"Информационно обслужване" АД
София, ул."Панайот Волов" № 2 тел. 943-67-10 факс 943-66-07 E-mail:office@is-bg.net

предоставяне на удостоверителни услуги от "Информационно Обслужване" АД,
"Наръчник **на потребителя"**

Практика на доставчика при предоставяне на удостоверителни услуги

Версия: 1.02
Дата на публикуване: 27 Март 2003 г.

одобрен с решение №260 от 27.03.2003 г. на Комисията за регулиране на съобщенията

Съдържание

Вие можете да изпращате Вашите коментари по този CPS на E-mail адрес support@mail.stampit.org или да ги изпратите по пощата на адрес:

"Информационно обслужване" АД - StampIT
Ул. "165" 3, ж.к. Изгрев,
1797 София, България
Тел.: + 359 2 9656 2044
Факс: + 359 2 9656 2012
E-mail:support@mail.stampit.org

"Информационно обслужване" АД
София, ул."Панайот Волов" № 2
тел. 943 6710
факс 943 6607
БУЛСТАТ: Ю 831641791
Данъчен номер: 1223007402

1 Общ преглед

Този раздел прави общ преглед на публичните удостоверителни услуги на StampIT.

1.1 Доставчик на удостоверителни услуги

"Информационно обслужване" АД е доставчик на удостоверителни услуги и работи в съответствие със Закона за електронния документ и електронния подпис (ЗЕДЕП) и подзаконовите нормативни актове, издадени по неговото прилагане. "Информационно обслужване" АД предоставя удостоверителни услуги посредством Удостоверяващ орган и мрежа от Регистриращи органи. Удостоверяващият орган и регистриращите органи извършват дейностите си по предоставяне на удостоверителните услуги от името и за сметка на "Информационно обслужване" АД.

1.1.1 Удостоверяващ орган

StampIT е Удостоверяващият орган на "Информационно обслужване" АД, който издава сертификати от висок клас на физически или юридически лица. Удостоверяващият орган извършва дейности, свързани с функциите на публичния ключ, които включват издаване, подновяване, спиране и възобновяване, прекратяване на сертификат, водене на регистър и осигуряване на достъп до него.

1.1.2 Регистриращи органи

Удостоверяващият орган издава сертификати 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 сертификати;
- регистрират подадените искания за сертификационни услуги на StampIT;
- участват във всички етапи при идентифицирането на абонатите, както е определено от StampIT, в зависимост от типа сертификат, който издават;
- позовават се на официални, нотариално заверени или други посочени документи, за да проверят искането, подадено от заявителя;
- след одобрение на искането, уведомяват StampIT да издаде сертификат;
- регистрират подадените заявки за подновяване, прекратяване, временно спиране и възобновяване на действието на сертификати.

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

1.2 Удостоверения за електронен подпис (Електронни сертификати)

Удостоверението за електронен подпис, наричано по-нататък за краткост Сертификат, представлява форматирани данни, които свързват определен абонат с публичния му ключ. Сертификатът дава възможност на дадено лице, което участва в електронна транзакция да докаже самоличността си пред другите участници в тази транзакция.

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

Сертификатите от типа StampIT Doc Certificate и StampIT DocPro Certificate имат статут на удостоверения за универсален електронен подпис, съгласно Закона за електронния документ и електронния подпис (ЗЕДЕП).

1.3 Взаимодействие с потребителите за избор на сертифицикационни услуги

StampIT оказва съдействие на клиентите си за избор на подходяща сертификационна услуга. Абонатите трябва внимателно да определят изискванията си към специфичните приложения за защитени комуникации, преди да подадат искане за издаване на съответния тип сертификат.

1.4 Абонати

Абонатите са физически или юридически лица, които са подали искане и след успешно завършване на процедурата, им е бил издаден сертификат. Преди да бъде извършена проверка и да му бъде издаден сертификат, абонатът е само заявител за услугите на StampIT.

Абонатът е титуляр и автор на електронния подпис, в случаите при които сертификатът е издаден на физическо лице.

Абонатът е титуляр на електронния подпис, когато сертификатът е издаден по искане на юридическо лице, а авторът на електронния подпис съхранява частния ключ и е упълномощен да представлява титуляра и да извършва действия от негово име и за негова сметка.

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

1.5 Доверяващи се страни

Доверяващите се страни са физически или юридически лица, които използват PKI услугите със сертификатите, издадени от StampIT и се доверяват на тези сертификати и/или електронни подписи, които могат да бъдат проверени чрез публичния ключ, записан в сертификата на абоната.

За да бъде потвърдена валидността на сертификата, който получават, доверяващите се страни трябва да се обръщат към StampIT директорията, която включва Списъка с Прекратените Сертификати, всеки път преди да вземат решение дали да се доверят на информацията посочена в сертификата.

1.6 Практика на доставчика при предоставяне на удостоверителни услуги-ПДПУУ (Certification Practice Statement - CPS)

Настоящият документ "Практика на доставчика при предоставяне на удостоверителни услуги", наричан за по-кратко CPS, е публично изявление за практиките на StampIT и условията на издаване, временно спиране, прекратяване и т.н. на сертификат издаден в йерархията от сертификати на StampIT. В съответствие с дейностите на Удостоверяващия орган, този CPS е разделен най-общо на следните раздели: Технически, Организационен и Правен.

Този CPS е разработен в съответствие с изискванията на общоприетата международна спецификация RFC 2527 и българското законодателство.

Този CPS е публично достъпен и може да бъде намерен на
http://www.stampit.org/repository/
E-mail: support@mail.stampit.org
И по поща на следния адрес:
"Информационно обслужване" АД - StampIT
Ул. "165" 3, ж.к. Изгрев,
1797 София, България
Тел.: + 359 2 9656 2044
Факс: + 359 2 9656 2012
E-mail: support@mail.stampit.org

2 Технология

Този раздел описва определени технологични аспекти на инфраструктурата и PKI услугите на StampIT.

2.1 Издаване и управление на сертификатите

Управлението на сертификатите, издадени от StampIT най-общо се отнася до функции, които включват следното:

- проверка на идентичността на заявителя;
- издаване и подновяване на сертификати;
- прекратяване, временно спиране и възобновяване действието на сертификати;
- неутрализиране на кореспондиращите частни ключове чрез процес, включващ прекратяване на сертификати;
- вписване на сертификатите в регистър на издадените удостоверения;
- публикуване на сертификатите;
- съхраняване на сертификатите.

StampIT извършва общото управление на сертификатите, директно или чрез свои представители.

2.2 StampIT директории, хранилище и списък с прекратени сертификати

Директно или чрез услугите на трети страни, StampIT предоставя публичен достъп и управлява директории с издадени, временно спрени и прекратени сертификати, за да бъде повишено нивото на доверие в неговите услуги. Списъкът с прекратени сертификати е такава директория. Потребителите и доверяващите се страни са уведомени, че винаги трябва да проверяват директориите с издадените и прекратените сертификати преди да решат дали да се доверят на информацията вписана в даден сертификат. StampIT обновява списъка с прекратени сертификати на всеки три часа.

StampIT публикува и осигурява достъп до хранилища, съдържащи данни и документи, касаещи PKI услугите, включително този CPS, а също и всяка друга информация, която счита за важна за предоставяните от него услуги.

2.3 Надеждни системи

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

2.4 Типове StampIT сертификати

StampIT предлага набор от сертификати и свързани с тях услуги, които могат да бъдат използвани по такъв начин, че да бъдат изпълнени изискванията на потребителите за защитени лични и бизнес комуникации.

StampIT може да обновява или разширява списъка си с продукти и услуги, включително типа на сертификатите, които издава в съответствие с нормативните изисквания.

Издадените, временно спрени или прекратени сертификати се публикуват в съответните директории на Удостоверяващия орган.

