавно след получаване на искане за спиране, като за приемане и изпълнение на искането не се изисква идентификация и проверка на информацията за самоличност на заявителя.

Искане за спиране може да бъде подадено от Титуляря/ Създателя/ Абоната на квалифицираното удостоверение на място при Регистриращия орган, по електронен път или по телефона.

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

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

StampIT прекратява действието на квалифицирано удостоверение при следните обстоятелства:

- 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 съответната Политика и настоящата Практика на StampIT;
- Титулярят/Създателят, съответно Абонатът е нарушил задълженията си по договора за предоставяне на квалифицирани удостоверителни услуги;
- изпълнението на някое задължение по съответната политика и настоящата Практика 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;
- смърт или поставяне под запрещение на Титуляря/ Абоната (когато абонатът е физическо лице);
- прекратяване на представителната власт на Титуляря спрямо Абоната.

Прекратяването се извършва по искане на Титуляря/Създателя или Абоната, както и по искане на посочени в нормативен акт органи, след идентификация и проверка на информацията за самоличност на лицето, заявило прекратяването и уточняване на причината за прекратяване. Удостоверението незабавно се включва в CRL списъка със съответната причина (Reason) за прекратяване.

StampIT съхранява надлежно информацията относно прекратяване на валидността на квалифицираните удостоверения и я предоставя на всяка доверяваща се страна.

StampIT не допуска подновяване или възобновяване на квалифицирано удостоверение след прекратяването му.

StampIT ще прекрати издадените от него квалифицирани удостоверения ако прекрати дейността си без да я е прехвърлил на друг доставчик. В този случай StampIT ще уведоми абонатите, титулярите/ създателите и ще прекрати удостоверенията с едномесечно предизвестие. В едномесечен срок след уведомяването StampIT ще възстанови на абонатите платената от тях сума, в размер изчислен съобразно оставащия срок на договора за квалифицирана удостоверителна услуга.

StampIT ще спре или прекрати удостоверение на Удостоверяващ орган от инфраструктурата при наличие на основателни сведения и обстоятелства от които е видно, че частният ключ на този орган е бил компрометиран. При прекратяване на удостоверение на оперативния удостоверяващ орган за издаване и управление на квалифицирани удостоверения, действието на всички издадени от него валидни удостоверения се прекратява.

Когато прекратяване на квалифицирано удостоверение е поради грешка на персонала на StampIT или поради компрометиране на оперативен частен ключ на StampIT, Доставчикът ще издаде на Абоната еквивалентно квалифицирано удостоверение за своя сметка при спазване на правилата и процедурите за издаване на съответния вид удостоверение.

Услугите по спиране, възобновяване и прекратяване са достъпни денонощно, 7 дни в седмицата, като при срив в системите доставчикът е длъжен да възстанови услугите не по-късно от 3 часа.

4.2 Обработка на исканията

Исканията за издаване и управление на квалифицирани удостоверения се подават на място при Регистриращия орган. Искания за подновяване (renewal) могат да се подават отдалечено – с електронно искане, подписано с валидно квалифицирано удостоверение.

4.2.1 Идентификация и проверка на информацията за самоличност

Действията за идентификация и проверка на информацията за самоличност на Титуляря/Създателя/ Абоната и на упълномощените лица са подробно уредени в раздел 3.

4.2.2 Обработка на искане от Регистриращия орган

Всяко постъпило искане в Регистриращия орган преминава следните обработки:

- получаване на искането;
- проверка на данните, съдържащи се в искането; проверка за притежание на частен ключ (когато е приложимо), проверка на други изисквани данни (когато е приложимо);
- проверка на информация за плащане на цената на исканата квалифицирана удостоверителна услуга (когато плащането се дължи преди предоставяне на услугата);
- при положителен резултат от проверката – Регистриращият орган потвърждава искането, генерира ключова двойка и изпраща заявка към Удостоверяващия орган;
- при отрицателен резултат от проверката – Регистриращият орган отхвърля искането или го коригира.

Регистриращият орган може да отхвърли искането:

- Когато заявителят не може да докаже правата си върху заявения DN;
- Когато предоставената информация и/или документи съдържат неверни данни или е възникнало съмнение, че съдържат неверни данни;
- Когато не е извършено плащане на цената (в случаите, когато се дължи преди предоставяне на услугата).

В случай на отхвърляне на искане, заявителят може да подаде ново искане.

4.2.3 Срок за разглеждане на искането

Искането за издаване се проверява от Регистриращия орган незабавно след получаването му.

Удостоверяващият орган издава квалифицираното удостоверение незабавно след получаване на заявка от Регистриращия орган.

Срокът за разглеждане на искането, за извършване на законово позволени проверки в публично достъпни електронни регистри и за издаване на квалифицирано удостоверение от StampIT не може да бъде по-дълъг от 3 (три) дни от подаване на искането.

4.3 Издаване на квалифицирано удостоверение

4.3.1 Обработка на заявката от Удостоверяващия орган

След изпълнение на дейностите по обработка на искането, Регистриращият орган изпраща заявка за издаване към Удостоверяващия орган.

Удостоверяващият орган незабавно (в реално време) издава искането квалифицирано удостоверение, подписва го с частния ключ на StampIT и го публикува незабавно в Списъка на издадените квалифицирани удостоверения.

Удостоверяващият орган изпраща издаденото удостоверение на Регистриращия орган за предоставяне на Титуляря/ Създателя/ Абоната или на упълномощеното лице.

4.3.2 Предоставяне на квалифицирано удостоверение

Регистриращият орган записва удостоверението на устройството за създаване на електронен подпис/ печат, на което е генерирана ключовата двойка за това удостоверение и го предава на Титуляря/ Създателя/ Абоната или на упълномощеното лице.

4.4 Приемане на издаденото квалифицирано удостоверение от Абоната

4.4.1 Потвърждение за приемане

Задължение на Титуляря/ Създателя/ Абоната е да провери съдържанието на издаденота квалифицирано удостоверение, както по отношение на вписаните данни, така и за наличието на публичен ключ, съответстващ на притежавания частен ключ.

Ако издаденото квалифицирано удостоверение съдържа непълноти или грешки, титулярят/ създателят, съответно абонатът може да възрази в 3-дневен срок от публикуването му в регистъра на издадените удостоверения. Те се отстраняват незабавно от доставчика чрез издаване на ново квалифицирано удостоверение без заплащане на възнаграждение, освен ако се дължат на предоставяне на не-верни данни.

Приема се, че квалифицираното удостоверение е прието, ако в 3–дневен срок от публикуването титулярят/ създателят, съответно абонатът не е възразил, че същото съдържа непълноти или грешки.

Приемането на квалифицираното удостоверение представлява и потвърждение, че титулярят/ създателят, съответно абонатът е бил запознат с процедурите за издаване на удостоверение и приема Практиката и съответната Политика.

4.4.2 Публикуване на квалифицирано удостоверение

Издаденото квалифицирано удостоверение се публикува незабавно в регистъра на издадените удостоверения и е валидно от момента на публикуването му. От този момент удостоверението е публично достъпно, включително и за всички заинтересовани страни.

4.4.3 Информация за доверяващите се страни

Публичният ключ в квалифицираното удостоверение, съответстващ на държания от Титуляря/ Създателя/ Абоната частен ключ, е достъпен за всички доверяващи се страни в Публичния регистър на издадените квалифицирани удостоверения. Всяка доверяваща се страна следва да използва публичния ключ и удостоверението на Титуляря/ Създателя/ Абоната в съответствие с изискванията на означената в квалифицираното удостоверение политика.

Доверяващите се страни трябва да използват публичния ключ само след проверки на: статуса на квалифицираното удостоверение и електронния подпис на Доставчика.

4.5 Употреба на квалифицирано удостоверение и на двойка ключове

4.5.1 Употреба от Титулярите / Създателите

При употребата на квалифицираните удостоверения и частните ключове, Титулярите/ Създателите са длъжни:

- да ги използват в съответствие с тяхното предназначение, определено в настоящата Практика и в съответствие с ограниченията и целите, вписани в самото приложение, както и в съответствие с договореното с Доставчика;
- да ги използват само в периода на тяхната валидност;
- да не използват спряно удостостоверение за създаване на електронен подпис/ печат;
- да не разкриват частния ключ пред трети лица, както и да не предоставят устройството за създаване на квалифицирания електронен подпис/ квалифицирания електронен печат и начина на идентификация (ПИН – код);
- да предприемат необходимите мерки за предотвратяване на компрометиране, загуба, разкриване, модифициране или друго неоторизирано използване на техния частен ключ чрез надлежна защита на персоналния си идентификационен код (ПИН) за работа с ключовата двойка и/или физическия достъп до устройството за създаване на квалифицирания електронен подпис/ квалифици-рания електронен печат, съхраняващ ключовата двойка.

4.5.2 Употреба от доверяващите се страни

При употреба на публичните ключове и съответните им удостоверения, доверяващите се страни са длъжни:

- да ги използват съгласно предназначението им и вписаните ограничения за ползване, съобразно тази Практика и с оглед атрибутите на удостоверението;
- да ги използват само след проверка на техния статус и проверка на електронния подпис на Удостоверяващия орган, издал квалифицираното удостоверение;
- да ги използват само когато са валидни (да не използват спрени и прекратени удостоверения, както и невалидни ключове).

4.6 Подновяване на квалифицирано удостоверение (renewal)

Подновяване (renewal) може да бъде извършено само ако квалифицираното удостоверение е издадено със срок на валидност 1 (една) година и всички данни в удостоверението останат непроменени, както са заявени в първоначалното искане.

Квалифицираното удостоверение може да бъде подновявано до достигане на максималния срок на валидност 3 (три) години.

Абонатът трябва постоянно да контролира верността и точността на информацията, публикувана в квалифицираното удостоверение.

4.6.1 Обстоятелства, при които се прилага подновяване (renewal)

StampIT ще изпълни искане за подновяване (renewal), при следните условия:

- искането да е подадено от същия Абонат;
- квалифицираното удостоверение да не е прекратено;
- да е подадено в срока на валидност на квалифицираното удостоверението или не по-късно от 30 (тридесет) дни след изтичане на срока на валидност, вписан в удостоверението;
- квалифицираното удостоверение да не е подновявано повече от един път.

4.6.2 Лица, които могат да правят искане за подновяване (renewal)

Искането за подновяване на квалифицирано удостоверение (renewal)може да бъде направено само от титуляря/ създателя на електронния подпис/ електронния печат или от абоната на квалифицираното удостоверение за автентичност на уебсайт. Подаването на искане за подновяване (renewal) може да се извърши на място при Регистриращия орган или отдалечено – с електронно искане, подписано с квалифицирано удостоверение.

Когато искането за подновяване е подадено след изтичане на срока на валидност, вписан в удостоверението, подновяване може да се извърши само на място при Регистриращия орган.

4.6.3 Обработка на искането за подновяване на квалифицирано удостоверение с генериране на нова двойка ключове (renewal)

Искането за подновяване на квалифицирано удостоверение (renewal) трябва да бъде получено от StampIT преди датата на изтичане на срока на валидност, вписан в удостоверението, но не по-късно от 30 (тридесет) дни след изтичане на срока на валидност.

Подаването на искане за подновяване може да се извърши на място при Регистриращия орган или отдалечено – с електронно искане, подписано с квалифицирано удостоверение.

След успешна идентификация и проверка за наличие на условията за подновяване на квалифицирано удостоверение (renewal), Регистриращият орган потвърждава искането и изпраща заявка към Удостоверяващия орган, който изпълнява искането.

При неуспешна идентификация и проверка за наличие на условията за подновяване на квалифицирано удостоверение (renewal), Регистриращият орган отхвърля искането и уведомява заявителя за причината. Отхвърлянето на искането не представлява пречка за подаване на ново искане за подновяване.

Удостоверяващият орган незабавно (в реално време) продължава срока на исканото квалифицирано удостоверение, подписва го с частния ключ на StampIT и го публикува незабавно в Списъка на издадените квалифицирани удостоверения.

Удостоверяващият орган изпраща подновеното удостоверение на Регистриращия орган за предоставяне на Титуляря/ Създателя/ Абоната или на упълномощеното лице.

4.6.4 Предоставяне на подновеното квалифицирано удостоверение

Регистриращият орган записва удостоверението на устройството за създаване на електронен подпис/ печат, на което е генерирана ключовата двойка за това удостоверение и го предава на Титуляря/ Създателя/ Абоната или на упълномощеното лице.

4.6.5 Потвърждение за приемане на подновено квалифицирано удостоверение

Прилагат се изискванията на т.4.4.1.

4.6.6 Публикуване на подновено квалифицирано удостоверение

Подновеното квалифицирано удостоверение се публикува незабавно в регистъра на издадените удостоверения и е валидно от момента на публикуването му. От този момент удостоверението е публично достъпно, включително и за всички заинтересовани страни.

4.7 Издаване на квалифицирано удостоверение с генериране на нова ключова двойка (rekey)

Генериране на нова ключова двойка с нов срок на валидност се извършва винаги, когато бъде заявено издаване на квалифицирано удостоверение от нов абонат или подновяване (rekey) от вече регистриран абонат.

Подновяване (rekey) се извършва когато има промени в заявените обстоятелства, вписани в квалифицираното удостоверение или е изтекъл максималният срок на валидност на квалифицираното удостоверение според съответната Политика.

Спазва се процедурата за издаване на квалифицирано удостоверение, като генерирането на нова ключова двойка не се свързва с други удостоверения.

Когато искането е за подновяване (rekey) на валидно удостоверение, съдържанието на новото удостоверение се различава по серийния номер, публичния ключ, срока на валидност и електронния подпис/електронния печат.

StampIT информира Абонатите за изтичане на срока на валидност на издадените от него квалифицирани удостоверения най-малко 30 дни преди датата на изтичане на срока, с изпращане на уведомление на посочен от абоната имейл адрес.

Процедурата за издаване на квалифицирано удостоверение с генериране на нова ключова двойка (rekey) се прилага и по отношение на квалифицираните удостоверения на Удостоверяващия и на Регистриращия орган.

4.7.1 Обстоятелства, при които се прилага издаване на квалифицирано удостоверение с генериране на нова двойка ключове (rekey)

StampIT ще изпълни искане за подновяване (rekey), при следните условия:

- искането да е подадено от същия Абонат;
- квалифицираното удостоверение да не е прекратено;
- може да бъде подадено в срока на валидност на квалифицираното удостоверение, както и до 30 дни след изтичане на този срок;
- ако искането за издаване е за същия тип квалифицирано удостоверение или за квалифицирано удостоверение по същата Политика, по която е издадено валидното квалифицирано удостоверение.

4.7.2 Лица, които могат да правят искане за актуализация на ключова двойка

Искането за подновяване на квалифицирано удостоверение с генериране на нова ключова двойка (rekey) може да бъде направено само от титуляря/ създателя на електронния подпис/ електронния печат или от абоната на квалифицираното удостоверение за автентичност на уебсайт.

4.7.3 Обработка на искането за подновяване на квалифицирано удостоверение с генериране на нова двойка ключове (rekey)

Искането за подновяване на квалифицирано удостоверение с генериране на нова ключова двойка (rekey) трябва да бъде получено от StampIT преди датата на изтичане на срока на валидност, вписан в удостоверението или най-късно до 30 (тридесет)дни след изтичане на този срок.

Подаването на искане за подновяване може да се извърши на място при Регистриращия орган или отдалечено – с електронно искане, подписано с квалифицирано удостоверение.

След успешна идентификация и проверка за наличие на условията за подновяване на квалифицирано удостоверение с генериране на нова ключова двойка (rekey), Регистриращият орган потвърждава искането и изпраща заявка към Удостоверяващия орган, който изпълнява искането.

При неуспешна идентификация и проверка за наличие на условията за подновяване на квалифицирано удостоверение с генериране на нова ключова двойка (rekey), Регистриращият орган отхвърля искането и уведомява заявителя за причината. Отхвърлянето на искането не представлява пречка за подаване на ново искане за издаване на квалифицирано удостоверение.

Удостоверяващият орган незабавно (в реално време) издава исканото квалифицирано удостоверение, подписва го с частния ключ на StampIT и го публикува незабавно в Списъка на издадените квалифицирани удостоверения.

Удостоверяващият орган изпраща издаденото удостоверение на Регистриращия орган за предоставяне на Титуляря/ Създателя/ Абоната или на упълномощеното лице.

В случаите на отдалечено подновяване Удостоверяващият орган изпраща удостоверението на Титуляря/ Създателя/ Абоната, който го записва на устройството за създаване на електронен подпис/ печат, на което е генерирана ключовата двойка за това удостоверение.

4.7.4 Предоставяне на ново квалифицирано удостоверение

Регистриращият орган записва удостоверението на устройството за създаване на електронен подпис/ печат, на което е генерирана ключовата двойка за това удостоверение и го предава на Титуляря/ Създателя/ Абоната или на упълномощеното лице.

4.7.5 Потвърждение за приемане на ново квалифицирано удостоверение

Прилагат се изискванията на т.4.4.1.

4.7.6 Публикуване на ново квалифицирано удостоверение

Издаденото ново квалифицирано удостоверение се публикува незабавно в регистъра на издадените удостоверения и е валидно от момента на публикуването му. От този момент удостоверението е публично достъпно, включително и за всички заинтересовани страни.

4.7.7 Информация за доверяващите се страни

Публичният ключ в квалифицираното удостоверение, съответстващ на държания от Титуляря/ Създателя/ Абоната частен ключ, е достъпен за всички доверяващи се страни в Публичния регистър на издадените квалифицирани удостоверения. Всяка доверяваща се страна следва да използва публичния ключ и удостоверението на Титуляря/ Създателя/ Абоната в съответствие с изискванията на означената в квалифицираното удостоверение политика.

Доверяващите се страни трябва да използват публичния ключ само след проверки на: статуса на квалифицираното удостоверение и електронния подпис на Доставчика.

4.8 Промяна в квалифицирано удостоверение

4.8.1 Обстоятелства при които се прилага промяна в квалифицирано удостоверение

Промяна в квалифицирано удостоверение е необходимо да се извърши при промяна на данните, които са вписани във вече издадено и публикувано квалифицирано удостоверение. В тези случаи се генерира нова двойка ключове и се издава ново квалифицирано удостоверение. При промяната се прилага процедурата за издаване на ново квалифицирано удостоверение.

4.8.2 Лица, които могат да правят искане за промяна в квалифицирано удостоверение

Искането за промяна в квалифицирано удостоверение може да бъде направено само от титуляря/ създателя на електронния подпис/ електронния печат или от абоната на квалифицираното удостоверение за автентичност на уебсайт.

4.8.3 Обработка на искането за промяна в квалифицирано удостоверение

Искането за промяна в квалифицирано удостоверение трябва да бъде получено от StampIT преди датата на изтичане на срока на валидност, вписан в удостоверението, но не по-късно от 30 (тридесет) дни след изтичане на срока на валидност.

Подаването на искане за промяна може да се извърши на място при Регистриращия орган или отдалечено – с електронно искане, подписано с квалифицирано удостоверение.

