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

Предоставяне на квалифицирани удостоверителни услуги от
„Информационно обслужване“ АД

ПОЛИТИКА
при предоставяне на квалифицирани удостоверения за автентичност на уебсайт (eIDAS-CP-SSL)

Версия: 2.0
Дата на публикуване: 07.06.2017 г.
Дата на последна корекция: 07.06.2017 г.

Съдържание

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

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

ИЗПОЛЗВАНИ ТЕРМИНИ И СЪКРАЩЕНИЯ

Регламент (ЕС) № 910/2014	Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета от 23 юли 2014 година относно електронната идентификация и удостоверителните услуги при електронни трансакции на вътрешния пазар и за отмяна на Директива 1999/93/ЕО.
Директива 95/46/ЕО	Директива 95/46/ЕО на Европейския парламент и на Съвета от 24 октомври 1995 г. за защита на физическите лица при обработването на лични данни и за свободното движение на тези данни
Удостоверителна услуга	Електронна услуга, предоставяна от „Информационно обслужване“ АД срещу възнаграждение, която се състои в: а) създаването и проверката на електронни подписи, електронни печати и електронни времеви печати, както и удостоверения, свързани с тези услуги; б) създаването и проверката на удостоверения за автентичност на уебсайт.
Квалифицирана удостоверителна услуга	Удостоверителна услуга, която отговаря на приложимите изисквания, определени в Регламент (ЕС) № 910/2014.
Титуляр на електронен подпис	Физическо лице, което създава електронен подпис.
Електронен подпис	Данни в електронна форма, които се добавят към други данни в електронна форма или са логически свързани с тях и които титулярят на електронния подпис използва, за да се подписва.
Усъвършенстван електронен подпис	Електронен подпис, който отговаря на следните изисквания: а) свързан е по уникален начин с титуляря на подписа; б) може да идентифицира титуляря на подписа; в) създаден е чрез данни за създаване на електронен подпис, които титулярят на електронния подпис може да използва с висока степен на доверие и единствено под свой контрол; и г) свързан е с данните, които са подписани с него, по начин, позволяващ да бъде открита всяка последваща промяна в тях.
Квалифициран електронен подпис	Усъвършенстван електронен подпис, който е създаден от устройство за създаване на квалифициран електронен подпис и се основава на квалифицирано удостоверение за електронни подписи.
Данни за създаване на електронен подпис	Уникални данни, които се използват от титуляря на електронния подпис за създаването на електронен подпис.
Удостоверение за електронен подпис	Електронен атестат, който свързва данните за валидиране на електронен подпис с физическо лице и потвърждава най-малко името или псевдонима на това лице.
Квалифицирано удостоверение за електронен подпис (КУЕП)	Удостоверение за електронни подписи, което се издава от доставчик на квалифицирани удостоверителни услуги и отговаря на изискванията, предвидени в приложение I към Регламент (ЕС) № 910/2014.
Устройство за създаване на електронен подпис	Конфигуриран софтуер или хардуер, който се използва за създаването на електронен подпис
Устройство за създаване на квалифициран електронен подпис	Устройство за създаване на електронен подпис, което отговаря на изискванията, предвидени в приложение II към Регламент (ЕС) № 910/2014
Създател на печат	Юридическо лице, което създава електронен печат.

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

	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
QSCD	Устройство за създаване на квалифициран електронен подпис или печат
NCP+	Засилена нормализирана удостоверителна политика, която включва допълнителни изисквания за квалифицирани удостоверения в съответствие с Регламент (ЕС) № 910/2014
Certification Authority (CA)	Удостоверяващ орган
Common Name (CN)	Публично име
Certificate Policy (CP)	Политика за предоставяне на квалифицирано удостоверение за електронен подпис, електронен печат и автентичност на уебсайт
Certification Practice Statement (CPS)	Практика при предоставяне на удостоверителни услуги
Certificate Revocation List (CRL)	Списък със спрени и прекратени удостоверения
Distinguished Name (DN)	Отличително име на субект, вписан удостоверението
Enhanced key usage	Разширени цели за използването на ключа
Federal Information Processing Standard (FIPS)	Федерален стандарт за обработка на информация
Hardware Security Module	Хардуерен криптографски модул
Object Identifier (OID)	Обектен идентификатор

Public Key Cryptography Standards (PKCS)	Серия стандарти в криптографията на публичния ключ
Public Key Infrastructure (PKI)	Инфраструктура на публичния ключ
Registration Authority (RA/PO)	Регистриращ орган

1. Въведение

Настоящият документ описва общите правила, прилагани от „Информационно обслужване“ АД при издаване и управление на квалифицирани удостоверения за автентичност на уебсайт, както и приложимите за тях услуги и обхвата на приложимост.