2.4.1 Сертификати за подписване на обекти – StampIT Object Certificate

StampIT Object сертификатите се издават на юридически лица и могат да се използват за подписване на обекти, като например софтуер. StampIT Object сертификатите са валидни за период от една година.

2.4.2 Сертификати за защитен сървър - StampIT Server Certificate

StampIT Server сертификатите се издават на юридически лица и са предназначени за защитени комуникации с уеб сайт. Те позволяват сигурна идентификация на сайта пред посетителите и дават възможност за конфиденциални комуникации. Валидността на тези сертификати е една година.

2.4.3 Персонални сертификати

2.4.3.1 StampIT Doc Certificate

StampIT Doc сертификати се издават на физически лица и могат да бъдат използвани за идентифициране на абоната, защитено изпращане на електронни съобщения и защитени комуникации, достъп до лична информация и онлайн Интернет транзакции от всякакъв вид, като например Интернет абонаментни услуги.

StampIT Doc Сертификатите осигуряват високо ниво на идентичност, като се изисква абонатът да се яви лично пред Регистриращ Орган, за да докаже идентичността си. Валидността на тези сертификати е една година.

2.4.3.2 StampIT DocPro Certificate

StampIT DocPro сертификати се издават на физически лица, които са упълномощени да представляват юридически лица.Те могат да бъдат използвани за идентифициране на абоната, защитено изпращане на електронни съобщения и защитени комуникации, достъп до лична информация и онлайн Интернет транзакции.

StampIT DocPro сертификатите осигуряват високо ниво на идентичност, като се изисква заявителят да се яви лично пред Регистриращ Орган, за да представи документи за юридическото лице и да докаже идентичността си. Валидността на тези сертификати е една година.

2.4.3.3 StampIT Enterprise Certificate

StampIT Enterprise сертификати се издават по заявка на корпоративни клиенти на StampIT за физически лица, които са служители на корпоративния клиент. Физическите лица са обвързани с името на юридическото лице, но не са упълномощени да правят електронни изявления от негово име. Сертификатите могат да бъдат използвани за идентифициране, защитено изпращане на електронни съобщения и вътрешни комуникации в организацията, достъп до лична информация и онлайн Интернет транзакции.

Физическите лица не се явяват лично пред Регистриращ орган, а процесът по идентификацията им се извършва от упълномощено лице на корпоративния клиент. Валидността на тези сертификати е една година.

2.5 Одобрение на софтуерни и хардуерни устройства

Удостоверяващият орган на StampIT одобрява директно или чрез оторизирани консултанти хардуерът и софтуерът, които той използва, за да предоставя публичните си PKI услуги.

2.6 Разширения

2.6.1 Разширения в сертификатите (Certificate Extensions)

StampIT използва X.509, версия 3 базирани формати, за издаваните от него сертификати. В съответствие с X.509v3 Удостоверяващият орган може да дефинира разширения към основната структура на сертификатите.

2.6.2 Включване на информация в разширенията на сертификата

Разширенията обикновено се отразяват в сертификата на абоната. Те могат също така да бъдат частично дефинирани в сертификата, а останалата част може да представлява документ, към който е направена препратка от сертификата на абоната. Информацията, която се включва по този начин е публично достъпна.

2.7 Процес за генериране на частните ключове

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

2.7.1 Генериране на ключовете на StampIT

StampIT генерира по сигурен начин и защитава собствените си частни ключове, като използва надеждна система и взема необходимите мерки, за да предотврати компрометирането или неоторизираното им използване. StampIT внедрява и документира процедурата по генериране на ключовете, в съответствие с този CPS. StampIT внедрява европейските и общопризнати в международната практика стандарти за надеждни системи и прави всичко възможно, за да ги съблюдава.

2.7.2 Поделяне на секретни части

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

2.8 Профили на Сертификатите на StampIT

Профилът на Сертификата съдържа задължително полетата, посочени по-долу:

2.8.1 Поле - Key Usage

Полето Key Usage - определя предназначението на ключа, който се съдържа в сертификата. Това поле се използува, когато даден ключ може да бъде използван за повече от една операция и употребата му трябва да бъде ограничена.

Евентуалното предназначение на ключовете, определени от стандарта X.509v3, са както следва:

a) **Digital Signature** (електронен подпис) – за проверка на електронни подписи, които са за автентификация на субекти и проверка на целостта на данните и имат предназначение различно от това определено в т. b), e) или f).

b) **Non-repudiation** (неотменяемост) – за проверка на електронни подписи, използвани при осигуряване на услугите по неотменяемост, които осигуряват защита в случай, че подписващият се опита да отрече дадени действия (като изключение правят подписване на сертификат или CRL както е в т. e) или f) по-долу).

c) **Key encipherment** (криптиране на ключове) – за криптиране на ключовете или друга защитена информация, например при транспортиране на ключове.
d) **Data encipherment** (криптиране на данни) – за криптиране на данни, но не на ключове и друга защитена информация, както е посочено в т. c) по-горе.
e) **Key Certificate signing** (подписване на сертификати) – за проверка на подписа на Удостоверяващия орган върху сертификатите (използва се само в сертификатите на Удостоверяващия орган).
f) **CRL signing** (подписване на CRL) – за проверка на подписа на Удостоверяващия орган върху списъка с прекратените сертификати (CRL).

2.8.2 Разширение Basic Constraints

Разширението Basic Constraints определя дали субектът на сертификата е Удостоверяващ орган или краен потребител. Това разширение трябва винаги да бъде отбелязано като критично, иначе някои от приложенията ще го игнорират и ще позволят да бъде използван сертификат, който е издаден на краен потребител като серификат на Удостоверяващ орган.

2.8.3 Политика за сертифициране

Политиката за сертифициране (Certificate policy) е изявление на издателя, което съответства на предписаната употреба на сертификата в контекста на издаването му. Идентификатор на политиката е уникално число, което ясно идентифицира политиката.

3 Структура на идентификаторите на обекти

Идентификаторът на обект (OID) представлява поредица от цели числа, която се присвоява на регистриран обект и е уникален сред всички идентификатори на обекти в рамките на конкретната област.

Object Identifier					
Information Services Plc.	StampIT	Roots	Sub CAs	End Entity	Certificates
1.3.6.1.4.1.11290	1	1	1	1	StampIT Doc Pro
				2	StampIT Server
				3	StampIT Object
				4	StampIT Enterprise
				5	StampIT Doc

3.1 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 Domestic Root CA	1.3.6.1.4.1.11290.1.1
StampIT Domestic CA	1.3.6.1.4.1.11290.1.1.1
StampIT DocPro	1.3.6.1.4.1.11290.1.1.1.1
StampIT Server Certificate	1.3.6.1.4.1.11290.1.1.1.2
StampIT Object Certificate	1.3.6.1.4.1.11290.1.1.1.3
StampIT Enterprise Certificate	1.3.6.1.4.1.11290.1.1.1.4
StampIT Doc Certificate	1.3.6.1.4.1.11290.1.1.1.5

4 Организация

Тази част от документа описва организацията и условията за доверяване на StampIT.

4.1 Инфраструктура на StampIT

StampIT се стреми да поддържа подходяща организация, действаща технология и рамка на публикуваните практики и процедури.

4.2 Спазване на този CPS

StampIT спазва този CPS и другите задължения, които поема при договаряне, когато предоставя услугите си.