След успешна идентификация и проверка за наличие на условията за промяна на квалифицирано удостоверение, Регистриращият орган потвърждава искането и изпраща заявка към Удостоверяващия орган, който изпълнява искането.

При неуспешна идентификация и проверка за наличие на условията за промяна на квалифицирано удостоверение Регистриращият орган отхвърля искането и уведомява заявителя за причината. Отхвърлянето на искането не представлява пречка за подаване на ново искане за издаване на квалифицирано удостоверение.

Удостоверяващият орган незабавно (в реално време) издава исканото квалифицирано удостоверение, подписва го с частния ключ на StampIT и го публикува незабавно в Списъка на издадените квалифицирани удостоверения.

Удостоверяващият орган изпраща издаденото удостоверение на Регистриращия орган за предоставяне на Титуляря/ Създателя/ Абоната или на упълномощеното лице.

4.8.4 Потвърждение за приемане на ново квалифицирано удостоверение

Прилагат се изискванията на т.4.4.1.

4.8.5 Публикуване на ново квалифицирано удостоверение

Издаденото ново квалифицирано удостоверение се публикува незабавно в регистъра на издадените удостоверения и е валидно от момента на публикуването му. От този момент удостоверението е публично достъпно, включително и за всички заинтересовани страни.

4.8.6 Информация за доверяващите се страни

Публичният ключ в квалифицираното удостоверение, съответстващ на държания от Титуляря/ Създателя/ Абоната частен ключ, е достъпен за всички доверяващи се страни в Публичния регистър на издадените квалифицирани удостоверения. Всяка доверяваща се страна следва да използва публичния ключ и удостоверението на Титуляря/ Създателя/ Абоната в съответствие с изискванията на означената в квалифицираното удостоверение политика.

Доверяващите се страни трябва да използват публичния ключ само след проверки на: статуса на квалифицираното удостоверение и електронния подпис на Доставчика.

От особена важност е доверяващите се страни да не използват публичния ключ след прекратяване на удостоверението или в момент, когато то е спряно.

4.9 Спиране и прекратяване на квалифицирано удостоверение

Спирането и прекратяването на валидността на квалифицирано удостоверение са установени оперативни практики на StampIT.

Спиране и прекратяване на квалифицирано удостоверение са действия на StampIT, които е възможно да бъдат извършени в периода на валидност на удостоверението.

Спирането на квалифицирано удостоверение цели да бъде временно спряна неговата употреба, като за периода на спирането квалифицираното удостоверение временно губи своята валидност.

Прекратяването на квалифицирано удостоверение спира за постоянно действието на удостоверението, като от момента на прекратяването квалифицираното удостоверение губи своята валидност и тя не може да бъде възстановена при никакви обстоятелства. StampIT не допуска подновяване или възобновяване на квалифицирано удостоверение след прекратяването му.

При спиране или прекратяване удостоверението се включва незабавно, но не-по - късно от 3 (три) часа от получаване на искането, в CRL списъка със съответната причина (Reason) за спиране. Действието на удостоверението се преустановява от датата и часа на публикуване в CRL списъка.

С прекратяване на удостоверението на Удостоверяващия орган, с което се подписват квалифицираните удостоверения за електронен подпис/ електронен печат/ автентичност на уебсайт, се прекратява действието на всички издадени от него валидни удостоверения.

Спирането и прекратяването може да бъде извършено само от Удостоверяващия орган, издал квалифицираното удостоверение.

StampIT съхранява надлежно информацията относно прекратяване на валидността на квалифицираните удостоверения и я предоставя на всяка доверяваща се страна без ограничения. Тази информация е достъпна както по време на срока на валидност на прекратеното квалифициране удостоверение, така и след изтичането на този срок.

StampIT ще прекрати издадените от него квалифицирани удостоверения, ако прекрати дейността си, без да я е прехвърлил на друг доставчик. В този случай StampIT ще уведоми абонатите, титулярите/ създателите и ще прекрати удостоверенията с едномесечно предизвестие. В едномесечен срок след уведомяването StampIT ще възстанови на абонатите платената от тях сума, в размер изчислен съобразно оставащия срок на договора за квалифицирана удостоверителна услуга.

Когато прекратяването на квалифицирано удостоверение е поради грешка на персонала на StampIT или поради компрометиране на оперативен частен ключ на StampIT, Доставчикът ще издаде на Абоната еквивалентно квали-

фицирано удостоверение за своя сметка при спазване на правилата и процедурите за издаване на съответния вид удостоверение.

Услугите по спиране, възобновяване и прекратяване са достъпни денонощно, 7 дни в седмицата, като при срив в системите доставчикът е длъжен да възстанови услугите не по-късно от 3 (три) часа.

Времето в системите, свързани със спиране и прекратяване на удостоверения се синхронизира спрямо UTC поне веднъж на 24 часа.

4.9.1 Основания за прекратяване на квалифицирано удостоверение

StampIT прекратява действието на квалифицирано удостоверение, издадено от него при следните обстоятелства:

- 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 съответната Политика и настоящата Практика на StampIT;
- Титулярят/Създателят, съответно Абонатът е нарушил задълженията си по договора за предоставяне на квалифицирани удостоверителни услуги;
- изпълнението на някое задължение по съответната политика и настоящата Практика 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;
- смърт или поставяне под запрещение на Титуляря/ Абоната (когато абонатът е физическо лице);
- прекратяване на представителната власт на Титуляря спрямо Абоната;
- прекратяване на договора за квалифицирана удостоверителна услуга;
- прекратяване на дейността на Удостоверяващия орган;

Квалифицирано удостоверение, което принадлежи на Удостоверяващия орган може да бъде прекратено от неговия издаващ орган, при наличие на някое от следните обстоятелства:

- когато Удостоверяващият орган има основания да смята, че информацията в издаденото удостоверение е невярна;
- когато частният ключ на Удостоверяващия орган или неговата информационна система са нарушени по начин, засягащ доверието на удостоверенията, издадени от този орган;
- когато Удостоверяващият орган съществено е нарушил задължение, произлизащо от настоящата „Практика при предоставяне на квалифицирани удостоверителни услуги".

4.9.2 Лица, които могат да правят искане за прекратяване на квалифицирано удостоверение. Гратисен период.

Прекратяването се извършва по искане на:

- Титуляря/Създателя или Абоната;
- упълномощен представител на Удостоверяващия орган (в случая овластеното лице е администратор по сигурността на StampIT).

Лицата, които имат право да поискат прекратяване на квалифицирано удостоверение са длъжни да подадат искане за прекратяване възможно най-скоро след узнаване, че е налице основание за прекратяване.

Прекратяването се извършва след идентификация и проверка на информацията за самоличност на лицето, заявило прекратяването и уточняване на причината за прекратяване.

Искането за прекратяване на квалифицирано удостоверение може да бъде подадено:

- на място при Регистриращия орган;
- отдалечено – с подадено по електронен път искане за прекратяване на квалифицирано удостоверение, когато е подписано с квалифицираното удостоверение, чието прекратяване се иска или с квалифицирано удостоверение за квалифициран електронен подпис, издадено на същия Титуляр/Създател или Абонат.

4.9.3 Процедура за прекратяване на квалифицирано удостоверение

4.9.3.1 Процедура за прекратяване на квалифицирано удостоверение на краен потребител

След подаване на искане за прекратяване на квалифицирано удостоверение до Регистриращия орган, искането се регистрира и проверява от Регистриращия орган.

Проверката обхваща идентификация и проверка на информацията за самоличност на лицето, заявило прекратяването и уточняване на причината за прекратяване.

При положителен резултат от проверката на искането, Регистриращият орган изпраща заявка за прекратяване към Удостоверяващия орган, който прекратява валидността на квалифицираното удостоверение.

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

При неуспешна идентификация и проверка на самоличността на заявителя и/ или на условията за прекратяване Регистриращият орган отказва да изпълни искането и незабавно уведомява заявителя за причините. Заявителят може да подаде ново искане за прекратяване на квалифицираното удостоверение, като отстрани причините за отказа.

4.9.3.2 Процедура за прекратяване на квалифицирано удостоверение на Удостоверяващ орган или Регистриращ орган

Квалифицирано удостоверение, издадено на Удостоверяващ или на Регистриращ орган, може да бъде прекратено от органа, който го е издал.

Прекратяването се извършва след подаване на искане за прекратяване от упълномощен представител на Удостоверяващия орган (в случая овластеното лице е администратор по сигурността на StampIT) до StampIT. Удостоверяващият орган незабавно прекратява валидността на квалифицираното удостоверение.

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

4.9.4 Срок за обработка на искането за прекратяване

StampIT обработва искането за прекратяване без неоправдано забавяне, като прекратява валидността на квалифицираното удостоверение и го публикува в CRL списъка не по-късно от 60 минути след потвърждаване на заявката за прекратяване.

4.9.5 Проверка в Списъка със спрени и прекратени удостоверения (CRL). Честота на публикуване.

Всяка Доверяваща се страна е длъжна, при получаване на електронен документ, подписан с квалифициран електронен подпис/ квалифициран електронен печат от Титуляр/Създател, да направи проверка на статуса на квалифицираното удостоверение в актуалния Списък със спрени и прекратени удостоверения (CRL).

Списъците със спрени и прекратени удостоверения (CRL), поддържани от StampITса достъпни на следните адреси:

Издател	Адрес	Честота на публикуване
StampIT Global Root CA	http://www.stampit.org/crl/stampit_global.crl	Незабавно след промяна, но не повече от 365 дни
StampIT Global Qualified CA	http://www.stampit.org/crl/stampit_global_qualified.crl	Незабавно след промяна, но не повече от 3 часа
StampIT Global AES CA	http://www.stampit.org/crl/stampit_global_aes.crl	Незабавно след промяна, но не повече от 3 часа

„Информационно обслужване“АД не носи отговорност за настъпили вреди за доверяващите се страни от неизпълнение на задължението за проверка на статуса на квалифицираното удостоверение.

4.9.6 Проверка на статуса на квалифицирано удостоверение в реално време

Всяко лице (титуляр/създател, абонат, доверяваща се страна и др.) има възможност за проверка на текущия статус на издадено от „Информационно обслужване“ АД квалифицирано удостоверение в реално време през осигурения от StampIT интерфейс за проверка на статуса на издадените квалифицирани удостоверения – OCSP.

OCSP услугата генерира отговор, основан на база данни. OCSP отговора е валиден в продължение на 7 дни. За да се поддържа правилното изпълнение на системата, отговорите на OCSP са кеширани за предварително определено време (обикновено не повече от няколко часа).

Услугата за проверка статуса на удостоверение е публично достъпна на адрес: http://ocsp.stampit.org.

Всяка Доверяваща се страна е длъжна, при получаване на електронен документ, подписан с квалифициран електронен подпис/ квалифициран електронен печат от Титуляр/Създател, да направи проверка на статуса на квалифицираното удостоверение.

„Информационно обслужване“АД не носи отговорност за настъпили вреди за доверяващите се страни от неизпълнение на задължението за проверка на статуса на квалифицираното удостоверение.

4.9.7 Уведомяване при нарушаване на сигурността на частния ключ на Удостоверяващия орган

В случай на нарушаване на целостта/ разкриване на частния ключ на Удостоверяващия орган, StampIT е длъжен незабавно да информира доверяващите се страни.

4.9.8 Основания за спиране на квалифицирано удостоверение

Спирането на квалифицирано удостоверение цели да бъде временно спряна не-говата употреба, като за периода на спирането квалифицираното удостоверение временно губи своята валидност.

StampIT спира действието на валидно квалифицирано удостоверение, издадено от него, при наличието на условия за спиране.

Действията за спиране се предприемат незабавно след получаване на искане за спиране.

4.9.9 Лица, които могат да правят искане за спиране на квалифицирано удостоверение.

Спиране на квалифицирано удостоверение се извършва по искане на:

- Титуляря/Създателя или Абоната;
- Лице, за което според обстоятелствата е видно, че може да знае за нарушение на сигурността на частния ключ;
- Надзорен орган.

Искането за спиране на квалифицирано удостоверение може да бъде по-дадено:

- по телефона;
- на място при Регистриращия орган;

- отдалечено – с подадено по електронен път искане.

4.9.10 Процедура за спиране на квалифицирано удостоверение. Период на спиране.

След подаване на искане за спиране на квалифицирано удостоверение до Регистриращия орган, искането се регистрира.

Регистриращият орган не може да отхвърли искане за спиране.

Регистриращият орган изпраща заявка за спиране до Удостоверяващия орган, който спира действието за квалифицираното удостоверение.

Удостоверението незабавно се включва в CRL списъка със съответната причина (Reason) за спиране и точния срок на спиране.

След спиране на удостоверението, Доставчикът незабавно уведомява Титуляря/ Създателя/ Абоната на спряното квалифицирано удостоверение.

StampIT спира действието на валидно квалифицирано удостоверение за период до уточняване на причините за спиране, но не повече от 48 (четиридесет и осем) часа.

4.9.11 Възобновяване на действието на спряно квалифицирано удостоверение

StampIT възобновява действието на спряно квалифицирано удостоверение, при следните условия:

- При отпадане на основанието за спиране преди изтичане на периода на спиране;
- По искане на Титуляря/Създателя или Абоната, след изясняване на причините, поради които е поискано спирането.

След възобновяване на действието, квалифицираното удостоверение се счита за действително.

4.9.12 Процедура за възобновяване на действието на спряно квалифицирано удостоверение

След подаване на искане за възобновяване на действието на квалифицирано удостоверение до Регистриращия орган, искането се регистрира и проверява от Регистриращия орган.

Проверката обхваща идентификация и проверка на информацията за самолич-ност на лицето, заявило възобновяването.

При положителен резултат от проверката на искането, Регистриращият орган изпраща заявка за възобновяване към Удостоверяващия орган, който изважда квалифицираното удостоверение от текущия CRL списък.

След изтичано срока на спиране Удостоверяващият орган незабавно възобновява действието на спряното удостоверение.

Във всички случаи, процедурата по възобновяване изважда спряното удостоверение от текущия CRL списък и публикува нов списък.

4.10 Проверка на статуса на квалифицираните удостоверения

Директно или чрез услугите на трети страни, StampIT предоставя публичен достъп и управлява директории с издадени, временно спрени и прекратени квалифицирани удостоверения, за да бъде повишено нивото на доверие в неговите услуги. Потребителите и доверяващите се страни са уведомени, че винаги трябва да проверяват директориите с издадените и прекратените квалифицирани удостоверения преди да решат дали да се доверят на информацията, вписана в дадено квалифицирано удостоверения.

StampIT обновява списъците със спрени и прекратени квалифицирани удостоверения съгласно посоченото в т.4.9.5.

StampIT публикува и осигурява достъп до хранилища, съдържащи данни и документи, касаещи удостоверителните услуги, включително тази ПДПКУУ, а също и всяка друга информация, която счита за важна за предоставяните от него услуги.

Услугата за проверка статуса на квалифицирано удостоверение, издадено от StampIT е публично достъпна на адрес: http://ocsp.stampit.org.

Услугите за проверка на статуса на квалифицираните удостоверения са достъпни в режим 24x7.

4.11 Прекратяване на договор за квалифицирани удостоверителни услуги от абонат

Договорът за квалифицирани удостоверителни услуги се прекратява:

- с изтичане на срока на валидност на удостоверението;
- с прекратяване действието на удостоверението при наличие на съответните основания;
- ако се установи, че удостоверението е издадено въз основа на неверни данни, предоставени от **Абоната**, съответно въз основа на премълчани от него данни;
- при прекратяване на юридическото лице на **Доставчика**, без прехвърляне на дейността на друг доставчик на удостоверителни услуги;
- при смърт или поставяне под запрещение на **Абоната** – физическо лице или при прекратяване на юридическото лице на **Абоната** или заличаване на **Абоната** – едноличен търговец от търговския регистър;
- в случай, че за която и да е от страните по договора бъде открито производство за обявяване в несъстоятелност или за обявяване в ликвидация;
- при настъпването на форсмажорни обстоятелства, за което обстоятелство страните си дължат надлежно уведомяване;
- при неизпълнение на задълженията на **Абоната**, посочени в договора, Практиката при предоставяне на квалифицирани удостоверителни услуги от „Информационно обслужване“ АД, съответната Политика при предоставяне на квалифицирани удостоверения и Общите условия за предоставяне на квалифицирани удостоверителни услуги, издадени от “Информационно обслужване” АД.
- при неизпълнение на задължението на Абоната за плащане на цената в договорения срок.

4.12 Доверително съхранение на частен ключ (ескроу)

„Информационно обслужване“АД не предоставя услуги по доверително съхранение на частен ключ (ескроу).

5 Контрол на физическата и организационната сигурност

В тази част на „Практиката при предоставяне на квалифицирани удостоверителни услуги" се описват общите изисквания, които изпълнява StampIT по отношение на контрола на физическата и организационната сигурност, както и по отношение на дейността на служителите.

5.1 Контрол на физическата сигурност

Мерките, предприети по отношение на физическата защита на StampIT са елемент от разработената и внедрена в „Информационно обслужване“ АД Интегрирана система за управление, съответстваща на изискванията на международните стандарти, ISO/IEC 9001:2008, ISO/IEC 27001:2013 и ISO/IEC 20000-1:2011.

Мерките, свързани с физическата защита на данните, технологичните системи, помещенията и свързаните с тях поддържащи системи са насочени към предотвратяване на:

- неразрешен достъп, нанасяне на щети и намеса в условията на работа;
- загуба, вреди или компрометиране на ресурси;
- компрометиране или кражба на информация или средства за обработка на информацията.

„Информационно обслужване“ АД осигурява физическа защита и контрол на достъпа на помещенията, в които има инсталирани критични компоненти в неговата инфраструктура:

- Квалифициран базов удостоверяващ орган - StampIT Global Root CA;
- Квалифициран оперативен удостоверяващ орган - StampIT Global Qualified CA;
- Квалифициран удостоверяващ орган на време- StampIT Global TSA;
- Квалифициран удостоверяващ орган за проверка на статуса на удостоверенията - StampIT Global OCSP;
- Регистри и хранилища;
- Регистриращи органи.

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.

5.1.1 Помещения и конструкция на помещенията

StampIT използва за дейността си два центъра за обработка на данни (основен и резервен), разположени в специално конструирани и оборудвани помещения в сгради, собственост на „Информационно обслужване“АД. Помещенията са с най-висока степен на контрол на физически достъп, защита от пожар, наводнение и земетресения, както и с датчици за следене на нерегламентирано проникване. В центровете за обработка на данни на „Информаци-

онно обслужване“АД са обособени **места (отделни шкафове с оборудване),** в които се помещават Удостоверяващият орган на Доставчика и всичките централни компоненти на инфраструктурата.

5.1.2 Физически достъп

Физическата сигурност на системите за издаване и управление на удостоверения е съобразена с изискванията на приложимите международни стандарти и препоръки. За оборудването на StampIT е осигурена физическа неприкосновеност, установен е двуфакторен контрол на достъпа и денонощна физическа охрана. Не е позволен достъп до шкафа с оборудването, без присъствието на минимум 2 (две) оторизирани технически лица на StampIT, като всеки достъп до помещенията с критична инфраструктура се документира в специални журнали и в електронната система за контрол на достъпа на „Информационно обслужване“ АД.