Целта на услугите по удостоверяване на уебсайт е да потвърди, че домейна се управлява от легитимен субект или организация.

Предлаганите услуги по удостоверяване на автентичност на уебсайт са в съответствие с Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета от 23 юли 2014 година относно електронната идентификация и удостоверителните услуги при електронни транзакции на вътрешния пазар, изискванията и насоките, дефинирани от CA/Browser Forum (https://cabforum.org/) и в съответствие с приложимото законодателство в Република България.

При издаване на квалифицирани удостоверения за автентичност на уебсайт се прилагат процедури и практики, гарантиращи най-висока сигурност при издаване, публикуване и управление на издаваните квалифицирани удостоверения.

1.1. Общ преглед на политиката

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

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

Политиката е съобразена със следните документи:

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

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

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

1.2. Наименование и идентификатор на политиката

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

Идентификаторите за политиките на квалифицираните удостоверения за автентичност на уебсайт, посочени в настоящия документ са както следва:

DVCP/Domain Validation Certificate Policy

itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) dvcp (6)

OVCP/Organizational Validation Certificate Policy

itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) ovcp (7)

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

Вид удостоверение	StampIT Policy Identifier	ETSI Policy Identifier
StampIT Server DVC	1.3.6.1.4.1.11290.1.2.1.8	0.4.0.2042.1.6
StampIT Server OVC	1.3.6.1.4.1.11290.1.2.1.9	0.4.0.2042.1.7

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.

1.3.1. Удостоверяващ орган

StampIT е Удостоверяващият орган на „Информационно обслужване“ АД, който издава квалифицирани удостоверения за автентичност на уебсайт (КУАУ). Удостоверяващият орган извършва дейности, които включват издаване, подновяване, спиране, възобновяване и прекратяване на КУАУ, водене на регистри и осигуряване на достъп до тях.

1.3.2. Регистриращи органи

Удостоверяващият орган издава 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 КУАУ в съответствие с вътрешните правила на StampIT;

- регистрират подадените искания за квалифицирани удостоверителни услуги на StampIT;
- участват във всички етапи при идентифицирането на Абонатите, както е определено от StampIT, в зависимост от типа квалифицирано удостоверение, което издават;
- позовават се на официални, нотариално заверени или други посочени документи, за да проверят искането, подадено от заявителя;
- след одобрение на искането, уведомяват StampIT за 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 при изграждане на връзка с уебсайт.

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

1.4. Приложимост и ограничения за употреба на издаваните квалифицирани удостоверения

1.4.1. Приложимост

Издаваните квалифицирани удостоверения за автентичност на уебсайт могат да се използват единствено за удостоверяване на уебсайт, в съответствие с ограниченията на вида на издаденото квалифицирано удостоверение.

1.4.2. Ограничения

Забранено е използването на издаваните квалифицирани удостоверения извън предвидените в настоящата политика начини и цели. Забранено е използването на издаваните квалифицирани удостоверения за извършване на дейности, попадащи под

ограниченията на законите на Република България и приложимите регламенти и директиви на Европейския съюз.

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

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

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

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

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

Информация за връзка със StampIT:

Ул. „Лъчезар Станчев“ 11, ж.к. Изгрев

1756 София, България

Тел.: + 359 2 9656 291

Факс: + 359 2 9656 212

Web: https://www.stampit.org

E-mail: support@mail.stampit.org

2. Публични регистри и управление

2.1. Поддържани публични регистри

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

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

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

2.2. Честота на опресняване

Честотата на опресняване на публикуваните квалифицирани удостоверения е както следва:

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

2.3. Достъп

StampIT осигурява HTTP/HTTPS(TLS) и OCSP базиран достъп до поддържаните регистри.

Достъпът до публикуваната информацията не се ограничава, освен по искане на Титуляря/Създателя и само по отношение на негово валидно издадено квалифицирано удостоверение.