4.3 Прекратяване дейността на Удостоверяващия орган

В случай на прекратяване на дейността на Удостоверяващия орган, независимо поради какви причини, StampIT трябва навреме да уведоми и да прехвърли отговорностите си по поддръжката на архивите на приемните страни. Преди да прекрати своята дейност като Удостоверяващ орган, StampIT извършва следните действия:

- информира за намеренията си Комисията за регулиране на съобщенията (КРС) и абонатите, които имат валидни сертификати, най-късно четири месеца преди датата на прекратяване на дейността си;
- прекратява всички сертификати, които все още не са прекратени или са все още валидни в края на четиримесечния период от време, без да иска съгласието на абонатите си;
- уведомява засегнатите абонати за прекратяване на сертификатите им в едномесечен срок от датата на уведомяване на КРС за прекратяване на дейността си;
- извършва необходимите действия за съхранение на архивите в съответствие с този CPS и нормативните изисквания;
- в случай, че StampIT прехвърля дейността си на друг доставчик, StampIT ще се договори с приемната страна за преиздаване на сертификатите от приемната страна, който има всички разрешения, за да извършва това и съблюдава всички всички необходими правила, като неговите действия са поне толкова защитени, колкото тези на StampIT.

4.4 Формат на архивите

StampIT съхранява архивите си на електронни и/или хартиени носители. StampIT може да изиска от Регистриращите си органи, абонатите или техни представители да предоставят документи в съответствие с това изискване.

4.5 Период на съхранение на архивите

StampIT запазва по надежден начин архивите на електронните сертификати и цялата свързана с това документация на StampIT за срок не по-кратък от десет (10) години. Периодът на съхранение започва от датата на изтичане на валидността или прекратяването на сертификата. Такива архиви могат да бъдат съхранявани в електронен или хартиен формат или всякакъв друг подходящ формат.

4.6 Журнали на дейностите

StampIT поддържа по надежден начин журнали на следните събития:

- генериране на ключовете;
- управление на ключовете.

4.7 Одит на основните функции

StampIT позволява да бъде извършен вътрешен одит на инфраструктурата му (различен от посочения в ЗЕДЕП) от лица, упълномощени по определен от него ред. StampIT не е задължен да подписва или одобрява съдържанието, заключенията и препоръките от такива одитни доклади и може да разглежда тези доклади като възможност за допълнително защитаване на удостоверителните услуги. StampIT прилага препоръките по своя преценка, в съответствие с прилаганите вътрешни и публично достъпни политики и процедури.

4.8 Планове за непредвидени случаи и възстановяване след бедствия

За да поддържа целостта на услугите си StampIT внедрява, документира и периодично тества подходящи планове и процедури за непредвидени случаи и възстановяване след бедствия. Такива планове се ревизират и обновяват поне веднъж годишно.

4.9 Наличност на сертификатите на StampIT

StampIT може да предоставя на други страни копия от сертификатите, в които StampIT е субект, а също така и всякакви данни за прекратяване на сертификатите, за да бъде проверен подписа му, посредством неговия сертификат.

4.10 Публикуване на информация за издадени сертификати

StampIT публикува всички издадени сертификати, цялата информация за прекратените сертификати или за валидността на тези сертификати.

4.11 Конфиденциалност на информацията

StampIT съблюдава всички приложими правила за защита на информацията, събирана с оглед на дейността. StampIT приема за конфиденциална информацията, съдържаща се в:

- договор за удостоверителна услуга;
- архиви на заявките за сертификати;
- архиви на транзакции;
- записи на външни и вътрешни одити и доклади;
- планове за непредвидени случаи и възстановяване след бедствия;
- вътрешни проследявания и записи на операциите на инфраструктурата на StampIT, управлението на сертификатите, 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 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.

StampIT може да определи административна такса за обработка при такова разкриване на конфиденциална информация.

4.12 Физическа защита

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.

4.13 Практики за управление на персонала

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

4.13.1 Конфиденциална информация

Всички служители, които имат достъп до информация са длъжни да спазват стриктно изискванията за конфиденциалност.

4.13.2 Декларации за конфиденциалност

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

4.14 Публикуване на информация

Достъп до сертификационните услуги на StampIT и хранилището на StampIT може да бъде получен чрез следните средства за комуникация:

На уеб адрес: http://www.stampit.org/repository/

Чрез E-mail: support@mail.stampit.org

Пощенски адрес:

“Информационно обслужване” АД - StampIT

Ул. "165" 3, ж.к. Изгрев,

1797 София, България

Тел.: + 359 2 9656 2044

Факс: + 359 2 9656 2012

E-mail: support@mail.stampit.org

5 Правила и процедури

Тази част от документа представя правилата и процедурите за PKI услугите на StampIT.

5.1 Изисквания към заявителите на сертификати

Преди или по време на процеса по заявяване на сертификат, заявителите на сертификати извършват следните стъпки:

- подават искане за издаване на сертификат и приемат условията на Договора за удостоверителна услуга и този CPS;
- предоставят доказателства за тяхната идентичност според стандартно определените процедури на StampIT.

5.1.1 Упълномощаване

Заявка за сертификат на StampIT може да бъде направена лично или чрез пълномощник/представител, в зависимост от типа на сертификата и условията за неговото издаване. Упълномощаването се доказва с нотариално заверено пълномощно, документ за актуално състояние и други документи, определящи връзката между упълномощител и пълномощник/представител и неговите права.

5.1.2 Генериране на ключовата двойка

Регистриращите органи на StampIT носят цялата отговорност за безопасното генериране на частната ключова двойка на абоната, когато за целта се използва защитен механизъм за създаване на електронен подпис. В зависимост от типа на сертификата и условията за неговото издаване абонатът може да присъства на процеса по генериране.

5.1.3 Защита на ключовата двойка

Абонатите носят пълна отговорност за предотвратяване на компрометиране, загуба, разкриване, модифициране или друго неоторизирано използване на техния частен ключ.

5.1.4 Делегиране на отговорности за частния ключ

Абонатите носят пълна отговорност за действия или пропуски на упълномощени от тях лица или техни партньори, които те използват за генериране, пазене, съхранение или унищожаване на техните частни ключове.

5.2 Идентифициране на заявителите

Преди издаване на сертификата StampIT определя контроли, които да установят идентичността на бъдещия абонат. Такива контроли се изпълняват от Регистриращите органи на StampIT. Регистриращият орган на StampIT прилага тези процедури на базата на дадените от StampIT указания.

5.3 Потвърждаване на информацията в заявките за издаване на сертификат

Заявките за издаване на сертификати от StampIT са придружени от съответните документи, за да бъде установена идентичността на заявителя, както е описано в информацията за продуктите по-долу.

StampIT може да модифицира изискванията към информацията, касаеща заявката на лицата, за да изпълни своите изисквания, бизнес контекста на употребата на сертификати или препоръките на закона.

Такава документация включва следните елементи за идентификация, в съответствие с типа на сертификата и условията на неговото издаване:

- име на заявителя;
- единен граждански номер;
- име на упълномощения представител и нотариално заверено пълномощно;
- име на Domain (URL);
- наименование на организацията/юридическото лице;
- звено в организацията;
- адрес, град, пощенски код, държава;
- лице за технически контакт и фактуриране или оторизиран представител;
- номер по националния данъчен регистър;
- идентификационен код БУЛСТАТ;
- инсталиран на сървъра софтуер;
- информация за плащане;
- доказателство за правото да се използва името;
- документ за регистриране на компанията;
- документ за актуално състояние, издаден не по-рано от един месец преди подаване на искането за издаване на сертификат, нотариално заверено пълномощно от Ректор или Директор (за учебните заведения), официално писмо от ръководител на държавен орган или орган на местното самоуправление;
- правилно попълнена и подписана бланка за регистрация;
- подписано искане за издаване на сертификат;
- подписан Договор за удостоверителни услуги.

5.4 Изисквания за потвърждаване на заявките за сертификати

При получаване на заявка за даден сертификат, като се базира на предоставената информация StampIT потвърждава следната информация:

- заявителят е същото лице, което е вписано в заявката за сертификат;
- заявителят за сертификат притежава частния ключ, който кореспондира на публичния ключ, включен в сертификата;
- информацията, която трябва да бъде публикувана в сертификата е точна, освен ако не е непотвърдена информация за абоната;
- представителят, който заявява издаване на сертификат, трябва да бъде надлежно упълномощен да направи това.