В помещенията на StampIT има система за видеонаблюдение, сигнално-охранителна система и система за контрол на достъпа. Всички системи се проверяват периодично, спрямо изискванията на интегрираната система за управление и приложимото национално право. Овластените лица от персонала на StampIT спазват стриктно разработените вътрешни процедури за достъп до различните зони с ограничен физически достъп.

В офисите на „Информационно обслужване“АД Регистриращите органи са обособени и отделени от останалите помещения и са оборудвани с техниката, която е необходима за безопасно съхранение на данни и документи. Достъпът до тези зони се контролира и ограничава до оторизирани лица, свързани с дейността на Регистриращия орган (оператори на регистриращия орган, системни администратори) и техните клиенти.

5.1.3 Електрическо захранване и климатични системи

Оборудването, обслужващо StampIT, се захранва от резервирана UPS система. В центровете за обработка на данни е инсталирана климатизираща система, която поддържа постоянна температура и влажност (съгласно параметрите препоръчани от производителя). В двата центъра се поддържа и допълнително външно електрическо захранване от дизелов генератор, който се включва при необходимост. В случай на срив в главния електропровод, системата превключва на авариен източник на захранване (UPS и/или дизелов генератор).

5.1.4 Наводнение

За следене на влажността в центровете за обработка на данни, са монтирани сензори за отчитане нивото на влага. Тези сензори са интегрирани в системите за сигурност на сградите на „Информационно обслужване“АД. Охраната и служителите на StampIT са инструктирани и задължени при настъпване на инциденти да уведомяват незабавно службите за пожарна и аварийна безопасност, администратора по сигурността и системния администратор.

5.1.5 Противопожарна защита

StampIT спазва всички норми за пожарна безопасност, като извършва дейност в съответствие с всички нормативни изисквания в тази област, както и с наличието на добри практики, свързани със защита от пожар.

Защитените помещения с критична инфраструктура (центрове за обработка на данни) се намират в сгради, в които са инсталирани: звукова и светлинна пожароизвестителна система и активна пожарогасителна система с газ.

При пожар е предвидено изключване на подаването на електрическото захранване към съоръженията и потушаване на пожара с газ, при невъзможност за локално (ръчно) гасене.

5.1.6 Съхранение на носители на данни

Всички носители, съдържащи софтуер, архиви на данни или одитна информация се съхраняват в огнеупорни каси в специални архивни помещения с въведен контрол на достъп. StampIT управлява съхранението на данните, както е указано в съответните приложими стандарти и спрямо политиките и процедурите на Интегрираната система за управление на „Информационно обслужване“ АД

5.1.7 Унищожаване на носители на данни

StampIT спазва правилата за надеждно унищожаване на носители на данни – електронни и/или хартиени – определени, спрямо Интегрираната система за управление на „Информационно обслужване“ АД, които включват:

- използване на средства за сигурно унищожаване на данни на електронни носители;
- нарязване на отпечатаните материали и ленти.

Хартиените и електронни носители, съдържащи евентуално значима информация за сигурността на StampIT, след изтичане на определения съгласно вътрешните правила период на съхранение, се унищожават в специални устройства за нарязване.

Носителите на информация за криптографските ключове и ПИН/ПУК номера, използвани за тяхното съхранение, се раздробяват с подходящи устройства. Това се отнася за носителите, които не позволяват окончателно заличаване на съхранени данни и тяхното повторно използване.

5.1.8 Срок на употреба на технически компоненти

Експлоатационният срок на физическите елементи в състава на всички критични компоненти на инфраструктурата на StampIT се определя съгласно предписаните експлоатационни изисквания на производителя. След изтичане на предвидения от производителя период на работа, същите се извеждат от употреба.

Извършва се редовна профилактика на всички критични устройства, с период на профилактиката минимум веднъж на 6 (шест) месеца.

5.2 Организационен контрол

Тази част от „Практиката при предоставяне на квалифицирани удостоверителни услуги" представя списъка на ролите, които са определени за служителите на „Информационно обслужване“ АД, отговарящи за функционирането на StampIT, като са описани отговорностите и задълженията, свързани с всяка определена роля.

Всички процедури, касаещи сигурността при издаването, администрирането и използването на квалифицирани удостоверения се изпълняват от собствен доверен персонал на StampIT. Доставчикът има достатъчен брой квалифицирани служители, които във всеки момент от осъществяването на дейността му да осигуряват изпълнение-

то на необходимите процедури в съответствие с действащото законодателство и вътрешните правила на Дружеството.

5.2.1 Доверени роли

Детайлното разпределение на функциите и отговорностите на персонала е регламентирано във вътрешните документи на „ИО“ АД: длъжностни характеристики, длъжностно - щатно разписание и съответни вътрешни оперативни процедури. Функциите са разпределени по такъв начин, че да бъде сведена до възможния минимум опасността от компрометиране, изтичане на конфиденциална информация и/ или възникване на конфликт на интереси.

5.2.1.1 Доверени роли в „Информационно обслужване“ АД

„Информационно обслужване“АД поддържа квалифицирани служители на длъжностите, които осигуряват изпълнението на задълженията му във всеки момент при осъществяването на дейността на квалифициран доставчик на квалифицирани удостоверителни услуги, в съответствие с нормативната уредба. Доставчикът осигурява дейността си със собствен персонал. Разработени и утвърдени са длъжностни характеристики за всяка една от доверените роли на персонала, както следва:

- администратор по сигурността - цялостна отговорност по управлението и изпълнението на процедурите по сигурност на системите: разработва политика по сигурността; предприема мерки за техническа защита на данните и системите; определя операционните мерки за сигурност; осъществява пряк контрол по отношение на спазването на изискванията за сигурност на информационните системи, като следи за спазването на процедурите за сигурност при инсталирането, конфигурирането, поддръжката и промените в информационните системи или мрежата.
- системен администратор - отговаря за инсталиране, конфигуриране и поддържане на надеждни системи за управление на услугите: възстановяване на системата при необходимост; извършване на преконфигурация на устройства и системи по повод реализация на нови услуги или решения; следене за техническото и софтуерно състояние на сървърите и сигнализиране за нередности;
- системен оператор - отговаря пряко за експлоатацията на надеждните технологични системи на StampIT и за създаване на резервно копие (backup) на системата: създаване и управление на квалифицираните удостоверения, включително създаване на двойка ключове - частен и публичен за квалифициран електронен подпис/печат; използване на ефикасни технологии за осигуряване на ежедневната работа на системата; провеждане на изпитвания и проверки за безотказна работа и сигурност на системата; спазване на техническите изисквания за работа с устройствата и при установяване на техническа неизправност - уведомяване на съответните длъжностни лица;
- системен одитор - отговаря за съхранение на данни, архивиране и управление на регистрите на събития (по-специално за проверката на тяхната цялост) при извършване на вътрешни проверки, както и за съответствието на дейността с Регламент (ЕС) № 910/2014. Системният одитор контролира дейността на всички Регистриращи органи, опериращи въз основа на възлагане от StampIT.

5.2.2 Изисквания за разделяне на отговорностите

Доверените роли на персонала на StampIT задължително се изпълняват от различни служители на „Информационно обслужване“АД..

5.2.3 Идентификация и проверка за самоличност за всяка роля

Персоналът на StampIT подлежи на идентификация и проверка за самоличност във всяка от следните ситуации:

- когато са включени в списък на лица с ограничен достъп до сгради/ помещения на StampIT;
- когато са включени в списък на лица с физически достъп до технологичната система и мрежови ресурси на StampIT;
- когато са овластени да изпълняват конкретна възложена роля;
- при създаване и възлагане на акаунт и парола в информационната система на
- StampIT;
- Всяко упълномощаване за изпълнение на определена роля изисква:
- ролята да бъде уникална и пряко свързана с конкретната личност;
- да не може ролята да бъде споделена с друго лице;
- да бъде ограничено до функцията, произтичаща от ролята и да се изпълнява от точно определен човек.

За изпълнението на всяка роля „Информационно обслужване“ предоставя на служителя софтуер, технологична система и достъп до операционните системи на StampIT.

5.3 онтрол на персонала

Персоналът на „Информационно обслужване“ АД се състои от голям брой високо квалифицирани служители. Лицата, извършващи доверени роли имат необходимата професионална подготовка и опит, което гарантира спазване на изискванията за сигурност и технически норми за оценка на сигурността. Професионалните познания в областта на информационните системи, криптографията и инфраструктурата на публичните ключове дава възможност на служителите с доверени роли да изпълняват качествено своите служебни задължения. Служителите на „ИО“ АД преминават периодично през курсове за допълнително обучение, отговарящо на съвременните изисквания в областта на предоставяне на услуги, свързани с квалифициран електронен подпис, както и съпътстващи такива услуги.

5.3.1 Квалификация на персонала

„ИО“ АД задължително се уверява, че лицето, което изпълнява доверена роля на Удостоверяващия орган или в системата на Регистриращите органи отговаря най-малко на следните изисквания за заемане на длъжността:

- има завършено най-малко средно образование;

- подписало е трудов или граждански договор, описващ неговата роля в системата и съответните отговорности;
- преминало е необходимото специализирано обучение, свързано с обхвата на задълженията и отговорностите за неговата позиция;
- преминало е обучение в областта на защита на личните данни;
- подписало е споразумение, съдържащо клауза, относно защитата на чувствителната информация и на конфиденциалност на данните на потребителите;
- не изпълнява други задачи, които могат да доведат до конфликт на интереси с дейността на StampIT.

5.3.2 Процедури за проверка на персонала

Всеки нов служител на „Информационно обслужване“ АД, който кандидатства да изпълнява доверена роля, се проверява:

- за да се потвърди предишна заетост и професионален опит;
- за препоръки (включително проверка на препоръки);
- за да се потвърди образователната степен;
- за да се провери свидетелство за съдимост;
- за да се провери медицинска пригодност;
- за да се провери самоличност.

„ИО“ АД може да отхвърли кандидатурата, свързани с изпълнението на доверената роля или да предприеме действия срещу лице, което вече е заело и изпълнява доверена роля, ако се установи, че:

- е било подведено от кандидат или служител по отношение на исканите данни, по-горе;
- получи силно неблагоприятни или не много надеждни препоръки от предишни работодатели;
- получи информация за кандидата за наличие на криминално минало или негов служител е осъден с влязла в сила присъда.

При наличие на някое от горните обстоятелства, по-нататъшните стъпки се извършват в съответствие с приложимото право.

5.3.3 Изисквания за обучение на персонала

Персоналът, който изпълнява функциите и задачите, произтичащи от неговата заетост в StampIT или заетост в Регистриращия орган (при наличие на външен Регистриращ орган), задължително преминава първоначално и периодично през обучения в следните области:

- 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);
- Практика при предоставяне на квалифицирани удостоверителни услуги от „Информационно обслужване“АД (eIDAS-CPS);
- Нормативни актове, процедури и документация, свързана със заеманата роля;
- Технологии за сигурност и процедури, свързани със сигурността, използвани от Удостоверяващия орган и Регистриращия орган;
- Системен софтуер на Удостоверяващия орган и Регистриращия орган;
- Отговорности, произтичащи от ролите, изпълнявани в системата;
- Процедури, изпълнявани при отказ на системата или прекъсване на дейностите на Удостоверяващия орган.

5.3.4 Честота на обученията и изисквания за повишаване наквалификацията на служителите

Обученията, описани по-горе се провеждат периодично – най-малко веднъж на 12 (дванадесет) месеца.

При промени в нормативни актове и/или в документацията и дейността на StampIT обученията се провеждат своевременно, задължително преди влизането в сила на съответната промяна.

5.3.5 Смяна на работата

„Информационно обслужване“АД няма изисквания в тази област.

5.3.6 Санкции за извършване на непозволени действия

В случай на откриване или на подозрение за неоторизиран достъп, системният администратор заедно с администратора по сигурността (служители на Доставчика) или единствено на системния администратор (служител на Регистриращия орган, при наличие на външен Регистриращ орган) прекратяват достъпа на извършителя до Доставчика или системата на Регистриращия орган. По-нататъшните дисциплинарни действия се предприемат от ръководството на „Информационно обслужване“АД.

5.3.7 Договор с персонала

Освен служителите, назначени на трудов договор, „Информационно обслужване“АД може да наема и външни лица на граждански договор за изпълняване на доверени роли в StampIT. В такива случаи, те следва да отговарят на изискванията, които се отнасят за служителите, назначени в „Информационно обслужване“АД. Същите изисквания се прилагат и по отношение на консултанти на „Информационно обслужване“АД, когато предмет на консултациите

са дейностите, изпълнявани от лицата с доверени роли в StampI. Изпълнителите и консултантите преминават през същата процедура за проверка, както служителите на „Информационно обслужване“АД.

5.3.8 Документация, предоставена на персонала

Ръководството на „Информационно обслужване“АД и Ръководството на Регистриращия орган (в случай на външен Регистриращ орган) трябва да предоставят на своите служители достъп до следните документи:

- 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);
- Практика при предоставяне на квалифицирани удостоверителни услуги от „Информационно обслужване“АД (eIDAS-CPS);
- Нормативни актове, процедури и документация, свързана със заеманата роля;
- Технологии за сигурност и процедури, свързани със сигурността, използвани от Удостоверяващия орган и Регистриращия орган;
- Системен софтуер на Удостоверяващия орган и Регистриращия орган;
- Отговорности, произтичащи от ролите, изпълнявани в системата;
- Процедури, изпълнявани при отказ на системата или прекъсване на дейностите на Удостоверяващия орган.
- Образци на искания, заявления и декларации;
- Извлечения от документи, съответстващи на изпълняваната роля, включително и на всички спешни процедури;
- Отговорности и задължения, свързани с изпълняваната роля в системата на Доставчика.

5.4 Записи на събития и поддържане на журнали

Управлението на събитията, записващи действията на потребители, изключителни случаи, грешки и събития, свързани със сигурността на информацията, се извършва според утвърдени политики и процедури за 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 услу-

ги", Регламент (ЕС) № 910/2014 и действащото национално законодателство. Одиторският екип оценява ефективността на съществуващите процедури за сигурност.

5.4.1 Видове записи

StampIT поддържа записи за всяка дейност в рамките на инфраструктурата, управляваща доставката на квалифицирани удостоверителни услуги и съпътстващите услуги.

Тези записи са разделени в три отделни категории:

- Записи на системата
  - при инсталиране на нов или допълнителен софтуер;
  - при стартиране на системите и приложенията в тях;
  - при успешни опити за стартиране на и достъп до хардуерни и софтуерни PKI-компоненти (Public Key Infrastructure/Инфраструктура на публичния ключ" на системите);
  - генериране и управление на двойките ключове и удостоверения за удостоверяващите органи и компоненти в инфраструктурата на StampIT;
  - управление на криптомодулите;
  - генериране и управление на двойките ключове и удостоверения на Потребителите; стартиране на системите и приложенията в тях;
  - при опити за стартиране и достъп до хардуерни и софтуерни PKI-компоненти на системите;
  - генериране на Списък със спрени и прекратени удостоверения (CRL);
  - публикуване на издадени валидни удостоверения в Публичния регистър;
  - конфигуриране на профили на удостоверения;
  - статус на удостоверение в реално време;
  - удостоверяване на време на представено съдържание.
- Грешки
  - записите съдържат информация за грешки на нивото на мрежови протоколи;
  - при спиране на системите и приложенията в тях;
  - при неуспешни опити за стартиране и достъп до хардуерни и софтуерни PKI-компоненти на системите;
  - при системни софтуерни и хардуерни сривове на системите и други аномалии в платформите.
- Одити - записите съдържат информация, свързана с квалифицираните удостоверителни услуги, например:
  - постъпили документи за регистриране с цел установяване на идентичност и проверка за самоличност;

- на искания за издаване, подновяване, спиране/възобновяване и прекратяване на квалифицирани удостоверения; вътрешни процедури за идентификация и регистрация;
- издаване на Списък на спрените и прекратени удостоверения (CRL);
- Други

- Дневниците на събитията съдържат следното, без да се ограничават до:
  - данни за идентификация на потребителите;
  - дата, час и подробности за важни събития, напр. влизане и изли-зане от системата;
  - записи за успешните опити за достъп в системата;
  - записи за успешните опити за достъп до данни и други ресурси;
  - използването на привилегии;
  - файловете, с които е работено и вида на достъпа;
  - предизвикани аларми на системата за контрол на достъпа;

Логовете на информационните системи се настройват да регистрират грешки и изключения при работата в операционните системи и приложните програми. Логовете се преглеждат периодично от упълномощени лица. Записаните грешки се анализират и при необходимост се предприемат действия за отстраняване на техните причини.

5.4.2 Честота на създаване на записи

Информацията за електронните журнали се генерира автоматично.

С цел да се идентифицират възможни незаконни дейности, администраторът по сигурността, системните администратори и одиторът, анализират информацията, най-малко веднъж в рамките на един работен ден.

Администраторът по сигурността има задължението да прави преглед и оценка на точността и пълнотата на регистрираните събития и да проверява съответствието с процедурите за сигурност на „Информационно обслужване“ АД.

Записите в регистъра на събитията се разглеждат в детайли най-малко веднъж месечно. Всяко събитие подлежи на обяснение и се описва в дневник на системния администратор.

5.4.3 Период на съхранение на записи

Журнали на записи на регистрирани събития се съхраняват във файлове на системния диск за най-малко 6 (шест) месеца. След този период, записите се съхраняват в архивите.

Архивирани журнали се запазват в продължение на поне 10 (десет) години.

5.4.4 Защита на записите

Въведени са правила за наблюдение на използването на средствата за обработка на информация, документирани в правилата и процедурите за управление на събитията, а резултатите от тях се преглеждат периодично от упълномощените служители.

Наблюдението на системите включва периодичен преглед на предоставените права за достъп, както е описано в ПИС 06 Контрол на достъпа и сигурност на мрежите.

Регистъра на събитията може да бъде преразгледан единствено от администратора по сигурността, системния администратор или одитора. Достъп до регистъра на събитията е конфигуриран по такъв начин, че:

- само упълномощени лица имат право на четене на записите в регистъра;
- само администраторът по сигурността може да архивира или изтрива файлове (след тяхното архивиране), съдържащи регистрираните събития;
- е възможно да се открие всяко нарушение на целостта.

5.4.5 Поддържане на резервни копия на записи на събития

Поддържат се резервни копия от записите в логовете на системите, които се съхраняват надеждно, спрямо процедура за създаване на архивни копия, която е част от ИСУ на „Информационно обслужване“ АД.

5.4.6 Система за уведомяване след анализ на записи

Честотата на прегледите на резултатите от наблюдението зависи от включените рискове, определени при извършената оценка на риска.

Рискови фактори са:

- критичността на процесите на програмата;
- стойността, чувствителността и критичността на участващата информация;
- натрупаният опит от предишно проникване и неправилно използване на системата и честотата на използваните уязвимости;
- степента на обвързаност на системата (особено с обществени мрежи);
- деактивиране на регистриращите устройства.