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

3. Идентификация и проверка на информацията за самоличност

3.1. Наименоване

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

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

Полето „Subject" съдържа уникалното наименование на уеб сървъра.

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

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

3.1.1. Наименоване на уеб сървър

Използваната структура на Subject 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 – име на домейн(квалифицирано DNS име) или публичен IP адрес;
- GN – собствено име на физическото лице. Незадължително;
- SN – фамилно име на физическото лице. Незадължително;

- O – наименование на организацията, представлявана от лицето. Задължително при издаването на тип OVC;
- organizationIdentifier – идентификатор на организацията. Задължително при издаването на тип OVC;
- OU – организационна единица. Попълва се при издаването на тип OVC, след надлежното удостоверяване. Незадължително;
- SA – адрес. Попълва се при издаването на тип OVC, след надлежното удостоверяване. Незадължително;
- L – местоположение. Попълва се при издаването на тип OVC, след надлежното удостоверяване. Незадължително;
- SerialNumber – уникален идентификатор на физическото лице
- Други полета, които се подробно описани в профилите на квалифицираните удостоверения

3.1.2. Алтернативни имена (Subject Alt Name)

Некритично разширение, трябва да съдържа минимум CN записа, както и да бъдат добавени допълнителни домейни/публични IP адреси, под контрола на Абоната.

3.1.3. Смислени имена

Имената трябва да са свързани с услугата, която представят. StampIT Може да откаже издаването на квалифицирано удостоверение по свое усмотрение.

3.1.4. Анонимност и псевдоними

Описано в „Практика при предоставяне на квалифицирани удостоверителни услуги“.

3.1.5. Тълкуване на различните форми на имената

StampIT съдейства на Абоната при необходимост от тълкуване на данни, свързани с издаването на квалифицираното удостоверение.

3.1.6. Уникалност на имената

Издаваните квалифицирани удостоверения трябва да бъдат уникални в рамките на регистъра, воден от StampIT. При необходимост може да се добави допълнителен идентификатор за гарантиране на уникалността.

3.1.7. Автентичност и търговска марка. Разрешаване на спорове

Описано в „Практика при предоставяне на квалифицирани удостоверителни услуги“.

3.2. Първоначална регистрация

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

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

3.2.1. Проверка за притежание на частен ключ

Описано в „Практика при предоставяне на квалифицирани удостоверителни услуги".

3.2.2. Проверка на юридическите лица

Описано в „Практика при предоставяне на квалифицирани удостоверителни услуги".

3.2.3. Проверка на физическите лица

Описано в „Практика при предоставяне на квалифицирани удостоверителни услуги".

3.2.4. Проверка от удостоверяващия орган

Описано в „Практика при предоставяне на квалифицирани удостоверителни услуги".

3.2.5. Осигуряване на оперативна съвместимост

При изпълнение на дейността си, StampIT може да се си сътрудничи и с трети лица, включително и доставчици на удостоверителни услуги, освен в случаите, когато са налице следните хипотези:

- възможен конфликт на интереси;
- обективна възможност за нарушаване правата на Абонатите;
- специфична законова или друга разпоредба.

3.2.6. Проверка на домейн и/или IP адрес

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.

3.2.7. Критерии за съответствие

Описано в „Практика при предоставяне на квалифицирани удостоверителни услуги".

3.3. Подновяване на квалифицираното удостоверение

Описано в „Практика при предоставяне на квалифицирани удостоверителни услуги“.

3.4. Временно спиране и прекратяване на действието на квалифицираното удостоверение

Описано в „Практика при предоставяне на квалифицирани удостоверителни услуги“.

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

Описано в „Практика при предоставяне на квалифицирани удостоверителни услуги“.

4. Оперативни дейности

Описано в „Практика при предоставяне на квалифицирани удостоверителни услуги“.

4.1. Валидна употреба на издаваните квалифицирани удостоверения

4.1.1. От страна на абонатите

Описано в „Практика при предоставяне на квалифицирани удостоверителни услуги“.

4.1.2. От страна на доверяващите се страни

Описано в „Практика при предоставяне на квалифицирани удостоверителни услуги“.

4.2. Подновяване и преиздаване на квалифицирани удостоверения

Описано в „Практика при предоставяне на квалифицирани удостоверителни услуги“.