StampIT контролира точността на публикуваната информация, която се предоставя от абоната, към момента на издаването на сертификата.

Във всички случаи и за всички типове сертификати на StampIT абонатът има постоянното задължение да съблюдава за верността на предоставяната информация и да уведомява StampIT за всякакви промени, настъпили след издаването на сертификата.

5.4.1 Физическо явяване

За да бъде осъществена връзката между абоната и публичния му ключ StampIT изисква физическо явяване на заявителя пред Регистриращ орган за определени типове сертификати.

5.4.2 Потвърждаване на информацията за дадено юридическо лице от трета страна

StampIT може да изиска трета страна да потвърди информацията за юридическото лице, което заявява сертификат. StampIT признава потвърждение от организации, които са трета страна, бази данни на трета страна, включително и на държавни органи, като може да проучи и препоръките на други трети страни, чийто бизнес е свързан с този на заявителя.

Контролите на StampIT може да включват проверка в Търговски Регистри или други бази данни, които потвърждават регистрацията на юридическото лице.

StampIT може да използва всички средства за комуникация, които има на разположение, за да установи идентичността на юридическо лице.

5.4.3 Определяне на сериен номер

Само StampIT има право да определя Relative Distinguished Names (RDNs) и серийните номера, които са включени в сертификатите, издадени от StampIT.

5.5 Време за издаване на сертификат

StampIT полага разумни усилия, за да потвърди информацията в подадените документи за сертификат и да издаде сертификата в срок до 5 работни дни от датата на приемане на документите.

5.6 Удовлетворяване и отхвърляне на заявки за сертификат

След успешно извършване на всички изисквани потвърждения, StampIT удовлетворява заявката за сертификат.

Ако процесът по потвърждаване на заявката за сертификат завърши неуспешно, StampIT отхвърля заявката за сертификат. StampIT незабавно уведомява заявителя и посочва причината за отхвърлянето на заявката. Заявители, чиито заявки са били отхвърлени, могат отново да подадат заявка за издаване на сертификат.

5.7 Издаване на сертификат и съгласие на абоната

StampIT издава сертификата при удовлетворяване на заявката за сертификат. Сертификатът влиза в сила в момента, в който абонатът го приеме. Издаването на сертификат означава, че StampIT е удовлетворил заявката за сертификат.

StampIT издава сертификата в съответствие със съгласието на заявителя. Съгласие за издаване на сертификата се демонстрира като се направи заявка, въпреки че все още не е получено съобщение за приемане на сертификата.

При удовлетворяване на искането за издаване, заявителят приема съдържанието на сертификата.

Доставчикът незабавно публикува издаденият сертификат в поддържания от него регистър.

5.8 Валидност на сертификата

Сертификатите са валидни при издаването им от StampIT и приемането им от абонатите.

5.9 Приемане на сертификата от Абоната

Приема се, че сертификатът е приет от абоната, когато:

- одобрението на абоната е показано на StampIT онлайн или чрез електронно съобщение, изпратено от абоната;
- сертификатът се използва от абоната за първи път;
- след изтичане на 15 дни от датата на издаване на сертификата, ако в този срок абонатът не е направил рекламация относно съдържанието на сертификата.

5.10 Публикуване на издадени сертификати

StampIT публикува копие от издадените сертификати в хранилището си. StampIT може да публикува сертификат в други хранилища, 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 сертификатите си, издадени от StampIT в други хранилища.

5.11 Проверка на електронните подписи

Целта на проверката на електронния подпис е да се установи, че:

- електронният подпис е бил създаден с частен ключ, който кореспондира на публичния ключ, вписан в сертификата на подписващия;
- съобщението не е било променяно след като е било електронно подписано.

5.12 Доверяване на електронни подписи

Крайното решение, дали да се довери или не на електронния подпис изцяло трябва да бъде взето от проверяващия. На електронния подпис може да се има доверие, ако:

- електронният подпис е бил създаден в период, когато сертификатът е бил валиден и това може да бъде проверено като се направи справка за валидността на сертификата;
- доверяването е разумно за дадените обстоятелства.

5.13 Подновяване

Периодът на валидност на StampIT сертификатите е отбелязан в съответното поле на сертификата и той е една година (365 дни) от датата на издаване. Тъй като изискванията за подновяване могат да се различават от тези при първоначално издаване, StampIT публикува и актуализира условията за подновяване на сертификати, издадени от него. Подновяване може да бъде извършено само ако всички данни в сертификата останат непроменени, както в първоначалната заявка.

Подновяването на сертификата се извършва в съответствие с условията действащи към момента на подновяване.

Абонатът трябва постоянно да контролира верността и точността на информацията публикувана в подновения сертификат. Заявка за подновяване трябва да бъде получена от StampIT поне 10 (десет) дни преди датата на изтичане на срока на валидност, вписан в сертификата.

5.14 Съобщение за изтичане на срока на валидност на сертификата

За да бъде запазена възможността на потребителите на електронни сертификати да се подписват електронно, StampIT ще направи всичко възможно да уве-

доми абонатите по електронна поща, приблизително 30 (тридесет) дни преди предстоящото изтичане на срока на валидност сертификата.

5.15 Временно спиране и прекратяване на сертификат

Временното спиране на сертификата цели да бъде временно спряна неговата употреба. Прекратяването на сертификата спира за постоянно действието на сертификата. StampIT временно спира или прекратява действието на електронните сертификати, при:

- наличие на основателни сведения и обстоятелства от които е видно, че има загуба, кражба, промяна, неоторизирано разкриване или друго компрометиране на частния ключ;
- титулярът на сертификата (независимо дали това е StampIT или абоната) е нарушил задълженията си по този CPS;
- изпълнението на някое задължение по този CPS 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 сертификата на абоната;
- по искане на посочени в нормативен акт органи.

5.15.1 Заявка за временно спиране или прекратяване

Абонатът или орган, посочен в нормативен акт може да поиска временно спиране или прекратяване на действието на сертификата. Идентичността на заявителя и представителната му власт ще бъде потвърдена, в зависимост от естеството на изискането действие.

5.15.2 Ефект от временното спиране или прекратяване

За периода на временното спиране или при прекратяването на сертификата валидността му незабавно се счита за прекратена. Действието на сертификата се възобновява с изтичане на срока на спиране, при отпадане на основанието за спиране или по искане на абоната в съответствие с нормативната уредба.

5.15.3 Уведомяване при спиране и прекратяване на сертификат

StampIT уведомява абоната за прекратяване или спиране на сертификата чрез средства за комуникация, които смята за подходящи.

5.16 Процедури за управление на сертификати

5.16.1 Подновяване на StampIT сертификати

Подновяване на сертификата, издаден от StampIT, може да бъде извършено само, ако всички данни в сертификата са непроменени, както в първоначалната заявка за издаване. Съдържанието на подновения сертификат е идентично с това на текущия сертификат с изключение на срока на валидност, който започва да тече от датата на подновяване, вписана в сертификата.

В съответствие с изискванията за подновяване операторът на Регистриращия орган на StampIT може да изиска актуални документи, доказващи точността и верността на информацията, включена в съдържанието на сертификата към текущия момент. Заявителят подписва декларация, че данните предоставени при

първоначално издаване и тези, вписани в сертификата са точни, верни и непроменени към настоящия момент.

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

5.16.1.1 Документи за подновяване на StampIT сертификати:

Документите, които могат да бъдат изискани от абоната включват, но не се ограничават до следното:

1. Съдебно решение за регистрация – оригинал и копие, заверено от заявителя.
2. Документ за данъчна регистрация – оригинал и копие, заверено от заявителя.
3. Документ за регистрация по БУЛСТАТ – оригинал и копие, заверено от заявителя.
4. Удостоверение за актуално състояние, издадено не по-рано от един месец преди подаване на искането за подновяване на сертификат – оригинал и копие, заверено от заявителя.
5. Документ за самоличност (лична карта) на физическото лице, което заявява подновяване на сертификат – оригинал и копие, заверено от заявителя.
6. Нотариално заверено пълномощно, от което произтича представителната власт на физическото лице спрямо юридическото лице – оригинал и копие, заверено от заявителя. Този документ е необходим в случай, че основанието за овластяване не е включено в другите документи за статуса на юридическото лице.
7. Подписано искане за подновяване на сертификат.
8. Документ, удостоверяващ заплащането на услугата.