Политиките за наблюдение на използването на системата осигуряват, че потребителите извършват само действия, за които са изрично упълномощени.

5.4.7 Уязвимост и оценка

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

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

Администраторът по сигурността е отговорен за извършване на вътрешните одити, в частта касаеща предоставянето на квалифицирани удостоверителни услуги. Той контролира опазването на записите по сигурността в журна-

лите, коректното архивиране на резервните копия, както и дейностите, изпълнени в случай на заплахи и съответствието с настоящата Практика.

5.5 Архивиране

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 абонатите;
- цялата информация за абонатите;
- 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.

5.5.1 Видове архиви

StampIT управлява два вида архиви: хартиени и електронни.

5.5.2 Период за съхранение на архива

StampIT съхранява по надежден начин архивите си за срок не по-кратък от 10 (десет) години. Периодът на съхранение започва от датата на получаване на информацията. Такива архиви могат да бъдат съхранявани в електронен или хартиен формат или всякакъв друг подходящ формат.

5.5.3 Защита на архивна информация

StampIT съхранява архивираните записи по начин, който изключва неоторизирани и недоверени лица да имат достъп до тях. Информацията, която е архивирана по електронен път, е защитена срещу неоторизирано разглеждане, модифициране, изтриване или фалшифициране, чрез внедряването на система за контрол на достъпа (посредством акаунти и пароли). За целите на архивирането се използват надеждни електронни носители, които не могат да бъдат лесно унищожени или изтрити през периода на съхранение. За целите на сигурното съхраняване на архивните файлове в електронна форма те се подписват с електронен подпис.

5.5.4 Възстановяване на архивирана информация

От съществено значение за правилното функциониране на StampIT е възможността резервните копия да бъдат напълно възстановени. Политиката и процедурите за възстановяване са описани в ПИС 09 „Сигурност на информацията“.

5.5.5 Изисквания за отбелязване на времето на архивиране

Архивните данни се обезпечават с удостоверяване на точното време на подписването им.

5.5.6 Съхраняване на архива

Системата за събиране на архивни данни е вътрешна система за StampIT.

Архивната информация (на хартия и на електронни носители) се съхранява надлежно в специални сейфове в отделно помещение с висока степен на физическа защита.

5.5.7 Процедури за достъп и проверка на архивираната информация

Достъп до архива е възможен само за оторизирани служители на StampIT след успешно удостоверяване и потвърждение на правата за достъп.

Данните се проверяват периодично и се съпоставят спрямо оригиналните данни, с цел проверка на целостта на архивираната информация. Тази дейност се извършва под надзора на администратор по сигурността, като се водят записи за всеки етап от процедурата. Резултатите от проверката се записват в съответните регистри на събитията.

Ако се установят повреди или модификации на оригиналните данни, щетите се премахват възможно най-бързо, съгласно вътрешните процедури и правила в StampIT.

5.6 Промяна на ключ на Доставчика

Доставчикът може да промени ключа, съответстващ на издадено удостоверение, само като издаде ново удостоверение или поднови текущото с „rekey".

Частният ключ на Удостоверяващ орган може да бъде променен в случай на:

- изтичане на срока на валидност на съпътстващото му удостоверение;
- въвеждане на нови услуги от StampIT, които налагат промени в характеристиките на частния ключ (например промени свързани със сигурността и изискване за нови приложими криптографски комбинации).

При промяна на частния ключ на Удостоверяващия орган на StampIT се спазват следните правила:

- Удостоверяващият орган, с чийто ключ се подписват потребителските удостоверения, и чийто ключ ще бъде променен, спира издаването на удостоверения 60 (шестдесет) дни преди момента, в който оставащият период на валидност на частния ключ се изравни с периода на валидност на последното издадено удостоверение;
- Удостоверяващият орган, с чийто частен ключ се подписва Списъка със спрени и прекратени удостоверения (CRL) и чийто частен ключ ще бъде променен, продължава да публикува списъци, подписани със стария частен ключ до момента, в който изтече срокът на валидност на последното публикувано удостоверение.

5.7 Компрометиране на ключове и възстановяване след аварии

Тази част от „Практиката при предоставяне на квалифицирани удостоверителни услуги" описва процедурите, извършвани от StampIT, при аварии (включително природни бедствия) за да се възстанови обслужването на потребителите, както е описано в ПИС 14-03 „План за възстановяване след бедствие“.

При евентуални заплахи за настъпване на аварии се прави анализ на наличността на критичните ресурси, необходими за възстановяване на системата. Правят се текущи оценки на разходите за възстановяване. Доставчикът има процедури за осигуряване на непрекъснатост на процесите, както свързани с информационните технологии, така и с бизнес процесите.

„План за възстановяване след бедствие“ се тества веднъж годишно и е обект на обучение от служителите на

StampIT. Основните цели на Плана са:

- Да се възстанови максимално бързо и рентабилно обичайната работа на структурните звена на Доставчика при възникване на извънредни обстоятелства или бедствие.
- Да се разработи, тества и документира добре структуриран и лесно разбираем План за възстановяване при бедствие, който да помогне на Организацията да се възстанови възможно най-бързо и ефективно от непредвидено бедствие или извънредно положение, което прекъсва информационните системи и работните операции.

5.7.1 Действия при аварии

В ситуация на криза или възникване на инцидент, криза, бедствие, авария, високорискова или интензивна ситуация Изпълнителният директор на „Информационно обслужване” АД обявява състояние на бедствие и определя кой сценарии ще бъде приложен за конкретната ситуация, за да се ограничи въздействието върху персонала, ресурсите и активите на организацията. В момента, когато на инцидента е противодействано и бедственото положение е овладяно, се преминава към „ОД ПИС 14-01 План за непрекъснатост на дейността”.

Архивните данни, съдържащи информация за исканията за издаване, управление и прекратяване на удостоверения, както и записите на всички издадени удостоверения в базата данни се съхраняват на сигурно и надеждно място и са на разположение в случаи на възникване на авария.

За своевременно откриване на възможни бедствия и аварии „Информационно обслужване“ АД наблюдава всички системи и услуги без прекъсване (24x7), като разполага с денонощен център за управление на услугите, посредством който потребителите могат да уведомяват за инциденти или неизправни услуги.

5.7.2 Инциденти, свързани със сривове в хардуера, софтуера и/или данните

При кражба на хардуер, софтуер и/или данни информацията се предава на администратора по сигурността, който действа, в съответствие с вътрешни процедури, разработени от „ИО“ АД.

Тези процедури са свързани с анализ на ситуацията, разследване на инцидента, мерки за минимизиране на последиците и недопускане на подобни инциденти в бъдеще.

В случай на сривове в хардуера, софтуера или в данните, Доставчикът уведомява потребителите, възстановява компонентите на инфраструктурата и приоритетно възобновява достъпа до Публичния регистър и Списъка със спрени и прекратени удостоверения (CRL).

За постигане на горепосоченото в „Информационно обслужване“ АД е разработена „Политика за управление на инциденти със сигурността на информацията". Доставчикът има план за управление на всички инциденти, които засягат нормалното функциониране на инфраструктурата на публичния ключ. Този план е в съответствие с План за непрекъснатост и План за възстановяване при бедствия.

5.7.3 Компрометиране или съмнение за компрометиране на частен ключ на удостоверяващия орган на StampIT

Доставчикът полага дължимата грижа, за да поддържа непрекъсваемост и цялостност на квалифицираните удостоверителни услуги, свързани с удостоверенията, които издава, поддържа и управлява.

Доставчикът полага максимални грижи в рамките на възможностите и ресурсите си, да минимизира риска от компрометиране на ключовете на Удостоверяващите си органи вследствие на природни бедствия или аварии.

В случай на компрометиране или съмнение за компрометиране на частен ключ на Удостоверяващ орган на StampIT, се предприемат следните действия:

- прекратява се незабавно удостоверението на оперативния орган;
- Удостоверяващият орган генерира нова двойка ключове и ново удостоверение;
- всички абонати на удостоверения се информират за случилото се незабавно, с помощта на средствата за масово осведомяване (информация на страницата на StampIT) и електронна поща;
- информират се всички доверяващи се страни;
- удостоверението, съответстващо на компрометирания ключ се вписва в Списъка със спрени и прекратени удостоверения (CRL), заедно с подходяща причина за прекратяване;
- всички потребителски удостоверения, издадени от удостоверението, съответстващо на компрометирания частен ключ се прекратяват и записват в Списъка със спрени и прекратени удостоверение, като се посочва подходяща причина за прекратяването им;
- издават се нови удостоверения на засегнатите абонати;
- новите удостоверения на абонатите се издават за сметка на StampIT (абонатите не дължат плащане на цената на удостоверенията);
- извършва се незабавен анализ и се изготвя доклад за причината за компрометирането.
- Тези операции се извършват в съответствие с плана, разработен от StampIT, за инциденти със сигурността. Този план се разработва от екип на StampIT под ръководството на администратора по сигурността и се одобрява от Съвета за управление.

5.7.4 Непрекъснатост на бизнеса и възстановяване след аварии

„Информационно обслужване“ АД е разработило и внедрило ПИС 14 Управление на непрекъснатостта на дейността, за случаите на възникване на аварии, като например големи системни или мрежови прекъсвания. Този документ урежда подготовката и процесите, за да се гарантира запазването на дейността на StampIT. Целта на политиката е осигуряване на непрекъснатото функциониране и свеждане до минимум на отрицателните въздействия, като прекъсване на обслужването на клиентите и уронване на обществения престиж на “Информационно обслужване” АД.

В рамките на тази обща цел, конкретната задача е да осигури успешното възобновяване на комуникациите и работата на информационните системи при възникване на аварийна ситуация или пробив в информационната сигурност чрез комбинация от превантивни действия и механизми за контрол и възстановяване. Политиката е съобразена с изискванията за управление на услугите.

Процедурите за възстановяване на системата след аварии са тестват върху всеки компонент на технологичната система на StampIT най-малко веднъж годишно. Тези тестове са част от вътрешния одит.

Актуализация на софтуера е възможна само след провеждане на интензивни тестове в тестова среда и действия в строго съответствие с описаните процедури на StampIT. Всяка промяна в системата изисква съгласие и приемане от администратора по сигурността.

При всяко възстановяване на системата след бедствие, администраторът по сигурността или системният администратор изпълняват следното:

- променят всички използвани преди това пароли;
- премахват всички права за достъп до ресурсите на системата;
-
- променят всички кодове и ПИН номера, свързани с физическия достъп до съоръженията и компонентите на системата;
- преглед на анализ на причините за бедствията.

5.8 Прекратяване на дейността на StampIT

Задълженията, описани по-долу, са разработени, за да минимизират прекъсванията в дейността на абонатите и доверяващите се страни, произтичащи от решението на StampIT да преустанови дейността си.

5.8.1 Изисквания, свързани с прехода до прекратяване на дейността на доставчика

Преди Удостоверяващият орган да прекрати услугите си, той е длъжен:

- да уведоми Надзорния орган за своето намерение да прекрати услугите си, в случай на иск за обявяване на дружеството в несъстоятелност, обявяване на дружеството за недействително или за друго искане за прекратяване, или за започване на процедура по ликвидация. Уведомлението следва да бъде направено 4 (четири) месеца преди договорената дата на прекратяване;

- да уведоми (най-малко 4 месеца преди това) своите абонати за решението да прекрати предоставяните от него услуги;
- да прекрати договорите с организациите, в които има разкрити външни Регистриращи органи;
- да промени статуса на своите удостоверения;
- да прекрати всички удостоверения на абонатите в рамките на обявения период за прекратяване на дейността;
- да уведоми всички свои абонати за преустановяване на услугите и за прехвърляне на поддръжката на информацията на друго надеждно лице;
- да предприеме търговски разумни усилия, за да сведе до минимум нарушаването на интересите на абонатите;
- да извърши необходимите действия, за прехвърляне на поддръжката на цялата имаща отношение информация, във връзка с данните, издадени и получени в качеството на квалифициран доставчик на квалифицирани удостоверителни услуги и по-специално с оглед предоставяне на доказателство при съдебни производства и осигуряване на приемственост при предоставянето на услугата, на друго надеждно лице за достатъчно дълъг период. Тази информация включва: данните, предоставени при издаване, спиране и прекратяване, архиви на логове за събития за съответен период, определен от абоната и доверените страни. Информацията включва и Списъка на спрените и прекратените квалифицирани удостоверения (CRL) за удостоверенията, на които не е изтекъл срока на валидност.
- да изплати компенсации на абонатите, пропорционални на оставащия период на валидност на удостоверенията.

Ако Регистриращ орган като външна организация, е взел решение за прекратяване на представителството на StampIT по повод предоставяни удостоверителни услуги, той е длъжен:

- да уведоми StampIT за своето намерение да прекрати дейността. Уведомлението следва да бъде направено 4 (четири) месеца преди договорената дата на прекратяване;
- да предаде на StampIT цялата документация, свързана с обслужването на абонатите, включително архива и данните за одит.

5.8.2 Прехвърляне на дейност към друг доставчик на квалифицирани удостоверителни услуги

За да се осигури непрекъснатост на квалифицираните удостоверителни услуги за абонатите, StampIT може да подпише споразумение с друг квалифициран доставчик на удостоверителни услуги.

В този случай, StampIT е длъжен и се съгласява да предприеме следното:

- да уведоми Надзорния орган за намерението си, не по-късно от 4 месеца преди датата на прекратяване и прехвърляне на дейността;

- да полага всички усилия и грижи, за да продължи действието на издадените потребителски удостоверения;
- да уведоми писмено Надзорния орган и абонатите, че дейността му се поема от друг регистриран доставчик, като посочи наименованието му. Уведомлението се публикува в Интернет страницата на StampIT;
- да уведоми абонатите относно условията по поддръжка на прехвърлените удостоверения към приемащия Доставчик;
- да промени статуса на оперативните удостоверения и надлежно да предаде цялата документация, свързана с дейността си на приемащия Доставчик, заедно с всички архиви, както и всички издадени удостоверения (валидни, прекратени и спрени);
- да извърши необходимите действия за прехвърляне на задълженията по поддръжка на информацията към приемащия Доставчик;
- да прехвърли управлението на вече издадените удостоверения за крайни потребители към приемащия Доставчик;

Приемащият Доставчик поема правата и задълженията на StampIT с прекратена дейност и продължава да управлява валидните удостоверения до изтичане на срока на тяхната валидност.

Архивът на StampIT с прекратен статус трябва да бъде предаден на Доставчика, приел дейността.

5.8.3 Отнемане на квалифицирания статут на StampIT или на квалифицирания статут на съответна услуга

При отмяна на квалифицирания статут на StampIT или на някоя от предоставяните от него удостоверителни услуги, той е длъжен и се съгласява да предприеме следното:

- да уведоми абонатите си за променения си статут или за променения статут на своите услуги;
- да промени статуса на своите удостоверения;
- да прекрати всички квалифицирани удостоверения на абонатите си от момента на влизане в сила на променения статут и да ги уведоми за прехвърляне на поддръжката на информацията на друго надеждно лице;
- да предприеме търговски разумни усилия, за да се сведе до минимум нарушаването на интересите на потребителите;
- да извърши необходимите действия, за прехвърляне на поддръжката на цялата имаща отношение информация, във връзка с данните, издадени и получени в качеството на квалифициран доставчик на квалифицирани удостоверителни услуги и по-специално с оглед предоставяне на доказателство при съдебни производства и осигуряване на приемственост при предоставянето на услугата, на друго надеждно лице за достатъчно дълъг период. Тази информация включва: данните, предоставени при издване, спиране и прекратяване, архиви на логове за събития за съответен период, определен от абоната и доверените

страни. Информацията включва и Списъка със спрените и прекратените квалифицирани удостоверения (CRL) за удостоверенията, на които не е изтекъл срока на валидност.

- да изплати компенсации на абонатите, пропорционални на оставащия период на валидност на удостоверенията.

6 Управление и контрол на техническата сигурност

Тази част от „Практиката при предоставяне на квалифицирани удостоверителни услуги“ описва процедурите за генериране и управление на криптографските ключове и свързаните с тях технически изисквания.

6.1 Генериране и инсталиране на двойка ключове

Криптографските двойки ключове за оперативните удостоверения на StampIT се генерират и инсталират съгласно инструкциите и процедурите, описани в този документ. Генерирането се осъществява от овластени лица от StampIT. За създаване на подпис се използва защитен механизъм, със защитен профил, определен в съответствие със технически спецификации, определящи нива на сигурността.

Доставчикът използва своите частни ключове само за целите на дейността си, както следва:

- да подписва издаваните оперативни удостоверения на Удостоверяващите органи в своята инфраструктура;
- да подписва издаваните и публикувани Списъци със спрени и прекратени удостоверения (CRL);
- да подписва всички издадени и публикувани удостоверения за електронен подпис/ електронен печат на Абонатите.

Криптографската двойка ключове (частен и публичен) на издаваните удостоверения за електронен подпис/електронен печат в инфраструктурата на StampIT се генерира от оператор на Регистриращия орган на StampIT, с хардуер и софтуер, който е под контрола на StampIT.

За генерирането на двойка ключове на квалифицирано удостоверение за електронен подпис/ електронен печат винаги се използва устройство за създаване на електронен подпис/печат, със защитен профил съгласно Регламент (ЕС) № 910/2014.

Само електронни подписи/ електронни печати, създадени с частен ключ на двойка ключове, които са генерирани в устройство за създаване на квалифициран електронен подпис/ печат имат характера на квалифициран електронен подпис/ квалифициран електронен печат.

Титулярят/ Създателят/ Абонатът се задължава да използва лицензиран софтуер за работа с устройство за създаване на електронен подпис/печат.

6.1.1 Генериране на двойка ключове на Удостоверяващ орган

Доставчикът генерира двойки криптографски (RSA) ключове на базовия и на оперативните удостоверяващи органи като използва хардуерна криптосистема (HSM/Hardware Security Module) с ниво на сигурност FIPS 140-2 Level 3 или по-високо, съответно CC EAL 4+ или по-високо.

Оторизирани лица от персонала на StampIT изпълняват стъпките по генериране, инсталиране и съхраняване на двойките ключове на базовия и на оперативните Удостоверяващи органи, съответно „StampIT Global Root CA“ и „StampIT Global Qualified CA" съгласно документирана вътрешна процедура, съгласувана и утвърдена от ръководството на Информационно обслужване АД.

Процедурата се изпълнява в присъствие на изпълнителния директор на Информационно обслужване АД и представител на отдел „Правен“.

Преди генерирането на двойките асиметрични ключове на StampIT се извършва процедура по инициализиране на криптомодул (HSM/ Hardware Security Module), като се генерират самостоятелно и независимо един от друг симетрични ключове, които се съхраняват върху администраторски смарт карти, защитени с персонален идентификационен номер (PIN) за достъп. Всяка от администраторските смарт карти съдържа част от ключовете за достъп и криптиране на асиметричните ключове на доставчика в криптомодула (HSM). За управление и възстановяване на съхраняваните в криптомодула частни ключове на StampIT са необходими три от общо пет генерирани при инициализирането на криптомодула (HSM) смарт карти и съответните PIN кодове за достъп.