4.2.1. Процедура по подновяване на квалифицирани удостоверения

Описано в „Практика при предоставяне на квалифицирани удостоверителни услуги“.

4.3. Промяна на информация в квалифицираните удостоверения

Описано в „Практика при предоставяне на квалифицирани удостоверителни услуги“.

4.4. Спиране на квалифицираните удостоверения

Описано в „Практика при предоставяне на квалифицирани удостоверителни услуги“.

4.4.1. Основания за спиране

Описано в „Практика при предоставяне на квалифицирани удостоверителни услуги".

4.4.2. Процедура за спиране

Описано в „Практика при предоставяне на квалифицирани удостоверителни услуги".

4.5. Възобновяване на квалифицираните удостоверения

Описано в „Практика при предоставяне на квалифицирани удостоверителни услуги".

4.5.1. Основания за възобновяване

Описано в „Практика при предоставяне на квалифицирани удостоверителни услуги".

4.5.2. Процедура за възобновяване

Описано в „Практика при предоставяне на квалифицирани удостоверителни услуги".

4.6. Прекратяване на квалифицираните удостоверения

Описано в „Практика при предоставяне на квалифицирани удостоверителни услуги".

4.6.1. Основания за прекратяване

StampIT може да прекрати по свое усмотрение издадено квалифицирано удостоверение при наличие на основателни съмнения за компрометиране на частния ключ или при използването му за незаконни дейности.

Описано в „Практика при предоставяне на квалифицирани удостоверителни услуги".

4.6.2. Процедура за прекратяване

Описано в „Практика при предоставяне на квалифицирани удостоверителни услуги".

4.7. Статус на издаваните квалифицирани удостоверения

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

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

Описано в „Практика при предоставяне на квалифицирани удостоверителни услуги".

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

Описано в „Практика при предоставяне на квалифицирани удостоверителни услуги".

4.7.3. Ръчно, чрез Интернет страницата на StampIT

Описано в „Практика при предоставяне на квалифицирани удостоверителни услуги".

5. Физическа и организационна сигурност

5.1. Физическа сигурност

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

„Информационно обслужване" АД е внедрило и поддържа Интегрирана система за управление, сертифицирана от външен сертифициращ орган по стандартите ISO 27001:2013 за управление на информационната сигурност, ISO 20000-1:2011 за управление на предоставяните ИТ услуги и ISO 9001:2015 за управление на качеството.

5.1.1. Сигурни помещения

Описано в „Практика при предоставяне на квалифицирани удостоверителни услуги".

5.1.2. Съхранение на данни

Описано в „Практика при предоставяне на квалифицирани удостоверителни услуги".

5.1.3. Сигурно унищожаване на данни

Описано в „Практика при предоставяне на квалифицирани удостоверителни услуги".

5.2. Организационна сигурност

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

Дейностите се изпълняват от служители със съответна квалификация и роля в съответния процес, така, че да се минимизира възможността от компрометиране на заложените контроли, изтичане на конфиденциална информация и избягване на конфликт на интереси. Ролите са регламентирани във вътрешните процедури на StampIT и длъжностните характеристики на всеки служител, имащ отношение към работата на Доставчика.

5.3. Сигурност на персонала

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

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

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

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

5.3.1. Обучение на персонала

Описано в „Практика при предоставяне на квалифицирани удостоверителни услуги".

5.4. Управление на записи и журнали

Описано в „Практика при предоставяне на квалифицирани удостоверителни услуги".

5.5. Управление на архивите

Описано в „Практика при предоставяне на квалифицирани удостоверителни услуги".

5.6. Прекратяване на дейността на Удостоверяващия орган

Описано в „Практика при предоставяне на квалифицирани удостоверителни услуги".

6. Управление на техническата сигурност

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

Описано в „Практика при предоставяне на квалифицирани удостоверителни услуги".

6.2. Генериране на ключовата двойка на Абонат

Използваните алгоритми за генериране на ключовата двойка трябва да отговарят на минималните изисквания, дефинирани в ETSI TS 119 312.

Описано в „Практика при предоставяне на квалифицирани удостоверителни услуги".

6.2.1. Изисквания към устройствата/системата

Описано в „Практика при предоставяне на квалифицирани удостоверителни услуги".