5.16.1.2 Процедура по подновяване на сертификат

Следните стъпки описват процеса по подновяване на сертификат:

1. Заявителят се явява лично пред Регистриращия орган и подава "Искане за подновяване", придружено с документите за подновяване на сертификат.
2. Проверява се самоличността, съответно идентичността на заявителя и съответствието на данните и обстоятелствата, касаещи абоната към момента на подновяване.
3. Операторът на Регистриращия орган проверява представените документи и подава заявка за подновяване на сертификата до Удостоверяващия орган.
4. Удостоверяващият орган подновява сертификата, който се изпраща обратно на Регистриращия орган.
5. Сертификатът се записва върху смарт карта и тя се предава на абоната.
6. Подновеният сертификат се публикува в поддържаната от StampIT публична LDAP директорийна структура.
7. Приемане на сертификата от абоната – подновеният сертификат се счита за приет с акта на неговото издаване, тъй като съдържанието му е било потвърдено при подаване на "Искане за подновяване" от страна на абоната.

Подновяване на сертификата може да бъде извършено само за сертификати, които са валидни към момента на подаване на заявката към Удостоверяващия орган. По тази причина искането за подновяване трябва да бъде получено в

Регистриращия орган не по-късно от 10 дни преди изтичане на срока на валидност на сертификата.

5.16.2 Прекратяване на сертификат

Прекратяване на действието сертификат се извършва от StampIT след подаване на заявка за прекратяване от страна на Регистриращия орган. За да направи тази заявка операторът на Регистриращия орган е длъжен да се увери в самоличността и представителната власт на заявителя.

5.16.2.1 Основания за прекратяване

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

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

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

5.16.2.2 Документи за прекратяване на StampIT сертификати:

Документите, които могат да бъдат изискани от абоната при подаване на искане за прекратяване на сертификат включват, но не се ограничават до следното:

1. Документ за самоличност (лична карта) на физическото лице, което заявява прекратяване на сертификат – оригинал и копие, заверено от заявителя.
2. За юридически лица – документ, от който произтича представителната власт на физическото лице спрямо юридическото лице – оригинал и копие, заверено от заявителя.
3. Подписано "Искане за прекратяване" на сертификат.

5.16.2.3 Процедура по прекратяване на действието на сертификат

Следните стъпки описват процеса по прекратяване на сертификат:

1. Заявителят се явява лично пред Регистриращия орган и подава "Искане за прекратяване", придружено с документите, доказващи неговата самоличност и представителната му власт.
2. Операторът на Регистриращия орган проверява идентичността на заявителя и представителната му власт към момента на подаване на "Искане за прекратяване".
3. Операторът на Регистриращия орган подава заявка за прекратяване до Удостоверяващия орган.
4. Удостоверяващият орган прекратява сертификата.

5. Прекратеният сертификат се включва в поддържания от StampIT списък с прекратените сертификати, който е публично достъпен на адрес http://www.StampIT.org/CRL/StampIT.crl.

След като е било прекратено действието на сертификата, абонатът може да подаде заявка за издаване на нов сертификат и след заплащане на дължимите такси и успешно завършване на процедурите по издаване да получи нов сертификат от StampIT.

5.16.3 Спиране на действието на StampIT сертификати

Действието на сертификатите, издадени от StampIT, може да бъде спряно при наличие на съответните основания, за необходимият според обстоятелствата срок, но за не повече от 48 часа.

За периода на временно спиране на сертификата, същият се счита за невалиден.

5.16.3.1 Основания за спиране

Действието на сертификати, издадени от StampIT може да бъде спряно само по разпореждане от страна на Комисията за регулиране на съобщенията (КРС) – при непосредствена опасност за интересите на трети лица или при наличие на достатъчно данни за нарушение на закона.

5.16.3.2 Процедура по спиране на действието на сертификати

Следните стъпки описват процеса по спиране на действието на сертификат:

1. Удостоверяващият орган получава издаденото от КРС писмено разпореждане за спиране на сертификат.
2. Удостоверяващият орган спира действието на сертификата, като го включва в списъка с прекратените сертификати, който е публично достъпен на адрес http://www.StampIT.org/CRL/StampIT.crl.
3. Удостоверяващият орган незабавно уведомява абоната за спирането на действието на сертификата.

5.16.4 Възобновяване на действието на сертификат

Действието на сертификата се възобновява с изтичане на срока на спиране, при отпадане на основанието за спиране или по искане на абоната, след като StampIT, съответно КРС се увери, че той е узнал причината за спирането и искането за възобновяване е направено вследствие на узнаването. Удостоверяващият орган възобновява действието на сертификата, като го изважда от списъка с прекратените сертификати. От момента на възобновяване на действието на сертификата, същият се счита за валиден.

5.16.4.1 Основания за възобновяване на действието на сертификат

1. По разпореждане на КРС – когато причината за спирането на действието е разпореждане на КРС.
2. След изтичане на срока на спиране на действието на сертификата.
3. По искане от страна на абоната.

5.16.4.2 Процедура за възобновяване на действието на сертификат

1. По разпореждане на КРС – StampIT получава разпореждането на КРС за възобновяване на действието на сертификата. Удостоверяващият орган възобновява действието на сертификата, като го изважда от списъка на прекратените сертификати.

2. След изтичане на срока на спиране на действието – след изтичане на 48 часа от момента на спиране на действието на сертификата, неговото действие се възобновява автоматично от Удостоверяващият орган, ако до този момент не е получена валидна заявка за прекратяване по реда за прекратяване на действието на сертификата.
3. По искане от страна на абоната – след като StampIT, съответно КРС се увери, че той е узнал причината за спирането и искането за възобновяване е направено вследствие на узнаването. Искането за възобновяване на сертификат може да бъде направено след явяване на заявителя пред Регистриращия орган. Искането за възобновяване на действието на сертификата от страна на абоната се реализира по следната процедура:
    - заявителят се явява лично пред Регистриращия орган и подава "Искане за възобновяване", придружено с документите, доказващи неговата самоличност и представителната му власт;
    - проверява се самоличността на заявителя и представителната му власт;
    - операторът на Регистриращият орган проверява представените документи и подава заявка за възобновяване на сертификата до Удостоверяващия орган;
    - Удостоверяващият орган възобновява действието на сертификата.

От момента, в който Удостоверяващият орган е възобновил действието на сертификата, същият се счита за валиден. Ако в периода на спиране на сертификата в Удостоверяващия орган се получи валидна заявка за прекратяване на действието му, то StampIT прекратява сертификата в съответствие с утвърдените процедури.

6 Правни условия за издаване на сертификат

Тази част на документа описва правните гаранции, основания и ограничения, свързани със сертификатите, издавани от StampIT.

6.1 Представяне на услуги

StampIT представя на всички абонати и доверяващи се страни своите услуги, които са описани по-долу. StampIT запазва правото си да променя тези услуги, както смята за подходящо и в съответствие с изискванията на нормативната уредба.

6.2 Информация, включена чрез препратка в сертификат

StampIT включва чрез препратка във всеки сертификат, който издава следната информация:

- общи условия за предоставяните услуги;
- приложимата политика за сертифициране;
- съдържанието на разширенията, които не са обяснени изцяло в сертификата;
- препратка към регистрацията на доставчика в КРС;
- всяка друга информация, която трябва да бъде включена в поле на сертификата.