Смарт картите за достъп, криптиране и възстановяване на частните ключове в криптомодула (HSM) се съхраняват поделени в защитени помещения на StampIT с достъп от задължително две или повече лица заедно, стриктно определени със заповед от ръководството на Информационно обслужване АД. Поделените смарт карти със съхранените ключовете, необходими за възстановяване на частните ключове на StampIT и множествения контрол на достъп до тях позволява тези ключове да не могат да бъдат компрометирани и/или нерегламентирано възстановени извън зоните за сигурност на StampIT.

6.1.2 Генериране на двойка ключове на титуляр/ създател

Двойката ключове на Титуляр/Създател на квалифицирано удостоверение за електронен подпис/печат се генерира само в одобрено от StampIT устройство за създаване на 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 електронен подпис/ електронен печат. Частният ключ на генерираната двойка ключове не може да бъде извлечен от устройството. Контролът на частния ключ е чрез код за достъп (PIN). Титулярът използва PIN за достъп до устройството, с цел да осъществи достъп до частния ключ за създаване на квалифициран електронен подпис/печат.

6.1.3 Доставка на частен ключ на потребителя

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 Титуляря/ Създателя 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 на 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.

6.1.4 Доставка на публичен ключ на доставчика на доверяващите се страни

Публичните ключове на StampIT са публикувани в удостоверенията на Удостоверяващия орган на Административен ("SO") във формат X.509 v.3/X.520.

Удостоверенията са публикувани и достъпни в хранилището на StampIT на адрес: https://www.stampit.org/bg/page/814.

Всяка Доверяваща се страна изгражда доверие към StampIT, като приеме и инсталира в системите под неин контрол базовите и оперативни удостоверения на StampIT.

6.1.5 Дължина на ключове

Дължината на базовия ключ на StampIT „StampIT Global Root CA“ е 4096 бита, с приложима комбинация на асиметрични и хеш алгоритми: sha256-with-RSA.

Дължината на двойката ключове на оперативния Удостоверяващ орган „ StampIT Global Qualified CA" е 4096 бита, с приложима комбинация на асиметрични и хеш алгоритми: sha256-with-RSA.

Дължината на двойката ключове на оперативните органи „StampIT Global TSA" е 2048 бита, с приложима комбинация на асиметрични и хеш алгоритми: sha256-with-RSA.

Дължината на двойка ключове за електронен подпис/печат на Титуляр/Създател, генерирана чрез инфраструктурата на StampIT е 2048 бита, с приложима комбинация на асиметрични и хеш алгоритми: sha256-with-RSA.

6.1.6 Параметри на частен ключ

Титулярят/Създателят на ключова двойка е отговорен за проверката на качеството на параметрите на генерирания частен ключ. Той е длъжен да провери способността на ключа да създава електронен подпис.

Устройствата за създаване на квалифициран електронен подпис/печат, предоставени от StampIT и осигурената среда за генериране и съхраняване на ключовете на Титуляря/Създателя са с ниво на сигурност CC EAL 4+, съответно FIPS 140-2 Level 3.

6.1.7 Използване на ключа

Параметрите на използване на двойката ключове, по-конкретно на частния ключ, се съдържат в удостоверението, което издава StampIT чрез атрибутите "Key Usage" и „Extended Key Usage", отговарящи на стандарта X.509 v3.

6.2 Защита на частен ключ и контрол на криптографския модул

Всеки потребител и оператор на Регистриращ орган създава и съхранява частен ключ, като използва надеждна система за неговата сигурност. Регистриращият орган генерира двойка ключове, като използва устройство за сигурно създаване и съхранение на ключове (sscd) и ги предава в защитен вид на потребител.

6.2.1 Стандарти за криптографски модули

Основните компоненти в инфраструктурата на StampIT използват надеждна криптографска система (Hardware Security Module/HSM), сертифицирана за ниво на сигурност FIPS 140-2 Level 3, което удовлетворява нормативните изисквания.

Устройството за създаване на квалифициран електронен подпис, в което се генерира и съхранява частния ключ на Титуляря/Създателя е с ниво на сигурност CC EAL 4+/FIPS 140-2 Level 3 или по-високо.

6.2.2 Контрол на използване и съхранение на частен ключ

Частните ключове на Удостоверяващите органи на StampIT се съхраняват и използват само в криптосистемата (HSM/Hardware Security Module) и са достъпни за възстановяване и използване само от оторизирани системи, които ги използват за подписване на крайни клиентски удостоверения и списъци с прекратени удостоверения /CRL/. Базовият удостоверяващ орган на StampIT е в режим „Offline“.

За управление на съхраняваните в криптомодула частни ключове на StampIT са необходими три от петте генерирани смарт карти и съответните персонални идентификационни номера (PIN) за достъп.

Архив на ключовете се прави първоначално – след създаването на всички ключове, както и в последствие след прегенериране на някои от тях. Частните ключове, намиращи се в криптосистемата (HSM) с ниво на сигурност FIPS 140-2 Level 3 се съхраняват и архивират в криптиран вид, като за възстановяването им са необхомими три от петте генерирани смарт карти при първоначалната инициализиция на криптомодула (HSM). След създаването на архива (Backup), той се съхранява и в сейф на отдалечено местоположение с необходимите мерки за сигурност.

Частният ключ на Титуляря/Създателя се използва само в устройство за създаване на електронен подпис/печат или в устройство с еквивалентно ниво на сигурност (съгласно изискванията на Регламент (ЕС) № 910/2014) и е достъпен посредством личен код за достъп. Едновременно с генериране на двойка ключове на Титуляр/Създател се изпълнява съхраняване на частен ключ в устройство за създаване на електронен подпис/печат.

Доставчикът по никакъв начин не съхранява и не архивира частен ключ на Титуляр/Създател за създаване на електронен подпис/печат.

6.2.3 Доверително съхранение на частен ключ (ескроу)

StampIT не извършва доверително съхранение на частен ключ.

6.2.4 Съхранение на частен ключ

Частните ключове на Удостоверяващите органи на StampIT се съхраняват в криптиран вид, като за декриптирането са необходими три от петте генерирани смарт карти и съответните персонални идентификационни номера (PIN) за достъп.

Разделното съхранение на ключовете върху няколко смарт карти, необходими за декриптиране на частните ключове на Удостоверяващия орган и контролирания достъп до тези устройства не позволява ключовете да бъдат компрометирани или нерегламентирано репродуцирани извън StampIT.

Репродуцирането/ възстановяването на частни ключове на StampIT върху резервен криптомодул след дефектиране на оперативния такъв, се изпълнява по строго контролирана процедура, след заповед на ръководството на Информационно обслужване АД и в присъствието на поне две оторизирани лица, всяко от които контролира достъпа до различни смарт карти.

StampIT не съхранява копия на частните ключове на операторите на Регистриращия орган.

Доставчикът не създава копия на частните ключове на потребителите. Частният ключ на Титуляря/Създателя се съхранява само на устройство за създаване на квалифициран електронен подпис/печат и не може да се възпроизведе на друго устройство.

При дефектиране на потребителско устройство за създаване на квалифициран електронен подпис/печат, Абонатът трябва да го подмени и да поиска издаване на ново квалифицирано удостоверение.

6.2.5 Архивиране на частния ключ

Частният ключ на Удостоверяващия орган, използван за създаване на квалифицирани електронни подписи/печати се архивира, за най-малко 10 години след изтичане на срока му на валидност или след неговото прекратяване. Същото изискване важи и за удостоверението на публичния ключ, съответстващо на частния ключ, след изтичане на срока му на валидност или след прекратяването му.

Удостоверенията на StampIT с изтекъл срок на валидност или прекратени са достъпни на официалния сайт на доставчика за срок от най-малко 10 години.

StampIT не създава архивни копия от частните ключове на операторите на Регистриращия орган и на частните ключове на крайните потребители.

6.2.6 Трансфер на частен ключ в криптографски модул

Трансфер на частен ключ в криптографски модул се извършва в следните случаи:

- В случай на създаване на огледални криптомодули, работещи в клъстер с цел load balancing и high avalibility;
- В случай на дефектирал криптомодул и необходимост от заместване с друг.

Трансферът на частен ключ в криптомодул е специфична операция. Такава операция изисква подходящи мерки и процедури, предотвратяващи разкриването на частния ключ или неговата промяна и/ или фалшифициране по време на изпълнение на операцията.

Трансферът на частен ключ в криптографски модул изисква възстановяване на ключа с кворум три от петте март карти, които са генерирани при първоначалната инициализация на криптомодула. Действията се изпълняват по строго контролирана процедура, след заповед на изпълнителния директор на Информационно обслужване АД и в присъствието на поне две оторизирани лица, всяко от които контролира достъпа до различни смарт карти.

6.2.7 Съхранение на частен ключ в криптографския модул

В зависимост от използвания криптографски модул, частните ключове на Удостоверяващия орган на StampIT се съхраняват винаги в криптиран вид. Независимо от формата на съхранение на частния ключ, той не е достъпен за неоторизирани лица и системи извън криптографския модул.

6.2.8 Метод за активиране на частен ключ

Частните ключове на доставчика се активират посредством отделните части на ключовете, които са записани на три от петте генерирани смарт карти при инициализацията на криптографския модул (HSM). Защитата на частните ключове и тяхното използване се осъществява от криптомодула и достъпа до тях е възможен само след добавяне на оторизирани клиенти през административния интерфейс на криптографския модул. Активирането на удостоверяващите органи /Root CA и SubCAs/, които използват съответните частни ключове на StampIT се извършва чрез административния интерфейс на системата за издаване и управление на удостоверения.

6.2.9 Метод за деактивиране на частен ключ

Частен ключ на Удостоверяващ орган на StampIT, намиращ се в криптографски модул (HSM) се деактивира посредством преустановяване на логическия достъп до този ключ. Деактивирането се осъществява и чрез изчистване на средата, в която се съхранява и криптира ключа. По този начин се прекратява възможността за достъп и използване на частния ключ. Всяко деактивиране на частен ключ на Удостоверяващ орган на StampIT, се изпълнява след заповед на изпълнителния директор на „Информационно обслужване“ АД, по процедура с дефинирани роли и отговорности.

Частен ключ на Титуляр/Създател се деактивира посредством изтриване на контейнерите, съдържащи частния ключ на устройството за създаване на квалифициран електронен подпис/печат или чрез физическо му унищожаване на самото устройство. По този начин окончателно се прекратява възможността за достъп и използване на частния ключ.

6.2.10 Оценка на криптографския модул

StampIT използват надеждни криптографски устройства (Hardware Security Module/HSM), сертифицирани за ниво на сигурност FIPS 140-2 Level 3

6.3 Други аспекти на управлението на двойката ключове

Изискванията описани в тази част на „Практика при предоставяне на квалифицирани удостоверителни услуги“ се прилагат в процедурите за архивиране на публични ключове и процедурите, описващи сроковете на валидност на потребителските ключове и на ключовете на удостоверяващия орган.

6.3.1 Архивиране на публичен ключ

Публичните ключове на Удостоверяващите органи се съдържат в издадените оперативни удостоверения на StampIT и се съхраняват във вътрешен регистър. Публичните ключове са достъпни за доверяващите се страни и потребителите, чрез публикуване на удостоверенията в хранилище, достъпно на интернет сайта на StampIT.

Публичните ключове на Удостоверяващите органи се архивират и съхраняват за период от най-малко 10 години след изтичане на периода на валидност или прекратяването на съответните удостоверения.

Публичните ключове на Титуляри/ Създатели се съдържат в издадените за тях удостоверения, които са публикувани в Публичен регистър на интернет страницата на StampIT.

Публичните ключове на Титуляри/Създатели се съхраняват и периодично архивират.

6.3.2 Период на валидност на квалифицирани удостоверения и употреба на ключове

Периода на употреба на публични ключове се определя от стойността на полето в удостоверението му, описващо валидността на публичния ключ. Валидността на удостоверенията и съответните им частни ключове могат да бъдат съкратени, в случай на прекратяване на удостоверенията.

Максимални периоди на използване на квалифицирани удостоверения:

StampIT Global Root CA	20 (двадесет) години
StampIT Global Qualified CA	20 (двадесет) години
StampIT Global AES CA	20 (двадесет) години
StampIT Global TSA	5 (пет) години
StampIT Global OCSP	5 (пет) години
Титуляр/Създател	не повече от 3 (три) години

Когато се използва ключ за подписване, след изтекъл период на валидност на удостоверението, подписът е невалиден.

Дванадесет месеца преди изтичането на периода на валидност на квалифицирано удостоверение на Удостоверяващ орган, Доставчикът издава ново квалифицирано удостоверение и генерира нова двойка ключове. Удостоверението се прави публично достояние съгласно процедурите, описани в настоящия документ.

6.4 Данни за активиране

Операциите по активиране на частен ключ на Титуляр/ Създател/ Абонат се извършват от Регистриращия орган. Потребителите използват контрол на достъпа до своя частен ключ, посредством потребителски ПИН.

6.4.1 Генериране и инсталиране на данни за активиране

Данни за активиране се използват при първоначално издаване на удостоверение, върху устройство за създаване на подпис/ печат, след генериране на двойка ключове. В този случай устройството се инициализира и се създават кодове за достъп: Потребителски („User“) и Административен („SO“). Тези кодове позволяват персонален достъп и използване до частния ключ, генериран и съхранен в устройството и при необходимост за деблокиране на същото.

Кодовете за достъп за създаване на квалифициран електронен подпис /печат се генерират от Титуляря/Създателя или от упълномощеното от него лице или се предоставят случайно генерирани от Регистриращия орган кодове в запечатен, непрозрачен хартиен плик.

В случай, че случайно генериран персоналния код за достъп се предоставя в запечатан, непрозрачен плик, титулярят е задължен да смени първоначалния потребителски код за достъп посредством софтуера, който се предоставя заедно с устройството.

Доставчикът препоръчва Титулярят/Създателят да сменя периодично своя Потребителски код за достъп до устройството за създаване на квалифициран електронен подпис/ квалифициран електронен печат.

Доставчикът следва да използва Административен код /SO PIN/ за деблокиране на блокирано устройство.

6.4.2 Защита на данни за активиране

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

Потребителите трябва да знаят, че при няколко неуспешни опити за достъп до устройството, то се блокира (заключва се). 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/ електронен 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/ електронен печат.

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

6.4.3 Други аспекти на данните за активиране

Данните за активиране трябва да се съхраняват винаги в един единствен екземпляр. Персоналният идентификационен номер (PIN) за достъп трябва периодично да бъде променян. Данните за активиране могат да бъдат архивирани.

6.5 Сигурност на компютърните системи

StampIT използва единствено надежден и сигурен хардуер.

Компютърните системи, на които работят всички критични компоненти от инфраструктурата на StampIT, са оборудвани и конфигурирани със средства за локална защита на достъпа до софтуера и информационните данни.

StampIT използва процедури за управление на информационната сигурност на цялата си инфраструктура в съответствие с общоприети в международната практика стандарти.

За по-голяма надеждност и сигурност на използваните системи и за гарантиране на техническата и криптографска сигурност на осъществяваните чрез тях процеси, StampIT извършва редица тестове и проверки на техническото оборудване и използваните технологии.

Тестове и проверки на компютърните системи се правят съгласно методика за оценка на сигурността (относно: статус на процесорите - консумиране, натоварване, употреба; статус на съхранение; състояние на паметта-основна, padding in-out; статус на съхранение; брой на протичащите процеси; балансиране на натоварването). Те се извършват както периодично, така и при всяка промяна, която засяга сигурността на инфраструктурата.

За управление на сигурността на компютърните системи в StampIT се взимат в предвид изискванията на ISO/IEC 27001:2013.

В „Информационно обслужване“АД има действащ Съвет на интегрираната система за управление на качеството, информационната сигурност и услугите, който е контролен орган по отношение на информационната сигурност. Съветът участва в анализа на информационните рискове и се свиква за обсъждане на възникнали въпроси или инциденти, свързани с информационната сигурност.

6.5.1 Степен на компютърна сигурност

Степента на сигурност на използваните системи в инфраструктурата на StampIT отговаря на нормативните изисквания за изпълнение на дейността на StampIT и се определя, чрез документа Политика за информационна сигурност на Информационно обслужване АД.

6.6 Сигурност на жизнения цикъл на технологичната система

6.6.1 Контроли за развитие на технологичната система

Софтуерните приложения, използвани в технологичната система на StampIT са разработени и внедрени от високо квалифицирани специалисти. Преди въвеждане на нови приложения те задължително преминават през тестов период. Тестванията се правят на отделни системи, независими от тези в редовната експлоатация, в специално изградена тестова среда.

Всички хардуерни промени са наблюдават и регистрират. При закупуване на ново техническо оборудване, то се доставя с необходимите процедури за експлоатация и инструкции за ползване.

Технологичната сигурност на системата се гарантира, както следва:

- технологично оборудване се доставя по начин, позволяващ неговото проследяване.
- доставка и подмяна на технологично оборудване се извършва единствено с оригинален хардуер. Смяната се извършва от доверен и обучен персонал.

6.6.2 Контроли за управление на сигурността на технологичната система

Целта на контрола за управление на сигурността е да се осъществява постоянен надзор на функционалността на технологичната система и да се гарантира, че тя функционира правилно и в съответствие с доставената производствена конфигурация.

Текущата конфигурация на технологичната система на StampIT, както и всички изменения и актуализации на системата, се записват и извършват контролирано. Контролите позволяват непрекъсната проверка на целостта на технологичната система и своевременна актуализация, както и своевременното отстраняване на неизправности.

6.6.3 Оценка на жизнения цикъл на сигурността на технологичната система

„Практиката при предоставяне на квалифицирани удостоверителни услуги“ не съдържа никакви изисквания в тази област.

6.7 Мрежова сигурност

В инфраструктурата на StampIT се използват съвременни технически средства за обмен и защита на информация, за да се гарантира мрежовата сигурност на системите срещу външни интервенции и заплахи.

Сървърите и критичната технологична система на StampIT са отделени в защитена вътрешна локална мрежа.

Отдалечения достъп до Registration Authority от мрежата на инфраструктурата (PKI) на StampIT се извършва чрез двустепенна защита на достъпа с автентификация и оторизация. За целта се използва специално инсталиран и конфигуриран VPN сървър, който приема автентификация, чрез потребителско име и парола, управлявани от активната директория на „Информационно обслужване“ АД или потребителско име и парола, които са издадени/ съответно генерирани само за тази цел на оторизирани лица /външни регистриращи органи/, участващи в издаването на електронен подпис/печат и администриране на инфраструктурата (Public Key Infrastructure/ PKI).

Последващата оторизация в системата за издаване и управление на удостоверения се извършва чрез персонални сертификати, издадени върху смарт карти (HSM, токъни) от вътрешен удостоверяващ орган и със строго дефинирани роли. Активирането/деактивирането на потребителите в системата се извършва от администратор по сигурността, след одобрена от мениджър информационна сигурност (МИС) заявка за предоставяне/ отнемане на достъп и заповед на изпълнителния директор на „Информационно обслужване“ АД за определяне на овластените лица.