6.2.2. Предоставяне на ключовата двойка на Абоната

Описано в „Практика при предоставяне на квалифицирани удостоверителни услуги".

6.2.3. Минимални дължини на ключовите двойки

Използваната дължина на ключовата двойка трябва да отговарят на минималните изисквания, дефинирани в ETSI TS 119 312.

Описано в „Практика при предоставяне на квалифицирани удостоверителни услуги".

6.2.4. Параметри на публичния ключ

Описано в „Практика при предоставяне на квалифицирани удостоверителни услуги".

6.2.5. Управление на частния ключ

6.2.5.1. Съхранение на частния ключ

Описано в „Практика при предоставяне на квалифицирани удостоверителни услуги".

6.2.5.2. Активиране на частния ключ

Описано в „Практика при предоставяне на квалифицирани удостоверителни услуги".

6.2.5.3. Деактивиране на частния ключ

Описано в „Практика при предоставяне на квалифицирани удостоверителни услуги".

6.2.5.4. Унищожаване на частния ключ

Описано в „Практика при предоставяне на квалифицирани удостоверителни услуги".

6.3. Управление на ключовата двойка

6.3.1. Архивиране на публичния ключ

Описано в „Практика при предоставяне на квалифицирани удостоверителни услуги".

6.3.2. Валидност и употреба на издаваните удостоверения

Описано в „Практика при предоставяне на квалифицирани удостоверителни услуги".

6.4. Активиране на частния ключ

Описано в „Практика при предоставяне на квалифицирани удостоверителни услуги".

6.4.1. Генериране и предоставяне на данни за активиране

Описано в „Практика при предоставяне на квалифицирани удостоверителни услуги".

6.4.2. Защита на данни за активиране

Описано в „Практика при предоставяне на квалифицирани удостоверителни услуги“.

6.5. Сигурност на използваните компютърни системи

Описано в „Практика при предоставяне на квалифицирани удостоверителни услуги“.

6.6. Управление на промените в системата на StampIT

Описано в „Практика при предоставяне на квалифицирани удостоверителни услуги“.

6.7. Управление на мрежовата сигурност

Описано в „Практика при предоставяне на квалифицирани удостоверителни услуги“.

7. Профили на удостоверенията

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

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

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

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

StampIT Global Qualified CA			
Signature Algorithm	SHA256/RSA		
Issuer	CN	StampIT Global Root CA	Име
	C	BG	Държава
	O	Information Services JSC	Организация
	L	Sofia	
	2.5.4.97 (organizationidentifier)	NTRBG-831641791	ЕИК
Validity	20 години		
Subject	CN	StampIT Global Qualified CA	Име
	C	BG	Държава
	O	Information Services JSC	Организация
	L	Sofia	Област
	2.5.4.97 (organizationidentifier)	NTRBG-831641791	ЕИК
Public Key	RSA 4096 bits		
Key Usage (Critical)	Certificate Signing, Off-line CRL Signing, CRL Signing (06)		
Friendly Name	StampIT Global Qualified CA		
Basic constrains (Critical)	Subject Type=CA Path Length Constraint=0		
Authority Information Access	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://www.stampit.org/repository/stampit_global_root_ca.crt [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.stampit.org/		
CRL Distribution Point /Non Critical/	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.stampit.org/crl/stampit_global.crl		
Certificate Policies (Non Critical)	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.11290.1.2.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS		

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

7.3. Профил на квалифицирано удостоверение за автентичност на уебсайт StampIT Server DVC