6.3 Указатели за включване на информация чрез препратка

StampIT използва URLs (Universal Resource Locators), OIDs (Object Identifiers) или други налични средства, за да включи информация чрез препратка в сертификата.

6.4 Ограничения и отговорности

Сертификатите на StampIT може да включват кратко изявление, описващо ограниченията на отговорностите, ограничение на стойността на транзакциите, които могат да бъдат извършени, период на потвърждаване, предназначение на сертификата и непоемане на отговорности. Такава информация може да бъде показвана и чрез хипервръзка. За да покаже необходимата информация StampIT може да използва:

- полето State – за включване на данни за абоната;
- полето за алтернативно име на издателя (Issuer alternative name) – за типа на сертификата;
- стандартен указател на ресурсите на StampIT за политиката за сертифициране;
- други подходящи полета в съдържанието на сертификата;
- частни или други регистрирани разширения.

6.5 Публикуване на данните от сертификата

StampIT си запазва правото, а абонатът приема, да публикува сертификата или данни от сертификата във всяко достъпно хранилище, като LDAP (Lightweight Directory Application Protocol) директории и списъци с прекратените сертификати-CRL (Certificate Revocation List).

StampIT управлява директории от сертификати с определени характеристики, с цел да се повиши нивото на доверие в предлаганите услуги. Потребителите и

доверяващите се страни трябва да направят справка в тези директории с издадени и прекратени сертификати всеки път, преди да вземат решение дали да се доверят на информацията, описана в сертификата.

6.6 Задължение относно предоставената информация

Във всички случаи и за всички типове сертификати, издадени от StampIT, абонатът (а не StampIT) има постоянното задължение да следи за точността, верността и пълнотата на информацията, предоставена при издаване на сертификата и при настъпване на промени незабавно да уведомява StampIT за това.

6.7 Публикуване на информация

Публичната информация, свързана с дейността на StampIT, може да бъде обновявана периодично. Такива обновявания ще бъдат отбелязвани чрез подходящо номериране на версиите и дата на публикуване за всяка нова версия.

6.8 Намеса в дейността на StampIT

Абонатите, доверяващите се страни и всички останали страни ще се въздържат от наблюдаване, намеса в процесите или реинжинеринг на информационните системи на StampIT, включително в процеса на генериране на ключовете, публичния уеб сайт и хранилищата, освен ако изрично не е разрешено от този CPS или след предварително писмено разрешение от страна на StampIT.

6.9 Стандарти

StampIT приема, че софтуерът на абонатите е съвместим със стандарта X.509v3 и другите приложими стандарти и изпълнява изискванията поставени от този CPS. StampIT не може да гарантира, че софтуерът на абонатите ще поддържа и изпълнява контролите, изисквани от StampIT. При необходимост абонатът трябва да потърси подходяща консултация.

6.10 Ограничения за партньорите на StampIT

Контрагентите на StampIT ще се въздържат от действия, които могат да изложат на опасност, подложат на съмнение или да намалят доверието в услугите и продуктите на StampIT.

6.11 Ограничения на отговорността, определени от StampIT за неговите контрагенти

Мрежата на StampIT може да включва Регистриращи органи, които оперират, подчинявайки се на практиките и процедурите на StampIT. StampIT гарантира целостта на всеки сертификат, издаден от неговия собствен Удостоверяващ орган в рамките на условията, посочени в този CPS на StampIT.

6.12 Секретни части

StampIT използва поделени секретни части, за да защити частния си ключ.

6.13 Избор на криптографски методи

Страните приемат, че те единствени са отговорни и са взели независимо решение в избора на софтуер, хардуер и алгоритми за криптиране/електронен подпис, включително съответните им параметри, процедури и техники, в съответствие с изискванията на нормативната уредба.

6.14 Доверяване на непроверени електронни подписи

Доверяващите се страни трябва да проверяват електронния подпис, като всеки път проверяват валидността на сертификата в директорията на CRL или всяка друга налична директория, която е публикувана от StampIT. Доверяващите се страни са предупредени, че непроверен електронен подпис не може да бъде определен като електронен подпис на абоната.

StampIT информира по подходящ начин доверяващите се страни за употребата и проверката на електронните подписи чрез този CPS и други документи публикувани в неговото публично хранилище.

6.15 Невалидни сертификати

Абонатът на издаден от StampIT сертификат, който абонатът или StampIT не приемат за валиден, няма право да създава електронен подпис, използвайки частния ключ, който кореспондира на публичния ключ, включен в сертификата. В този случай няма условия за доверяване на такъв сертификат.

6.16 Отказ да бъде издаден сертификат

StampIT си запазва правото да откаже да издаде сертификат на всяко лице, което не спазва процедурите по издаване и/или не представи необходимите данни и документи за издаване на сертификат, без да носи каквато и да е отговорност за вреди, които могат да възникнат в следствие на такъв отказ.

6.17 Задължения на абоната

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

- да имат познания за ползване на сертификати и PKI;
- в случаите, когато генерират ключовата двойка, гарантират, че публичният ключ, предоставен на StampIT, кореспондира с използвания частен ключ;
- да предоставят вярна, точна и пълна информация на StampIT;
- да подадат отново заявка за издаване на сертификат, ако на даден етап от подновяването на сертификата се окаже, че предоставената информация се е променила, след като е била първоначално предоставена на StampIT;
- да се запознаят и приемат сроковете и условията на този CPS на StampIT и свързаните с него документи, публикувани в хранилището на StampIT;
- да използват сертификатите, издадени от StampIT само за законни цели и в съответствие с този CPS на StampIT;
- да уведомяват StampIT или Регистриращия орган на StampIT за промени и непълноти в предоставената информация;
- да преустановяват използването на сертификата, ако някаква част от информацията се окаже, че е остаряла, променена, неточна или невярна;

- да преустановяват използването на сертификата, ако същият е с изтекъл срок и да го деинсталират от приложенията или устройствата, в които той е бил инсталиран;
- да предотвратяват компрометиране, загуба, разкриване, модифициране или друго неоторизирано използване на частния ключ, който кореспондира на публичния ключ, публикуван в сертификата;
- да заявят прекратяване на сертификата в случай, че има съмнения относно целостта на издадения сертификат;
- да заявят прекратяване на сертификата в случай, че някаква част от информацията, включена в сертификата се окаже остаряла, променена, неточна или невярна;
- за действия и пропуски на представители, които използват, за да генерират, контролират, управляват или унищожават техния частен ключ;
- да се въздържат от предоставяне пред StampIT на материали, с клеветнически, нецензурен, порнографски, обиден, фанатичен или расистки характер.

6.18 Изявление на абоната при приемане

При приемане на сертификата, абонатът декларира пред StampIT и пред доверяващите се страни, че от момента на приемане на сертификата и след това ще съблюдава, че:

- всички заявления, направени от абоната пред StampIT по отношение на информацията, съдържаща се в сертификата, са точни и верни;
- цялата информация, която се съдържа в сертификата е точна и вярна, като абонатът ще информира незабавно StampIT за всякакви неточности и промени в тази информация;
- сертификатът се използва само за законни цели и в съответствие с този CPS;
- използва StampIT сертификата само във връзка с неговото предназначение;
- абонатът запазва контрола върху частния ключ, използва надеждни системи и предприема разумни мерки, за да предотврати загубата, разкриването, модифицирането или неоторизираната му употреба;
- абонатът е краен потребител и няма право да използва частния ключ, който кореспондира на публичния ключ, записан в сертификата с цел подписване на който и да е сертификат (или всякаква друга форма на сертифициран публичен ключ) или на Списък с прекратените сертификати (CRL) като Удостоверяващ орган, освен ако това не е писмено договорено между абоната и StampIT;
- абонатът приема сроковете и условията на този CPS.