Компютърната система на StampIT е защитена срещу отказ на услугите при наличие на атаки. Контролът за сигурност е разработен на базата на защитна стена (firewall) и филтриране на трафика на рутерите и прокси услугите. Опитите за проникване в системата се наблюдават посредством изградената IDS/ IPS. Всички аларми, включили се при проникване или потенциално проникване, както и атаки от тип „Отказ от достъп“ се изпращат към системните администратори за анализ. Опитите за неправомерен достъп до системата се документират чрез Intrusion prevention System (IPS).

Подробно описание на мрежовата конфигурация на StampIT и средствата за защита на StampIT са представени в техническата документация на инфраструктурата. Документацията е достъпна само за оторизирани лица.

6.8 Удостоверяване на време

StampIT издава удостоверения за време съгласно Регламент (ЕС) № 910/2014 и в пълно съответствие с ETSI EN 319 422, ETSI TS 119 421, IETF RFC 3161 и IETF RFC 5816.

Органът за издаване на квалифицирани електронни времеви печати „StampIT Global TSA“ е обособена и неделима услуга към Удостоверяващия орган на StampIT в структурата на „Информационно обслужване“ АД.

„StampIT Global SA“ (Time-stamping service/услуга по удостоверяване на време) издава Удостоверение за време в съответствие с ETSI EN 319 422. Чрез включването на обектен идентификатор: 1.3.6.1.4.1.11290.1.2.1.1 в издадените удостоверения на услугата по издаване на удостоверения за време, StampIT потвърждава съответствие с „Политика при предоставяне на услуги за удостоверяване на време (eIDAS-CP-TS)“. Обектният идентификатор е в съответствие с ETSI BTSP (best practices policy for time-stamp) OID=0.4.0.2023.1.1, съгласно ETSI EN 319 422.

Издаваните квалифицирани електронни времеви печати (time stamp токъни) са съвместими с RFC 3161. Услугата издава RSA 2048 битови криптирани с алгоритъм SHA256 удостоверения за време.

Органът за издаване на квалифицирани електронни времеви печати „StampIT Global TSA“ приема заявки за издаване на квалифицирани електронни времеви печати на представено съдържание на електронен документ от Титуляря или Доверяваща се страна. Той изготвя квалифициран електронен времеви печат на представената хеш-стойност на електронен документ и осигурява възможност за последващо (след периода на валидност на квалифицираното удостоверение за електронен подпис/печат) доказване спрямо приемащата страна на факта на подписването на изявление или на електронен документ.

Квалифицирани електронни времеви печати могат да се интегрират в процеса на създаване или приемане на квалифициран електронен подпис/печат, на електронно подписани документи и електронни транзакции, при архивиране на електронни данни, в електронни нотариати и други.

За изпълнението на своята услуга „StampIT Global TSA“ използва частен ключ, съхранен в криптомодул HSM с FIPS 140-2 Level 3, използван подписване на заявките и издаване на времеви печати. За услугата могат да бъдат използвани и повече от една ключови двойки с цел увеличаване на производителността на услугата.

Политиката при предоставяне на услуги за удостоверяване на време (eIDAS-CP-TS) на органа за удостоверяване на време „StampIT Global TSA“ се отнася към ETSI EN 319 401 относно общите изисквания, обичайни за всяка една услуга на StampIT. Политиката е насочена към изпълнение на изискванията за удостоверяване на време с дълъг период на валидност (ETSI EN 319 122), но е приложима към всяка употреба с еквивалентни изисквания към качеството.

Алгоритъмът за хеш, дължината на подписващия ключ и криптиращия алгоритъм, използван за подписване на удостоверенията за време е съобразно ETSI TS 119 312.

TSA удостоверението се издава от оперативния удостоверителен орган на StampIT – StampIT Global Qualified CA, отговарящ на ETSI EN 319 411-1.

Услугата по удостоверяване на време използва набор от Stratum -1 NTP (Network Time Protocol/ протокол за синхронизиране на часовниците в компютърните системи) сървъри като независим източник на точно време. Посредством тази конфигурация TSS постига точност на времето в рамките на +/- 500ms (половин секунда) или по-добро спрямо UTC. StampIT Global TSA гарантира интегритета и автентичността на TSU публичен ключ посредством TSU публични ключове, които са достъпни за доверяващите се страни в TSU удостоверенията на сайта на StampIT на адрес: https://www.stampit.org. Удостоверенията за време се записват в регистър, който се публикува в хранилището на StampIT и е достъпен на официалната страница на доставчика. Връзка за достъп до Time stamp услугата: http://tsa.stampit.org

7 Профили на квалифицирани удостоверения, CRL и на OCSP

Профилите на потребителските квалифицирани удостоверения и на Списъка със спрени и прекратени удостоверения (CRL) отговарят на формата, описан в стандарт ITU-T X.509 v.3.

Удостоверение от тип X.509 v.3 представлява набор от данни, чрез който еднозначно се удостоверява принадлежност на публичния ключ към Титуляря/ Създателя на квалифицирания електронен подпис/ квалифицирания електронен печат. Профилът на OCSP отговаря на изискванията на RFC 2560, а профилът на квалифицираното удостоверение за времеви печат отговаря на RFC 3161.

7.1 Профили на квалифицирани удостоверения

В съответствие със стандарта X.509 v.3, електронното удостоверение е последователност от следните полета:

- Version: версия на удостоверението (X.509 v.3);
- SerialNumber: уникален идентификационен код на удостоверението;
- SignatureAlgorithm: идентификатор на алгоритъм за създаването на електронния подпис;
- Issuer: наименование на издателят на удостоверението (DN);
- Validity: срок на валидност, описан от дата и час на издаване на удостоверението (notBefore) до дата и час на изтичане на срока (notBefore) на удостоверението (универсално координирано време, представено във формат Zulu);
- Subject: уникалното име (DN) на Титуляря/Създателя, подлежащ на вписване в удостоверението;
- SubjectPublicKeyInfo: идентификатор на ключа;
- Signature: идентификатор на алгоритъм за създаването на електронния подпис/печат, в съответствие с RFC 5280.

7.1.1 Версия

Всички удостоверения, които издава StampIT, са в съответствие с версия 3 (X.509 v.3).

7.1.2 Допустими разширения във формата на квалифицирано удостоверение

Стойностите на разширенията са създадени в съответствие с препоръката RFC 5280. Функцията на всяко разширение се определя от стандартната стойност на съответния идентификатор на обект (IDENTIFIER):

- Subject Key Identifier - формира се от публичния ключ, удостоверен в удостоверението като хеш-стойност на публичния ключ;
- Authority Key Identifier - формира се като хеш-стойност на публичния ключ на оперативния Удостоверяващ орган на StampIT;
- Issuer Alternative Name - съдържа URL-стринг като алтернативно име на StampIT;
- Basic Constrains - определя типа на удостоверението и има стойност „End entity" в удостоверението на Потребителя;

- Certificate Policy - определя идентификатора на Политиката за квалифицирано удостоверение за квалифициран електранен подпис/печат;
- Key Usage - атрибут, който определя ограниченията в употреба на удостоверението;
- Extended Key Usage - допълва значението на атрибут "Key Usage" и указва допълнителните и специфични приложения на удостоверението;
- CRL Distribution Point - съдържа връзка към актуалния CRL на оперативния Удостоверяващ орган на StampIT;
- Authority Information Access - съдържа URL-адреса на OCSP сървъра на удостоверението;
- Qualified Statements - атрибутът съдържа указание, че удостоверението е квалифицирано и показва дали частния ключ е генериран и се съхранява върху устройства за създаване на електронен подпис (QSCD).

7.1.3 Идентификатори на алгоритмите на електронен подпис/ електронен печат

Атрибутът „Signature algorithm" идентифицира алгоритмите (криптографските механизми), които се използват.

В StampIT се използва приложима комбинация на асиметрични и хеш алгоритми:

- sha256-with-RSA и sha384-with-RSA.

7.1.4 Форми на именуване

Формите на именуване са описани в настоящия документ в т.3.1 „Имена“.

7.1.5 Ограничения на имената

Видовете ограничения на имената са описани в настоящия документ в т.3.1 „Имена“.

7.1.6 Идентификатор на политика

Квалифицирано удостоверение се издават съгласно Политика на StampIT, която се вписва в атрибута „Certificate Policy" на удостоверението.

7.1.7 Идентификатор за продължение

Този идентификатор („Extensions“) дава специфична, свързана с услугата информация. За употребата му на този етап Практиката не поставя никакви ограничения.

7.1.8 Означение на квалифицираното удостоверение

StampIT използва в квалифицирано удостоверение с профил по стандарта X.509 v.3 атрибута „Qualified Statements" с идентификатор: „esi4-qcStatement-1“ (OID=0.4.0.1862.1.1).

StampIT използва в квалифицирано удостоверение за квалифициран електронен подпис с профил по стандарта X.509 v.3 атрибута „Qualified Statements" с идентификатори: „esi4-qcStatement-1“ (OID=0.4.0.1862.1.1) и „esi4-qcStatement-4“ (OID=0.4.0.1862.1.4).

StampIT използва в квалифицирано удостоверение с профил по стандарта X.509 v.3 атрибута "Certificate Policy", на който се присвоява идентификатора (OID) със значение, както следва:

	Наименование	Policy Identifier
Квалифицирано удостоверение за подписване на клиентски удостоверения за време	StampIT Global TSA	1.3.6.1.4.1.11290.1.2.1.1
Квалифицирано удостоверение за квалифициран електронен подпис на физическо лице, асоциирано с юридическо	StampIT DocPro Certificate	1.3.6.1.4.1.11290.1.2.1.2
Квалифицирано удостоверение за квалифициран електронен подпис на физическо лице	StampIT Doc Certificate	1.3.6.1.4.1.11290.1.2.1.3
Квалифицирано удостоверение за квалифициран електронен печат	StampIT Seal Certificate	1.3.6.1.4.1.11290.1.2.1.4
Квалифицирано удостоверение за усъвършенстван електронен подпис на физическо лице	StampIT Enterprise	1.3.6.1.4.1.11290.1.2.1.5
Квалифицирано удостоверение за усъвършенстван електронен подпис на физическо лице, асоциирано с юридическо	StampIT Enterprise Pro	1.3.6.1.4.1.11290.1.2.1.6
Квалифицирано удостоверение за усъвършенстван електронен печат	StampIT Enterprise Seal	1.3.6.1.4.1.11290.1.2.1.7
Квалифицирано удостоверение за автентичност на уебсайт /валидация на домейн/	StampIT Server DVC	1.3.6.1.4.1.11290.1.2.1.8
Квалифицирано удостоверение за автентичност на уебсайт /валидация на организация/	StampIT Server OVC	1.3.6.1.4.1.11290.1.2.1.9
Квалифицирано удостоверение за OCSP респондер	StampIT Global OCSP	1.3.6.1.4.1.11290.1.2.1.10

Други идентификатори (OID), вписани в атрибута "Certificate Policy“ в квалифицираните удостоверения

	Наименование	Policy Identifier
Удостоверителна политика за квалифицирани удостоверения, издадена за публични услуги, която изисква използване на secure signature-creation device (SSCD)	qcp-public-with-sscd	OID=0.4.0.1456.1.1
Удостоверителна политика за квалифицирани удостоверения, издадена за публични услуги	qcp-public	OID=0.4.0.1456.1.2
QCP-n: Удостоверителна политика на Европейския съюз (ЕС) за Квалифицирани удостоверения, издавани на физически лица	qcp-natural	OID=0.4.0.194112.1.0
QCP-l: Удостоверителна политика на Европейския съюз (ЕС) за Квалифицирани удостоверения, издавани на юридически лица/организации	qcp-legal	OID=0.4.0.194112.1.1
QCP-n-qscd: Удостоверителна политика на Европейския съюз (ЕС) за Квалифицирани удостоверения, издавани на физически лица с частен ключ, свързан с удостоверения публичен ключ, разположен в QSCD	qcp-natural-qscd	OID=0.4.0.194112.1.2
QCP-l-qscd: Удостоверителна политика на Европейския съюз (ЕС) за Квалифицирани удостоверения, издавани на юридически лица/организации с частен ключ, свързан с удостоверения публичен ключ, разположен в QSCD.	qcp-legal-qscd	OID=0.4.0.194112.1.3
QCP-w: Удостоверителна политика на Европейския съюз (ЕС) за удостоверения за автентичност на уебсайт	qcp-web	OID=0.4.0.194112.1.4
DVCP (Domain Validated Certificate Policy) според ETSI TS 102 042	dvcp	OID=0.4.0.2042.1.6
OVCP (Organizational Validation Certificate Policy) според ETSI TS 102 042)	ovcp	OID=0.4.0.2042.1.7

7.1.9 Използване на идентификатор за разширение на ключа „критично“

В Практиката няма изисквания за използване на „CRITICAL CERTIFICATE EXTENSIONS“.

7.2 Профил на списъка със спрени и прекратени удостоверения (CRL)

CRL профил на StampIT:

StampIT Global CRL, StampIT Global Qualified CRL, StampIT Global AES CRL		
Version	Version 2	
Issuer Name	CN	
	C	
	L	
	O	
	2.5.4.97 /organizationIdentifier/	
Effective date	[Date of CRL issuance]	
Next Update	[Next update]	
Signature algorithm	Sha256/RSA	
CRL Number	[CRL number]	
Authority key identifier	[Issuing Authority Key ID]	
Revocation List	CRL Entries	
	Certificate Serial Number	[Certificate Serial Number]
	Date and Time of Revocation	[Date and Time of Revocation]
	Reason code	[Revocation reason code] (optional)

7.2.1 Версия

StampIT, чрез своя Удостоверяващ орган издава, публикува и поддържа Списъци със спрени и прекратени удостоверения (CRL) във формата X.509 v.2. Версията се вписва в издадения CRL.

7.2.2 Формат

StampIT издава, публикува и поддържа Списък със спрени и прекратени удостоверения (CRL), чийто формат е в съответствие с изискванията в международната препоръка RFC 5280.

StampIT не издава и не поддържа схема на „частичен" (delta) Списък със спрени и прекратени удостоверения (CRL), но си запазва право при необходимост да въведе такава схема.

7.2.3 Основни атрибути на списъка със спрени и прекратени удостоверения (CRL)

- Version - версия на Списъка;
- Issuer Name – наименование на издателя на Списъка (Удостоверяваш орган);
- Effective Date/This update – дата и час на издаване на Списъка (CRL);
- Next Update - времето на валидност на CRL. След посоченото време, Удостоверяващия орган издава незабавно нов Списък. През периода на валидност, в случай на прекратяване/спиране на удостоверение, Удостоверяващия орган издава автоматично нов CRL;

- Signature algorithm – идентификатор на алгоритъма за създаване на електронен подпис на CRL;
- Signature hash algorithm – алгоритъм за създаване на електронен подпис.

7.2.4 Допълнителни атрибути в списъка със спрени и прекратени удостоверения (CRL)

„Authority Key Identifier"- идентификатор на Удостоверяващия орган, който издава и подписва Списъка със спрени и прекратени удостоверения (CRL), съдържа значението на „subjectKeyIdentifier" от удостоверението на Удостоверяващия орган.

7.2.5 Формат на елемент в списъка със спрени и прекратени удостоверения (CRL)

Списъкът със спрени и прекратени удостоверения (CRL) на Удостоверяващия орган съдържа елементи за всички спрени удостоверения. Тези елементи са постоянни в Списъка.

Списъкът със спрени и прекратени удостоверения (CRL) на Удостоверяващия орган съдържа елемент за всяко спряно удостоверение от Удостоверяващия орган. Такъв елемент е временен в списъка до момента на възобновяване на удостоверението.

7.2.5.1 Атрибути на елемент в Списъка със спрени и прекратени удостоверения (CRL)

- Serial number - сериен номер на спряно удостоверение;
- Revocation date - време на прекратяване/спиране на удостоверение;
- CRL Reason Code - код идентифициращ причината за прекратяване/спиране.

7.2.5.2 Означения на причината за прекратяване/ спиране на удостоверение

- **Key Compromise** – компрометиран е частния ключ, съответстващ на публичния ключ, включен в съдържанието на квалифицираното удостоверение, следователно няма основания за доверяване на това удостоверение.
- **CA Compromise** – компрометиран е частния ключ на Удостоверяващия орган, който се използва за подписване на квалифицираните удостоверения на абонатите.
- **Affiliation Changed** – промени в юридическото лице – субектът, вписан в квалифицираното удостоверение вече е с променен статут по отношение на юридическото лице.
- **Superseded** – квалифицираното удостоверение е заместено от друго квалифицирано удостоверение.
- **Cessation of Operation** – прекратени са дейностите, свързани с първоначалното издаване на квалифицираното удостоверение.
- **Certificate Hold** – действието на квалифицираното удостоверение е спряно (удостоверението е невалидено в момента).
- **Unspecified** – квалифицираното удостоверение е прекратено без посочване на причина, когато е налично валидно искане за прекратяване.

7.3 Профил на отговор за онлайн проверка на статуса на удостоверение (OCSP/Online Certificate Status Protocol)

Удостоверяващият орган за валидация „StampIT Global OCSP" на оперативния удостоверяващ орган „StampIT Global Qualified CA“ на StampIT работят и предоставят квалифицираната услуга „онлайн проверка на статус на удостоверение в реално време" в съответствие с международно утвърдената препоръка IETF RFC 6960.

OCSP-потребителят изпраща искане за проверка на статус на подпис/ печат до OCSP-сървъра и получава отговор – удостоверение за статус, подписан от Органа за валидация. Отговорът съдържа информация за статуса на проверяваното удостоверение за електронен подпис/печат, периода на валидност на получения отговор и има доказателствен характер. OCSP сървърът, който издава потвърждения за състоянието на квалифицираните удостоверения притежава специално генерирана ключова двойка, издадени единствено за тази цел.

7.3.1 Версия

StampIT чрез своите Удостоверяващи органи за валидация, издава удостоверения за статус на издадените квалифицирани удостоверения във формат, определен в международната препоръка RFC 6960. Версията се вписва в издадените удостоверения за статус.

7.3.2 Формат

StampIT издава удостоверения за статус, чийто формат е в съответствие с изискванията в международната препоръка RFC 6960.

7.3.3 Основни атрибути на удостоверенията за статус

- Version - версия на удостоверението за статус;
- Response Type – тип на отговора за статус;
- OCSP Response Status – статус на отговора;
- Responder Id - Идентификатор на услугата по валидация
- Produced At - дата и час на издаване на удостоверението за статус;
- Responses – информация, уникално идентифицираща квалифицираното удостоверение, за което е отправено запитване и за което органа за валидация издава настоящесто удостоверение за статус;
- Cert Status – статус на квалифицираното удостоверение, за което е отправено запитване;
- This Update - времето на издаден CRL, на базата на който е издадено удостоверението за статус;
- Next Update - времето на валидност на CRL, на базата на който е издадено удостоверението за статус;
- Response Extensions – допълнителни разширения, включени в отговора;
- OCSP Nonce - съдържа същата информация, която е подадена при заявката в полето за Nonce;
- Signature Algorithm - използван алгоритъм за електронно подписване на удостоверението за статус;
- Certificate – Съдържа квалифицираното удостоверение на органа за валидация на StampIT.