StampIT Server DVC Profile			
Signature Algorithm	SHA256withRSA		
Issuer	CN	StampIT Global Qualified CA	
	C	BG	
	O	Information Services JSC	
	L	Sofia	
	OrganizationIdentifier (2.5.4.97)	NTRBG- 831641791	
Validity	1 or 3 years		
Subject	*C	Country	
	L	Locality	
	*CN	Common Name	
	*E	E-mail	
Public Key	RSA 2048 bits		
Key Usage (Critical)	Digital Signature Key Encipherment		
Authority Information Access	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=https://www.stampit.org/repository/stampit_global_qualified.crt [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.stampit.org/		
Extended key usage (Non Critical)	Server Authentication		
Subject Alternative Name	DNS		
Qualified Certificate Statement (Non Critical)	id-etsi-qcs-semanticsId-Legal(oid=0.4.0.194121.1.2) id-etsi-qcs-QcCompliance (oid=0.4.0.1862.1.1) id-etsi-qct-web (oid=0.4.0.1862.1.6.3) id-etsi-qcs-QcPDS(oid=0.4.0.1862.1.5) PdsLocation=https://www.stampit.org/pds/pds_en.pdf language=en		
Basic constrains (Critical)	End entity		
CRL Distribution Point/Non Critical/	DP Name: http://www.stampit.org/crl/stampit_global_qualified.crl		
Certificate Policies (Non Critical)	[1] Certificate Policy: Policy Identifier=1.3.6.1.4.1.11290.1.2.1.8 Policy Qualifier Id=CPS/1.3.6.1.5.5.2.7.1/ Qualifier=https: /www.stampit.org/repository/		

7.4. Профил на квалифицирано удостоверение за автентичност на уебсайт StampIT Server OVC

StampIT Server OVC Profile			
Signature Algorithm	SHA256withRSA		
Issuer	CN	StampIT Global Qualified CA	
	C	BG	
	O	Information Services JSC	
	L	Sofia	
	OrganizationIdentifier (2.5.4.97)	NTRBG-831641791	
Validity	1 or 3 years		
Subject	*C	Country	
	L	Locality	
	*CN	Common Name	
	*E	E-mail	
	O	Organization	
Public Key	RSA 2048 bits		
Key Usage (Critical)	Digital Signature Non-Repudiation Key Encipherment		
Authority Information Access	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.stampit.org/ [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://stampit.org/repository/stampit_global_qualified.crt		
Extended key usage (Non Critical)	Server Authentication		
Subject Alternative Name	DNS name		
Qualified Certificate Statement (Non Critical)	id-etsi-qcs-semanticsId-Legal(oid=0.4.0.194121.1.2) id-etsi-qcs-QcCompliance (oid=0.4.0.1862.1.1) id-etsi-qct-web (oid=0.4.0.1862.1.6.3) id-etsi-qcs-QcPDS(oid=0.4.0.1862.1.5) PdsLocation=https://www.stampit.org/pds/pds_en.pdf language=en		
Basic constrains (Critical)	End entity		
CRL Distribution Point/Non Critical/	DP Name: http://www.stampit.org/crl/stampit_global_qualified.crl		
Certificate Policies (Non Critical)	[1] Certificate Policy: Policy Identifier=1.3.6.1.4.1.11290.1.2.1.9 Policy Qualifier Id=CPS/1.3.6.1.5.5.2.7.1/ Qualifier=http://www.stampit.org/repository		

8. Контрол на дейността на Доставчика

Описано в „Практика при предоставяне на квалифицирани удостоверителни услуги“..

9. Бизнес и правни въпроси

9.1. Цени

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

9.1.1. Отстраняване на неточности и възстановяване на извършено плащане

Описано в „Практика при предоставяне на квалифицирани удостоверителни услуги“.

9.2. Финансова отговорност

Описано в „Практика при предоставяне на квалифицирани удостоверителни услуги“.

9.2.1. Гаранции за плащане на обезщетенията

Описано в „Практика при предоставяне на квалифицирани удостоверителни услуги“.

9.3. Защита на личните данни

Описано в „Практика при предоставяне на квалифицирани удостоверителни услуги“.

9.4. Права върху интелектуалната собственост

Описано в „Практика при предоставяне на квалифицирани удостоверителни услуги“.

9.4.1. Собственост на ключовите двойки

Описано в „Практика при предоставяне на квалифицирани удостоверителни услуги“.

9.5. Задължения и отговорност на StampIT

Описано в „Практика при предоставяне на квалифицирани удостоверителни услуги“.

9.5.1. Отговорност пред Абоната

Описано в „Практика при предоставяне на квалифицирани удостоверителни услуги“.

9.5.2. Ограничения на отговорността на регистриращия орган

Описано в „Практика при предоставяне на квалифицирани удостоверителни услуги“.

9.6. Задължения на абоната

Описано в „Практика при предоставяне на квалифицирани удостоверителни услуги“.

9.7. Освобождаване от отговорност

Описано в „Практика при предоставяне на квалифицирани удостоверителни услуги“.