6.19 Задължения на Регистриращите органи на StampIT

Регистриращите органи на StampIT имат следните задължения:

- приемат заявки за издаване и подновяване на сертификати на StampIT в съответствие с този CPS;
- извършват всички действия, които са предписани от процедурите на StampIT и този CPS;
- приемат, проверяват и предоставят на StampIT заявките за прекратяване, спиране и възобновяване на действието на сертификат, издаден от StampIT в съответствие с процедурите на StampIT и този CPS.

6.20 Информация за доверяващата се страна

Страната, която се доверява на сертификат, издаден от StampIT следва да се придържа към следните общопризнати в международната практика правила:

- да има познания за използване на сертификати и PKI;
- да се запознае с ограниченията за използване на сертификати;
- да се запознае с условията на CPS на StampIT;
- да проверява сертификата, издаден от StampIT като използва освен другите допустими средства и CRL (включително StampIT CRL);
- да се доверява на сертификат само до степен, разумна за дадените обстоятелства.

6.21 Точност, вярност и пълнота на информацията

Абонатът носи пълна отговорност за верността, точността и пълнотата на информацията, която предоставя за използване при издаване на сертификата, според този CPS.

6.22 Отговорност на абоната пред доверяващата се страна

Без да бъдат ограничавани другите задължения на абоната, посочени в този CPS, абонатите са отговорни за всякакви неверни изявления, направени от тях в сертификатите пред трети страни, които основателно се доверяват на информацията посочена там, след като са проверили един или повече електронни подписи със сертификата.

6.23 Задължение за наблюдение на представителите на абоната

Абонатът има постоянното задължение да контролира данните, които неговият представител предоставя на StampIT. Абонатът трябва незабавно да уведоми издателя за неточно представяне или пропуск, направен от страна на неговия представител.

6.24 Използване на представители

За сертификати, издадени по заявка на представител на абоната, представителят и абонатът отговарят заедно и поотделно пред StampIT и неговите представители и контрагенти.

6.25 Условия за използване на хранилището и уеб сайта на StampIT

Страните (включително абонати и доверяващи се страни), които имат достъп до хранилището и уеб сайта на StampIT, приемат клаузите на този CPS и другите условия за използване, посочени от StampIT, с изключение на информацията, която се предоставя в демонстрационните, безплатните и тестовите сертификати. Страните приемат условията за използване, когато направят запитване за статуса на сертификата или като използват или се доверяват на предоставената информация или услуги. Условията за използване на хранилището на StampIT включват:

- информация осигурена в следствие на търсене на сертификат;
- осигуряване на възможност за проверка на статуса на електронните подписи, създадени с частния ключ, който кореспондира на публичния, включен в сертификата;
- информация публикувана на уеб сайта на StampIT;

- всякакви други услуги, които StampIT може да рекламира или осигурява чрез неговия уеб сайт.

6.26 Доверяване на собствен риск

Отговорността за оценката и доверяването на информацията в хранилището и уеб сайта на StampIT е на страните, които използват тази информация.

Страните приемат, че са получили необходимата информация, за да решат дали да се доверят на информацията, посочена в сертификата.

6.27 Точност на информацията

StampIT, оценявайки доверената си позиция, полага всички усилия за да осигури на страните, които имат достъп до хранилищата точна, обновена и вярна информация.

6.28 Пропуски при спазване на условията

Неспазването на условията за използване на хранилищата и уеб сайта на StampIT може да доведе до прекратяване на взаимоотношенията между StampIT и съответната страна.

6.29 Задължения на StampIT

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

- спазва този CPS и своите вътрешни или публични политики и процедури;
- спазва приложимото законодателство и подзаконовата нормативна уредба;
- осигурява инфраструктура и сертификационни услуги, включително изграждането и пускането в действие на хранилището и уеб сайта на StampIT за извършване на PKI услугите;
- 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 сертификати;
- издава и подновява сертификати в съответствие с този CPS и изпълнява задълженията си посочени в него;
- при получаване на заявка от Регистриращия орган, издава и подновява сертификати, в съответствие с този CPS;
- при получаване на заявка за прекратяване на сертификат от Регистриращия орган прекратява сертификата, в съответствие с този CPS;
- публикува сертификатите, в съответствие с този CPS;
- осигурява поддръжка на абонатите и доверяващите се страни, както е описано в този CPS;
- прекратява, спира и възобновява сертификатите в съответствие с този CPS;
- осигурява информация за изтичането на срока на валидност и подновяването на сертификатите в съответствие с този CPS;

- предоставя копия от този CPS и действащите си документи за публичен достъп.

StampIT заявява, че няма други задължения по този CPS.

6.30 Съответствие с определеното предназначение

StampIT отхвърля всички гаранции и отговорности, в случай, че продуктите и/или услугите са ползвани не според определеното им предназначение и всякакви гаранции за точността на предоставена, но непотвърдена информация.

6.31 Други гаранции

Освен това, което е посочено в българското законодателство за електронния подпис, StampIT не дава гаранции за:

- точността, автентичността, пълнотата или съответствието на всяка непотвърдена информация, която се съдържа в сертификата или разпространява от StampIT или от негово име, както е посочено в съответното описание на продукта в този CPS на StampIT;
- точността, автентичността, пълнотата или съответствието на всяка информация, която се съдържа в безплатни, тестови или демонстрационни сертификати, издадени от StampIT;
- представяне на информация в сертификат, освен ако не е посочено друго в съответното описание на продуктите в този CPS;
- качеството, функциите или действието на софтуера или хардуерните устройства;
- въпреки, че StampIT има задължения за прекратяването на сертификата, той не носи отговорност, ако не може да го прекрати поради причини, които са извън неговия контрол;
- валидността, точността и наличието на директории с издадени сертификати и списъци с прекратени сертификати, поддържани от трети страни, освен ако това не е посочено изрично от StampIT.

6.32 Непотвърдена информация за абоната

Непотвърдена информация е тази, която е извън обхвата на задължителните данни, включени в съдържанието на сертификата, съгласно чл. 24 на ЗЕДЕП и не може да бъде потвърдена от доставчика въз основа на официални документи или по друг, допустим от закона начин. Обхватът на непотвърдената информация може да включва, но не е ограничен само до:

- E-mail адрес;
- Телефон и/или факс;
- Организационно звено;
- Длъжност на овластеното физическо лице.

6.33 Ограничаване на отговорността на StampIT

Освен в случай на небрежност StampIT не носи отговорност за:

- пропуснати ползи;
- загуба на данни;
- други косвени вреди, произтичащи от или във връзка с използването, доставката, лицензирането, действието или невъзможността за действие на сертификатите и електронните подписи;

- всякакви други вреди, освен тези, които са свързани с доверяване на информацията, посочена в дадения сертификат, базирана на потвърдената информация в сертификата;
- грешка в потвърдената информация, която е в следствие на измама или умишлено невярно изявление на заявителя;
- използването на сертификат, който не е бил издаден или използван в съответствие с този CPS;
- използването на сертификат, който не е валиден;
- използването на сертификат, при което са надвишени определените ограничения, посочени в него или в този CPS;
- сигурността, използването, целостта на продуктите, включително хардуера и софтуера, които абонатът използва;
- компрометиране на частния ключ на абоната.

6.34 Ограничения на вредите

При никакви условия (освен в случай на небрежност) общата отговорност на StampIT към всички страни, включително и без ограничение на абонат, заявител, получател или доверяваща се страна за всички електронни подписи и транзакции, свързани с такъв сертификат, няма да надвишава лимита за такива сертификати, който е определен в този CPS.

6.35 Приложение на CPS

Когато този CPS противоречи на други правила, указания или политики, ще се прилагат условията на този CPS и той ще има задължителна сила за абоната, освен за договори, които са сключени преди публикуване на този CPS.

6.36 Права върху интелектуалната собственост

StampIT или неговите контрагенти притежават правата върху интелектуалната собственост, касаещи базата данни, уеб сайтовете, електронните сертификати на StampIT и всякакви други публикации, които са били извършени от StampIT, включително и този CPS.