Съдържанието на удостоверението за статус на StampIT е:

StampIT Global OCSP			
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 Years		
Subject	CN	StampIT Global OCSP	Име
	C	BG	Държава
	O	Information Services JSC	Организация
	L	Sofia	Област
Public Key	RSA 2048 bits		
Key Usage (Critical)	Digital Signature		
Friendly Name	StampIT Global OCSP		
Extended key usage (Critical)	OCSP Signing (1.3.6.1.5.5.7.3.9)		
Basic constrains (Critical)	End entity		
CRL Distribution Point/Non Critical/	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.stampit.org/crl/stampit_global_qualified.crl		
Certificate Policies (Non Critical)	[1]Certificate Policy: Policy Identifier= **1.3.6.1.4.1.11290.1.2.1.10** [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier:		

	http://www.stampit.org/repository/

7.4 Други профили

7.4.1 Профил на квалифициран електронен времеви печат

Удостоверяващият орган за квалифицирани електронни времеви печати „StampIT Global TSA“ издава квалифицирани електронни времеви печати (Timestamp Tokens/TST) с един или повече частни ключове, запазени единствено за тази цел. Според препоръка RFC 3280 удостоверенията за квалифицирани електронни времеви печати в техните разширения на атрибути, съдържат поле за ограничаване на употребата им (Extended Key Usage), маркирани като критични. Това означава, че удостоверението може да се използва от „StampIT Global TSA“ единствено за целите на подписването на квалифицираните електронни времеви печати, издадени от този орган.

7.5 Основни полета в профила на квалифицирани електронни времеви печати:

- Version – версия (Version 3);
- Serial Number – уникален идентификационен код на времевия печат;
- Signature Algorithm – алгоритъм за създаване на електронния подпис (sha256WithRSAEncryption)
- Issuer (Distinguished Name) – наименование на издателя на времевия печат (StampIT TSA);
- Not before (validity period/beginning date) – дата и час на издаване (универсално координирано време, представено в Zulu);
- Not after (validity period ending/date) – дата и час на изтичане на срока на валидност;
- Subject (Distinguished Name) – наименование на Титуляря/Създателя;
- Subject Public Key Info - Кодирана поле в съответствие с RFC 3280, което съдържа информация за RSA публичния ключ (ключов идентификатор и стойност на публичния ключ);
- Signature - електронен подпис, генериран и кодиран в съответствие с изисквания, описани в RFC 3280;
- Basic Constraints – основни ограничения на времевия печат;
- Key Usage – предназначение на времевия печат;
- Extended Key Usage - Time Stamping Authority (TSA);
- Certificate Policies – политика, въз основа на която е издаден времевия печат;
- Authority Key Identifier – идентификатор на ключа на Удостоверяващия орган (SHA1 hash of the public key).

Удостоверяващият орган „StampIT Global TSA“ приема заявки за удостоверяване на време, които да отговарят на спецификациите IETF RFC 3161 и ETSI EN 319 422:

- Заявката за квалифициран електронен времеви печат трябва да съдържа алгоритъма на хеш функция SHA256;
- Заявката за квалифициран електронен времеви печат указва идентификатора на политиката на StampIT Global TSA Policy OID.

Квалифицираният електронен времеви печат, издаден от „StampIT Global TSA“ съдържа информация за печата (TSTinfo структура), разположен в SignedData структура (виж RFC 2630), подписан от StampIT Global TSA и вградени в ContentInfo структура (виж RFC 2630).

8 Одит

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 се изпълняват съгласно очакваното. Вътрешните одити обхващат всички регистриращи органи в структурата на Организацията. Ръководството на „Информационно обслужване“ АД възлага провеждането на периодични вътрешни одити за съответствие на дейността с утвърдените Практики и Полити-ка при предоставяне на удостоверителни услуги.

Ръководството на „Информационно обслужване“ АД осъществява постоянен оперативен контрол на служителите, за стриктното изпълнение на инструкциите за работа.

8.1 Планиране на одити

8.1.1 Вътрешни одити

Вътрешните одити се планират, провеждат и документират съгласно процедура ПУ 08-01 Вътрешни одити, чиято цел е да определи реда и начина за провеждане на вътрешни одити на Интегрираната система за управление на качеството, информационната сигурност и услугите в „Информационно обслужване“ АД.

Вътрешните одити се провеждат от одиторски екипи, по предварително изготвена годишна Програма за провеждане на вътрешни одити на ИСУ ДК 08-01-01. Програмата се изготвя от Представителя на ръководството за ИСУ със съдействието на Мениджъра по информационна сигурност и Мениджъра по управление на услугите и се утвърждава от Изпълнителния директор. Годишната програма за провеждане на вътрешните одити се изготвя съобразно състоянието и важността на одитираните зони и процесите, които се извършват в тях и като се вземат предвид резултатите от предишни одити.

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.

Ръководството на „Информационно обслужване“ АД осъществява постоянен оперативен контрол на служителите, за стриктното изпълнение на инструкциите за работа.

8.1.2 Одити за оценка на съответствието

„Информационно обслужване“ АД е обект на одит от независим Орган за оценяване на съответствието, веднъж годишно.

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.

8.2 Квалификация на проверяващите лица

Ръководител на вътрешен одит на ИСУ може да бъде служител на организацията с квалификация за одитор, съгласно ISO 27001, ISO 9001 и ISO 20000-1.

Вътрешните одити в „Информационно обслужване“ АД се извършват от служители на Организацията с квалификация и опит за одитор, съгласно ISO 27001, ISO 9001, ISO 20000-1.

За целите на вътрешните одити, „Информационно обслужване“ АД разполага със служители, които притежават необходимата експертиза и познания, свързани с инфраструктурата на публичния ключ, надеждна и сигурна работа на технологичната система, информационна сигурност, с богат практически опит.

Независимите Органи за оценка на съответствието подлежат на акредитация от съответния държавен орган за акредитация (ИА „Българска служба за акредитация“). Системата за акредитация и компетентност на одиторите са определени в Регламент (ЕО) № 765/2008 на европейския парламент и на съвета от 9 юли 2008 г. за определяне на изискванията за акредитация и надзор на пазара във връзка с предлагането на пазара на продукти и за отмяна на Регламент (ЕИО) № 339/93 и се регулира от международния стандарт ISO/IEC 17065:2012 „Оценяване на съответствието. Изисквания към органите за сертификация на продукти, процеси и услуги“.

Надзорният орган има правомощията да извършва проверка на доставчика на удостоверителни услуги, по всяко време чрез оправомощени експерти.

8.3 Отношения на проверяващите външни лица с „Информационно обслужване“АД

Позовавайки се на принципите за одит, проверяващите външни лица трябва да бъдат независими и обективни, да не са пряко или косвено свързани с „Информационно обслужване“ АД и да нямат конфликт на интереси с дружеството.

Взаимоотношенията на „Информационно обслужване“ АД и проверяващите външни лица се уреждат с договор.

8.4 Обхват на одита

Вътрешните одити в „Информационно обслужване“ АД обхващат проверка на дейността на доставчика и съответствие с Политиката и Практиката при предоставяне на удостоверителни услуги, съпоставка на практики и процедури посочени в този документ с тяхната практическа реализация при изпълнение на дейността на Организацията, проверка на дейността на Регистриращия орган, други обстоятелства, факти и дейности, свързани с инфраструктурата на „Информационно обслужване“ АД, по преценка на ръководството.

В обхвата на вътрешните одити също така се проверява поддържането и прилагането на изискванията на Интегрираната система за управление на качеството, информационната сигурност и услугите в дейността на структурните единици, в съответствие с EN ISO 9001:2008, ISO/IEC 27001:2013, ISO/IEC 20000-1:2011.

Проверката от страна на Надзорния орган обхваща нормативно регламентираните изисквания към дейността на „Информационно обслужване“ АД, съгласно приложимото законодателство в сектора на удостоверителните услуги.

Външен одит от страна на Орган за оценка на съответствието, обхваща цялостната дейност на „Информационно обслужване“ АД по предоставяне на удостоверителни услуги, прилагане и изпълнение на стандартите свързани с Регламент (ЕС) № 910/2014 - документация; архиви; информационни данни, свързани с издаване и управление на квалифицирани удостоверения; физическа и информационна сигурност и надеждност на технологичната система и управление; Удостоверителни органи, както и с изискванията на международните стандарти ISO 27001, ISO 9001, ISO 20000-1.

8.5 Действия, предприети в резултат на проведен одит

Резултатите от проведените вътрешни и външни одити се документират в Доклади.

Одитните доклади се представят на ръководството на „Информационно обслужване“ АД.

Доклад от одит, изготвен от Орган за оценка на съответствието се представя на Надзорния орган.

Въз основа на направените констатации и оценки в доклад от одит, ръководство на „Информационно обслужване“ АД набелязва конкретни мерки, срокове и отговорници за отстраняване на причините за установените несъответствия и предприемане на действия за отстраняване на потенциални несъответствия или други нежелани събития.

8.6 Съхранение на резултатите

Докладите от извършените вътрешни и външни одити се съхраняват в „Информационно обслужване“ АД по установения ред.

Сертификатите на „Информационно обслужване“ АД, получени от Орган за оценка на съответствието се публикуват на интернет страницата на дружеството.

9 Други бизнес и правни въпроси

9.1 Цени

Цените на квалифицираните удостоверителни услуги, цените на хардуерните устройства, които се предлагат във връзка с тези услуги, както и цените на консултанските услуги са посочени в Ценова листа за стоките и услугите, предоставяни от „Информационно обслужване“ АД като Доставчик на квалифицирани удостоверителни услуги, която е утвърдена от изпълнителния директор на „Информационно обслужване“АД и е публично достъпна на https://www.stampit.org.

„Информационно обслужване“АД има право по всяко време да променя цените, като публикува актуалната Ценова листа на https://www.stampit.org. Новите цени влизат в сила от датата на публикуване, освен ако в Ценовата листа не е посочена друга, по-късна дата.

9.1.1 Цена по договора за квалифицирани удостоверителни услуги. Фактуриране и плащане.

Цената по договора за квалифицирани удостоверителни услуги включва цените на стоките и услугите, които са включени в предмета на договора:

- цената за издаване/ подновяване и ползване на квалифицираното удостоверение;
- цените на хардуерните устройства, които се предоставят във връзка с удостоверителните услуги (когато е приложимо);
- цените на други услуги, които се предоставят във връзка с удостоверителните услуги (когато е приложимо).

Плащането на цената по договора за квалифицирани услуги се извършва от Абоната по един от следните начини:

1. в брой или чрез ПОС-терминал (при наличие в офиса на Доставчика) - при сключване на договора. Тези начини за плащане са възможни за всички Абонати;

2. по банков път – в 3 (три) – дневен срок след сключване на договора и издаване на оригинална фактура. Плащането се извършва по посочената във фактурата банкова сметка на Доставчика. Този начин за плащане е възможен само за Абонати – юридически лица или ЕТ. В случай, че Абонатът не извърши плащане в уговорения срок, действието на договора и удостоверението/ удостоверенията се прекратява.

В случай на предсрочно прекратяване на квалифицираното удостоверение и/или на договора за квалифицирани удостоверителни услуги по причини, за които Доставчикът не отговаря, на Абоната не се дължи връщане на цената за остатъка от срока на прекратеното квалифицирано удостоверение.

В цената по договора за квалифицирани удостоверителни услуги не са включени разходите на Абоната за банкови преводи и за осигуряване на комуникации на Абоната във връзка с ползване на квалифицираните удостоверителни услуги. Тези разходи се дължат от Абоната на доставчика на съответната услуга.

При предоставяне на консултантски услуги общата дължима цена се определя на база отработеното време, въз основа на подписан приемо - предавателен протокол за предоставените услуги и се заплаща в 3 (три) – дневен срок след подписване на протокола и издаване на оригинална фактура.

Доставчикът издава фактура за услугите съгласно националното право.

При забавяне на плащането след изтичане на срока, посочен в договора за квалифицирани удостоверителни услуги, Абонатът дължи на Доставчика и обезщетение в размер на законната лихва до окончателното погасяване на задължението.

9.1.2 Безплатни услуги за Абонатите/ Доверяващите се страни

„Информационно обслужване“АД предоставя безплатно достъп до следните услуги, свързани с издаването и ползването на квалифицирани удостоверения:

- проверка на удостоверение, публикувано в Регистъра на издадените квалифицирани удостоверения;
- проверка за валидност на издадено удостоверение;
- проверка на статус на удостоверение в реално време;
- издаване на удостоверение за време за предоставено съдържание/ електронно изявление чрез потребителски интерфейс от Абонат на StampIT, притежаващ валидно квалифицирано удостоверение;
- изтегляне на актуален Списък със спрени и прекратени удостоверения (CRL);
- достъп до архива на Списък със спрени и прекратени удостоверения (CRL);
- изтегляне на оперативните удостоверения на StampIT;
- изтегляне на публични документи на StampIT;
- други услуги.

9.1.3 Връщане на удостоверение и възстановяване на цената

Когато издаденото квалифицирано удостоверение съдържа непълноти или грешки, титулярят/ създателят, съответно абонатът може да възрази в 3-дневен срок от публикуването му в регистъра на издадените удостоверения.

Когато непълнотите или грешките са допуснати поради пропуски или грешки, допуснати от оператор на Регистриращия орган, те се отстраняват незабавно от доставчика чрез издаване на ново квалифицирано удостоверение без заплащане на възнаграждение.

Когато непълнотите или грешките са допуснати поради предоставяне на неверни данни от абоната, квалифицираното удостоверение се прекратява и Доставчикът не дължи връщане на цената.

Когато Абонатът откаже да приеме издаденото квалифицирано удостоверение с вярно съдържание, квалифицираното удостоверение се прекратява и Доставчикът не дължи връщане на цената.

9.2 Финансова отговорност

StampIT носи отговорност за предоставяните квалифицирани удостоверителни услуги пред титуляря на електронен подпис/ създателя на печат/, пред абоната и пред всички трети лица, които се доверяват на издадените от StampIT квалифицирани удостоверения.

StampIT ще отговаря за всички вреди, причинени по негова вина или по вина на външен Регистриращ орган.

В случаите на настъпване на вреди, за които StampIT носи отговорност, той ще заплати обезщетение на Абоната до размера на настъпилите вреди.

StampIT носи отговорност само за вредите, настъпили в резултат на използване на квалифицирано удостоверение в периода на неговата валидност (между началната и крайната дата на валидност) и само ако не са налице обстоятелства, изключващи отговорността на StampIT.

9.2.1 Гаранции за плащане на обезщетения

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. При сключване на застрахователен договор StampIT се задължава да публикува информация за застрахователя и срока на застраховката на интернет страницата на StampIT.

9.2.2 Процедура за плащане на обезщетения

Срокът за предявяване на претенция от абонатите или доверяващите се страни към StampIT или застрахователя е 7 (седем) дни от датата на узнаване за настъпването на вредата. StampIT покрива също и претенции, които са предявени в период от 15 (петнадесет) дни след крайната дата на валидност на квалифицираното удостоверение и се основават на вреди, настъпили по време на валидността на удостоверението.

Абонатите са длъжни:

- да изпращат незабавно писмено уведомление за откритата грешка и вредите с препоръчано писмо или куриерски услуги;
- да съдействат на StampIT и Застрахователя на StampIT, за да се установят фактите, потвърждаващи претенцията за обезщетяване.

9.2.3 Максимален лимит на обезщетение

С цел ограничаване на действието на квалифицираните удостоверения, StampIT определя максимален лимит на обезщетение за претърпени вреди, причинени от използването на квалифицирано удостоверение, издадено от него, в размер на максималния лимит, определен съгласно националното право.

StampIT има право да откаже да изплати сума, надвишаваща максималия лимит на обезщетение за вредите.

В отношенията на StampIT с абонатите и всички трети страни се прилагат тези лимити на обезщетение и условия, които са в сила към датата на настъпване на вредата.

9.3 Конфиденциалност на бизнес информацията

StampIT съблюдава всички приложими правила за защита на информацията, събирана с оглед на дейността.

9.3.1 Конфиденциална информация

StampIT приема за конфиденциална информацията, съдържаща се в:

- договор за квалифицирана удостоверителна услуга;
- архиви на заявките за квалифицирани удостоверения и за квалифицирани електронни времеви печати;
- архиви на транзакции;
- записи на външни и вътрешни одити и доклади (с изключение на докладите, които са публични);
- планове за непредвидени случаи и възстановяване след бедствия;
- вътрешни проследявания и записи на операциите на инфраструктурата на StampIT, управлението на квалифицираните удостоверения, услугите по вписване и данни.

StampIT не разкрива, нито може да се изисква от него да разкрива конфиденциална информация, без да е налична автентифицирана обоснована заявка от Титуляря/ Създателя/ Абоната или друга оторизирана страна, в която е посочено следното:

- страната, на която StampIT вменява отговорността за опазване на конфиденциалността на информацията;
- страната, изискваща тази информация;
- разпореждане или решение на оторизирани органи, ако има такова.

9.3.2 Неконфиденциална информация

Не е конфиденциална информацията, включена в съдържанието на квалифицираните удостоверения и в Списъка със спрените и прекратените удостоверения (CRL).

Публично достъпна е следната информация, публикувана в Хранилището:

- Актуални и предходни версии на всички документи, които подлежат на публикуване, включително: Практика при предоставяне на квалифицирани удостоверителни услуги от „Информационно обслужване“АД, Политики при предоставяне на квалифици-рани удостоверителни услуги, Политика при предоставяне на услуги за удостоверяване на време, правила, процедури и документи, които са предназначени за Абонатите и Доверяващите страни;
- Доклади от одити, извършени от органи за оценка на съответствието и надзорни органи;
- Допълнителна информация, която доставчикът е длъжен да публикува.

9.3.3 Защита на конфиденциалната информация

„Информационно обслужване“ АД съхранява конфиденциалната информация при стриктно спазване на политиките и процедурите на Интегрираната система за управление на „Информационно обслужване“ АД.

Абонатът по договора за квалифицирани удостоверителни услуги е длъжен да не разпространява и да не допуска да бъде разпространявана без съгласието на StampIT конфиденциалната информация, която му е била предоставена във връзка със сключването и изпълнението на договора.

9.4 Неприкосновеност на личните данни

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

Личните данни се събират, съхраняват и обработват в съответствие с правилата за поверителност, съдържащи се в Инструкция за мерките за защита на личните данни, утвърдена от изпълнителния директор на „Информационно обслужване“АД.

9.4.1 Декларация за поверителност

„Информационно обслужване“ АД съхранява и обработва личните данни, които са му предоставени в качеството му на Квалифициран доставчик на квалифицирани удостоверителни услуги, в съответствие със Закона за защита на личните данни.

Видът и количеството на събираните лични данни е пропорционално на целите и употребата им. Личните данни се използват само във връзка с предоставяне на квалифицирани удостоверителни услуги.

9.4.2 Лична информация

„Информационно обслужване“ АД приема, че всяка информация за Абонатите, която не е публично достъпна съгласно т.9.3.2. е лична.

Не се счита за лична информацията, която се съдържа в квалифицираните удостоверения, публикувани от StampIT.

9.4.3 Отговорност за защита на личните данни

„Информационно обслужване“АД носи отговорност за защита на личните данни на личните данни на Титуляря/ Създателя/ Абоната и на упълномощените лица и не допуска разкриването им пред трети лица. Предоставянето на достъп до лични данни се извършва само в съответствие с разпоредбите на Закона за защита на личните данни.

9.4.4 Съгласие за използване на лични данни

Освен ако не е посочено друго в съответната Политика, личните данни на Титуляря/ Създателя/ Абоната и на упълномощените лица не могат да се използват без тяхно съгласие, освен по изключение, предвидено в закон.

9.5 Права върху интелектуална собственост

Данните, включени в квалифицираните удостоверения, издадени от StampIT или публикувани в Хранилището/ Публичния регистър са обект на права на интелектуална собственост и други имуществени и неимуществени права. Отношенията, във връзка с използването на тези права се уреждат съгласно националното право.

Всички права върху използваните от „Информационно обслужване“АД търговски марки са и остават собственост на дружеството.

„Информационно обслужване“АД притежава правата върху интелектуалната собственост, касаещи базата данни, уеб сайтовете, КУЕП на StampIT и всякакви други публикации, които са били извършени от StampIT, включително и тази ПДПКУУ

Всички права върху използваните от абонатите наименования и търговски марки, включени в съдържанието на квалифицираните удостоверения, остават за притежателя им, като включването им в съдържанието на квалифицираните удостоверения и използването им за предоставяне на удостоверителни услуги не представлява нарушение.

9.5.1 Право на собственост на данни в квалифицирани удостоверения

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.

9.5.2 Право на собственост на имена и търговски марки

„Информационно обслужване“АД е собственик на търговската марка „StampIT“, регистрирана съгласно националното право. Търговската марка не може да бъде използвана от други лица без изричното писмено съгласие на „Информационно обслужване“АД.

Абонатите на StampIT са длъжни, когато предоставят на StampIT и използват domain и distinguished name (и всяка друга информация при подаване на заявка) да не нарушават права на трети страни по отношение на техни търговски марки, търговски наименования или други права върху интелектуална собственост.

Абонатите на StampIT запазват правата върху имената и търговските марки, които са тяхна собственост и са включени в съдържанието на квалифицираните удостоверения.

9.5.3 Право на собственост на двойка ключове

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.

9.6 Задължения и гаранции

Задълженията, отговорностите и гаранциите на Доставчика, Абонатите и доверяващите се страни са уредени в Регламент (ЕС) № 910/2014, в националното право, в тази Практика, в Политиките на Доставчика, в договорите за квалифицирани удостоверителни услуги, както и в други документи на Доставчика, само и доколкото са публично обявени и достъпни.

Договорите за предоставяне на квалифицирани удостоверителни услуги следва да бъдат сключвани в писмена форма, при спазване на Регламент (ЕС) № 910/2014, в националното право.

9.6.1 Задължения, отговорности и гаранции на StampIT

До нивото, определено в съответния раздел на ПДПКУУ, StampIT се задължава да:

- спазва тази ПДПКУУ и своите вътрешни или публични 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 тази ПДПКУУ и изпълнява задълженията си посочени в нея;
- при получаване на искане от Регистриращия орган, издава и подновява квалифицирани удостоверения, в съответствие с тази ПДПКУУ;
- при получаване на искане за прекратяване на квалифицирано удостоверение от Регистриращия орган прекратява удостоверението, в съответствие с тази ПДПКУУ;
- публикува квалифицираното удостоверение, в съответствие с тази ПДПКУУ;
- осигурява поддръжка на абонатите и доверяващите се страни, както е описано в тази ПДПКУУ;
- прекратява, спира и възобновява квалифицираните удостоверения в съответствие с тази ПДПКУУ;
- осигурява информация за изтичането на срока на валидност и подновяването на квалифицираното удостоверение в съответствие с тази ПДПКУУ;
- предоставя копия от тази ПДПКУУ и действащите си документи за публичен достъп.

StampIT заявява, че няма други задължения по тази ПДПКУУ.

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 ДУУ;
- Неизпълнение на задълженията на ДУУ, съгласно Регламент (ЕС) № 910/2014 и националното право, регламентиращи издаването, управлението и съдържанието на квалифицираното удостоверение;
- 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;
- неналичност към момента на издаването на квалифицираното удостоворение на частния ключ, кореспондиращ с публичния ключ при лицето, посочено като Титуляр/ Създател;
- пропуски в установяване на идентичността на Титуляря/ Създателя/ Абоната.

9.6.2 Задължения, отговорности и гаранции на Регистриращите органи

Регистриращите органи на StampIT имат следните задължения:

- приемат искания за издаване и подновяване на квалифицирани удостоверения на StampIT в съответствие с тази ПДПКУУ;
- извършват всички действия, които са предписани от процедурите на StampIT и тази ПДПКУУ;
- приемат, проверяват и предоставят на StampIT исканията за прекратяване, спиране и възобновяване на действието на квалифицираното удостоверение, издадено от StampIT в съответствие с процедурите на StampIT и тази ПДПКУУ;
- спазват тази ПДПКУУ и вътрешните или публични политики и процедури на StampIT;
- спазват Регламент (ЕС) № 910/2014 и националното право;
- използва надеждни и сигурни устройства и софтуер;
- стриктно изпълнява процедурите за правилна идентификация на заявителите;
- въвежда правилно и точно данните в базата данни на StampIT и актуализира тази информация в момента на потвърждаване на данните;
- въвежда коректно информацията, съдържаща се в удостоверенията;
- осигуряват защита на личните данни в съответствие със Закона за защита на личните данни;
- осигуряват съхранение на частните ключове на операторите в съответствие с изискванията за сигурност, определени в настоящия документ;
- осигуряват частните ключове на операторите да се използват само за целите, посочени в настоящата ПДПКУУ

В случаите, когато задълженията на Регистриращи органи са възложени на външни лица (юридически или физически лица), същите, освен задълженията изброени по-горе имат и следните допълнителни задължения:

- да спазват правилата и процедурите на StampIT за проверка на самоличността, съответно идентичността и представителната власт на заявителите на квалифицирани удостоверения и съответствието на данните и обстоятелствата, касаещи потребителите на услугите;
- да следват стриктно последователността и да изискват и проверяват всички необходими документи, съгласно стандартно определените процедури, подробно отразени в тази ПДПКУУ;
- да осигурят достъп до всички места и дейности, в това число архиви на документи и техническо оборудване, свързани с дейността им като Регистриращ органи/мрежа от регистриращи органи, при извършване на цялостни одити или внезапни и тематични проверки, както и при извършване на одити и проверки от контролните органи, определени съгласно националното право, като не пречат или възпрепятстват по никакъв начин проверяващите лица;
- да осигурят необходимото техническо оборудване във връзка с изпълнението на дейността им като Регистриращи органи на StampIT;
- В края на всяко тримесечие да изпращат на Доставчика под опис всички документи, представени по подадените искания за издаване на квалифицирани удостоверения;
- да спазват стриктно вътрешните правила и процедури на StampIT във връзка със събирането, съхраняването и архивирането на документите по подадените искания и издадените квалифицирани удостоверения;
- да не разпространяват на трети страни и да не се възползват неправомерно от търговски тайни, ноу-хау или друга конфиденциална информация, станала им известна при осъществяване на дейността им като Регистриращи органи.

9.6.3 Задължения на абонатите

Освен ако в тази ПДПКУУ 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 ПДПКУУ на StampIT и свързаните с него документи, публикувани в хранилището на StampIT;
- да използват квалифицираните удостоверения, издадени от StampIT само за законни цели и в съответствие с тази ПДПКУУ на StampIT;
- 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 или устройствата, 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, 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.

9.6.4 Задължения на Доверяващите страни

Страната, която се доверява на квалифицирано удостоверение, издадено от StampIT следва да се придържа към следните общопризнати в международната практика правила:

- да има познания за използване на квалифицирани удостоверения;
- да се запознае с ограниченията за използване на квалифицирани удостоверения, предвидени в Политиката, спрямо която е издадено съответното удостоверение;
- да се запознае с условията на ПДПКУУ на StampIT;
- да проверява квалифицираното удостоверение, издадено от StampIT, като използва освен другите допустими средства и CRL (включително StampIT CRL);
- да се доверява на квалифицираното удостоверение само до степен, разумна за дадените обстоятелства;
- да използва механизъм за сигурна проверка на електронен подпис/ електронен печат, който гарантира: проверка на публичния ключ, проверка на частния ключ, проверка на съдържанието на подписания електронен документ; проверка на автентичността и валидността на квалифицираното удостоверение към момента на подписване, правилно представяне на резултатите от проверката и възможност да бъдат установени всякакви промени, които имат отношение към сигурността.
- „Информационно обслужване“АД не носи отговорност за вреди, настъпили за Доверяващата страна поради неполагане на дължимата грижа.

9.6.5 Задължения на други страни

9.6.5.1 Задължения на квалифицирания орган за удостоверяване на време

Квалифицираният орган за установяване на време StampIT Global TSA издава квалифицирани електронни времеви печати в съответствие с Регламент (ЕС) № 910/ 2014, приложимите стандарти и националното право и при спазване на съответната Политика.

При предоставяне на услугата, StampIT:

- използва технология за обвързване датата и часа с данните по начин, който до голяма степен изключва възможността за незабелязана промяна на данните;
- основава се на източник на точно време, свързан с координираното универсално време;
- използва надеждни устройства и софтуер в съответствие с изискванията на прриложимите технически стандарти и препоръки;
- подписва с квалифициран електронен подпис на StampIT;
- осигурява възможност за доказване в последващ период във времето (след изтичане периода на действие на КЕВП) на факта на подписване/ подпечатване на електронен документ/ друг обект;
- предоставя непрекъснат достъп (24/7/365) до услугата (с изключение на времето на техническа профилактика);
- издава квалифицирани електронни времеви печати в съответствие с ETSI EN 319 422 Time-stamping protocol and electronic time-stamp profiles.

9.6.5.2 Задължения на квалифицирания оперативен Удостоверяващ орган за квалифицирани електронни подписи/ квалифицирани електронни печати

Квалифицирания оперативен Удостоверяващ орган за квалифицирани електрон-ни подписи/ квалифицирани електронни печати StampIT Global Qualified CA осъществява функциите си съгласно Регламент (ЕС) № 910/ 2014, приложимите стандарти и националното право и при спазване на съответната Политика и техническите изисквания за устройствата за създаване и проверка на квалифицирани електронни подписи/ печати.

Прилаганите от StampIT процедури изключват всякаква възможност за манипулиране на удостоверенията или данните.

9.6.5.3 Задължения на StampIT по отношение на поддържане на публични регистри/ хранилище

StampIT управлява и контролира публичните регистри, както следва:

- публикува и архивира квалифицираните удостоверения на Квалифициран базов удостоверяващ орган - StampIT Global Root CA; Квалифициран оперативен удостоверяващ орган - StampIT Global Qualified CA; Квалифициран удостоверяващ орган на време- StampIT Global TSA и Квалифициран удостоверяващ орган за проверка на статуса на удостоверенията - StampIT Global OCSP;

- публикува и архивира Политиките и Практиките при предоставяне на квалифицирани удостоверителни услуги, образци на договори за квалифицирани удостоверителни услуги, общи условия, списъци на Регистриращи органи, доклади от одити, извършени от органи за оценка на съответствието и надзорни органи, както и други документи, свързани с дейността на квалифициран доставчик на квалифицирани удостоверителни услуги;
- предоставя достъп до издадените квалифицирани удостоверения, в случаите, когато абонатът не е заявил несъгласие за публикуване;
- предоставя достъп до информация относно статуса на квалифицираните удостоверения: с публикуване на Списък на спрените и прекратени квалифицирани удостоверения – CRL. и през интерфейс за статуса на издадените квалифицирани удостоверения – OCSP;
- предоставя постоянен достъп до информацията в публичния регистър на Удостоверяващ орган, Регистриращите органи, абонатите и доверяващите страни.

Страните (включително абонати и доверяващи се страни), които имат достъп до хранилището и уеб сайта на StampIT, приемат клаузите на тази ПДПКУУ и другите условия за използване, посочени от StampIT, с изключение на информацията, която се предоставя в демонстрационните и тестовите квалифицирани удостоверения. Страните приемат условията за използване, когато направят запитване за статуса на квалифицираното удостоверение или като използват или се доверяват на предоставената информация или услуги.

9.7 Освобождаване от отговорност

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

- конкретно поети задължения от абонат, като например поемане на отговорност към трета страна, договорни санкции и др.;
- обезщетения за съдебни, административни или дисциплинарни санкции, както и присъдени на абоната съдебни разноски;
- обявяването в несъстоятелност на абонат или трета страна;
- закъснение или невъзможност на абонатите да подадат искане за прекратяване действието на квалифицирано удостоверение на StampIT;
- неполагане от страна на абонатите на дължимата грижа, за да предотвратят компрометиране или загуба на частния ключ;
- неспазване от страна на абонатите на изискванията и задълженията, посочени в “Практиката на доставчика при предоставяне на квалифицирани удостоверителни услуги” (ПДПКУУ);
- неприлагане на проверка на електронния подпис на абонат;
- неприлагане на подходящи мерки за сигурност преди и по време на създаването и по-нататъшното обработване на криптирани съобщения;

- незаконни действия на абонатите и трети страни. StampIT има право на обезщетение за вреди, претърпени в резултат на подобни незаконни действия;
- повреди, които са извън контрола на StampIT, включително и при енергийни или телекомуникационни повреди извън контрола на StampIT;
- използването на квалифицирани удостоверения за оперирane с чувствително оборудване, включително и, но не ограничено до: ядрено оборудване, навигационни или комуникационни системи в авиацията, системи за управление на въздушното движение, системи за управление на оръжия и всички случаи, които могат да доведат до смърт, телесни увреждания или да нанесат вреди на околната среда;
- злоупотреба от страна на абонатите и трети страни с Интернет, телекомуникации или мрежи с добавена стойност, включително чрез използване или възпроизвеждане на компютърни вируси;
- форсмажорни обстоятелства.

9.8 Ограничения на отговорността

Максималният лимит на обезщетение за претърпени вреди, причинени от използ-ването на квалифицирано удостоверение, издадено от StampIT е в размер на максималния лимит, определен съгласно националното право.

9.9 Отговорност на Абоната

Абонатът/ Титулярят/ Създателят отговаря пред Доставчика и пред всички доверяващи се лица:

- ако при създаването на ключовата двойка е използвал алгоритъм и устройства за създаване на електронен подпис/ електронен печат, които не съответстват на изискванията на Регламент (ЕС) № 910/2014;
- ако не е спазвал изискванията за сигурност,определени от Доставчика;
- ако не е поискал спиране и прекратяване на валидността на удостоверението след като е узнал, че са налице обстоятелства, свързани с узнаване или компрометиране на частния ключ или с неправомерното му използване;
- за всякакви неверни изявления, направени от него при издаване на квалифицираното удостоверение;

Абонатът/ Титулярят/ Създателят отговаря пред Доставчика:

- когато не е съхранявал правилно частния ключ, съответстващ на посочения в удостоверението публичен ключ.
- ако при издаването на квалифицираното удостоверение е предоставил неверни данни/ премълчал е данни, които имат отношение към съдържанието или към процедурата по издаване на удостоверението.

9.10 Срок и прекратяване на действието на документа

Тази Практика влиза в сила след одобрение от изпълнителния директор на „Информационно обслужване“АД и публикуването ѝ на адрес: http://www.stampit.org/repository/.

Този документ може да бъде променян от „Информационно обслужване“АД по всяко време, като всяка приета промяна се отразява в нова актуална версия на документа, която влиза в сила след публикуването ѝ на адрес: https://www.stampit.org/repository/.

В отношенията с Абонатите и третите лица е валидна само версията, която е актуална към момента на ползването на услугите на „Информационно обслужване“АД.

Действието на Практиката се прекратява с прекратяването на дейността на StampIT.

При прекратяване на действието на версия на документа, същата се съхранява в хранилището на документите на StampIT.

9.11 Бележки и съобщения

Комуникацията между StampIT и Абонатите/ Титуляри/ Създатели, доверяващите страни и трети лица може да се осъществява по пощата, по електронна поща, телефон, факс и мрежови протоколи – в зависимост от вида на обменяната информация и използваните услуги.

Информацията за пробиви в сигурността, както и всяка друга информация, която подлежи на публично оповестяване, се обявява на http://www.stampit.org.

9.12 Изменения в Практиката

Ако някоя от клаузите в тази ПДПКУУ или нейното прилагане се окаже недействителна или неизпълнима до известна степен или по някаква причина, останалата част от условията на тази ПДПКУУ (и прилагането на тази клауза, касаещо други лица или обстоятелства) ще бъдат тълкувани по такъв начин, че да отговарят на националното право и на първоначалните намерения на страните.

Всяка една от клаузите на тази ПДПКУУ, която предвижда ограничаване на отговорността, отхвърляне или ограничаване на гаранции или други задължения или изключване на вреди, се смята от страните за отделна и независима от другите клаузи и трябва да бъде прилагана като такава.

Доставчикът може да пристъпи към изменения в Практиката, когато са възникнали нормативни, технологични или процедурни промени.

Измененията в Практиката, които водят до нови редакции или нови версии на документа се публикуват на адрес: https://www.stampit.org/repository/.

9.13 Процедури за решаване на спорове

Споровете между Доставчика и Абонатите, свързани с квалифицираните удостоверителни услуги на „Информационно обслужване“ АД, първо ще бъдат уреждани по взаимно съгласие.

„Информационно обслужване“ АД ще разглежда само писмени претенции, изпратени на адрес: гр.София 1504, район Оборище, ул.“Панайот Волов“№2, факс +359 2 943 6607.

Претенциите ще бъдат разглеждани от правния отдел на „Информационно обслужване“АД. Жалбоподателят следва да получи отговор в рамките на 14 дни от получаване на жалбата.

В случай на невъзможност за уреждане на спора чрез преговори в рамките на 30 дни, страните могат да предадат спора за решаване от съответния компетентен съд със седалище в гр.София.

9.14 Приложимо право

За неуредените в тази Практика въпроси се прилага националното право.

9.15 Съответствие с приложимото право

Тази ПДПКУУ е издадена и се тълкува в съответствие с Регламент (ЕС) № 910/2014 и националното право. Изборът на законодателство е направен, за да гарантира непротиворечиво тълкуване на тази ПДПКУУ, независимо от местоживеенето или седалището на абоната или мястото на използване на квалифицираното удостоверение, или други продукти и услуги, предоставяни от StampIT. Националното право се прилага за всички договорни отношения на StampIT, в които тази ПДПКУУ може да бъде прилагана във връзка с продуктите и услугите на StampIT.

9.16 Други разпоредби

Практиката не посочва други разпоредби.