6.37 Нарушения и вреди

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 са длъжни да не използват domain и distinguished names с незаконни цели, за нелоялна конкуренция и да не предоставят информация, обърквaща или подвеждаща дадено лице, независимо дали то е физическо или юридическо.

Абонатите са длъжни да обезщетят StampIT от загуби и вреди, които са резултат на всякакви такива нарушения.

6.38 Собственост

Сертификатите са собственост на StampIT. StampIT разрешава сертификатите 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 сертификати, които не трябва да бъдат публикувани в ни-

какви 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 техните лични данни, посочени в сертификата.

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.

6.39 Приложимо законодателство

Този CPS е издаден и се тълкува в съответствие с българското законодателство. Изборът на законодателство е направен, за да гарантира непротиворечиво тълкуване на този CPS, независимо от местоживеенето или седалището на абоната или мястото на използване на сертификатите, или други продукти и услуги, предоставяни от StampIT. Българското законодателство се прилага за всички договорни отношения на StampIT, в които този CPS може да бъде прилаган във връзка с продуктите и услугите на StampIT, когато StampIT действа като доставчик, получател или по друг начин.

6.40 Юрисдикция

Уреждането на всички възникнали спорове, които могат да произлизат от или са във връзка с този CPS или осигуряването на PKI услугите на StampIT ще бъде отнесено пред компетентния за това съд в гр. София.

6.41 Разрешаване на спорове

При възникване на спорове във връзка с издаване, подновяване, спиране или прекратяване на действието на сертификатите на StampIT, заинтересованите лица могат да подават жалби.

Жалбите се подават в писмена форма до изпълнителния директор на "Информационно обслужване" АД чрез началника на отдел "Инфраструктура за удостоверителни услуги – PKI" на адрес гр. София – 1797, р-н "Изгрев", ул. "165" № 3.

В седемдневен срок от подаването на жалбата, началникът на отдел "Инфраструктура за удостоверителни услуги – PKI" изпраща жалбата и писменото си становище по нея на изпълнителния директор на "Информационно обслужване" АД.

Изпълнителният директор на "Информационно обслужване" АД се произнася по жалбата в четиринадесет дневен срок от получаването ѝ, за което писмено уведомява жалбоподателя.

6.42 Правоприемство

Правата и задълженията, посочени в този CPS могат да бъдат прехвърляни от страните по взаимно съгласие, по силата на закона (включително в резултат на преобразуване) или по друг начин, при положение, че такова прехвърляне се предприема в съответствие с условията на този CPS и при условие, че такова прехвърляне няма за последици поемането на други задължения, които прехвърлящата страна дължи на трети страни към момента на прехвърлянето.

6.43 Отделяне на условията

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

ВСЯКА ЕДНА ОТ КЛАУЗИТЕ НА ТОЗИ CPS, 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.

6.44 Тълкуване

Този CPS ще бъде тълкуван в съответствие с общоприетите бизнес практики при дадените обстоятелства и ползването на продукта или услугата по предназначение. При тълкуването на този CPS страните ще имат предвид обхвата и приложението на услугите и продуктите на StampIT и неговата мрежа от Регистриращи органи и принципите на добрата воля и доверие, които се прилагат в търговските отношения.

Заглавията и подзаглавията в този CPS са възприети по този начин само за удобство и справки и не трябва да бъдат използвани при тълкуване или изпълнение на някои от клаузите в този CPS.

Приложенията и определенията в този CPS, са обвързваща и неразделна част от този CPS.

6.45 Отказ от изпълнение

Този CPS ще бъде изпълняван като цяло и ако някое от лицата не успее да изпълни някоя от клаузите на този CPS, то това няма да бъде разглеждано като отказ от бъдещо изпълнение на тази или на други клаузи.

6.46 Уведомяване

StampIT приема съобщения, касаещи този CPS чрез електронно подписани съобщения или на хартиен носител. При получаване на валидно, електронно подписано потвърждение за получаване на електронното съобщение от StampIT, подателят на съобщението приема, че комуникацията е осъществена. Ако подателят не получи такова потвърждение в рамките на 5 (пет) дни, той трябва да изпрати писмено съобщение на хартиен носител чрез куриерски услуги, които ще потвърдят доставката или чрез препоръчано писмо или писмо с обратна разписка, адресирано както следва:

"Информационно обслужване" АД - StampIT

Ул. "165" 3, ж.к. Изгрев,

1797 София, България

Тел.: + 359 2 9656 2044

Факс: + 359 2 9656 2012

E-mail: support@mail.stampit.org

6.47 Такси

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

6.48 Продължаване на действието на CPS

Задълженията и ограниченията, които се съдържат в точките: О*дит на основните функции, Конфиденциалност на информацията, Задължения на StampIT, Ограничаване на отговорностите и Задължения на Абоната* запазват действието си и след отмяната на този CPS.

7 Продукти и услуги, предоставяни от StampIT

7.1 Общи положения

Сертификатите на StampIT предлагат гаранция за идентичността, което изисква физическо явяване пред регистриращите органи при издаване на сертификати на физически лица. При издаване на сертификати на юридически лица или корпоративни клиенти StampIT изисква документи, за да бъде проверена идентичността на юридическото лице, заявяващо сертификат.

Сертификатите на StampIT се издават на физически или юридически лица.

Обичайният срок на валидност на StampIT сертификатите е една (1) година или както е посочено в уеб сайта на StampIT.

7.2 Предоставяни документи за идентифициране на заявителя

Във всички случаи, заявителят трябва да представи пред Регистриращия орган на StampIT, подписана бланка за регистрация, подписано искане за издаване на сертификат, подписан договор за удостоверителна услуга и документ за самоличност, както е отбелязано в процедурата по издаване. В зависимост от типа на сертификата, заявителят трябва допълнително да предостави и документи, идентифициращи юридическо лице, основанието за овластяване и т.н.

StampIT може да поиска и допълнителни доказателства за проверка на идентичността на заявителя и/или юридическото лице.

За сертификати, издавани на физически лица, които са упълномощени да представляват юридически лица, заявителят трябва да предостави пред Регистриращия орган на StampIT подписана бланка за регистрация, искане за издаване на сертификат, подписан договор за удостоверителна услуга, документи за юридическото лице и всички други, изисквани за целта документи.

За сертификати, издавани на държавни органи, организации и учебни заведения, освен документите упоменати по-горе, заявителят трябва да предостави пред Регистриращия орган на StampIT нотариално заверено пълномощно, с което е оторизиран да направи заявката за издаване на сертификат.

7.3 Време за потвърждаване на предоставените данни

StampIT полага усилия да потвърди информацията в заявката за сертификат и да издаде сертификата в разумно време, което може да варира от един (1) до пет (5) работни дни.

7.4 Персонални StampIT Doc сертификати

StampIT Doc сертификати се издават на физически лица и могат да бъдат използвани за идентифициране, защитено изпращане на електронни съобщения и защитени комуникации, достъп до лична финансова информация и онлайн Интернет транзакции от всякакъв вид, като например Интернет абонаментни услуги.

7.4.1 Съдържание

Съдържанието на информацията, публикувана в сертификата може да включва, но не е ограничено до следните елементи:

- e-mail адрес на абоната;
- име на абоната;
- постоянен адрес;

- данни за абоната;
- публичен ключ;
- код на страната;
- издаващ Удостоверяващ орган (StampIT);
- електронен подпис на StampIT;
- вид на алгоритъма;
- срок на валидност на сертификата;
- сериен номер на сертификата.

7.4.2 Документи за издаване на StampIT Doc сертификати:

1. Документ за самоличност (лична карта) на физическо лице, името на което се вписва в съдържанието на сертификата – оригинал и копие, заверено от заявителя.
2. Подписан договор за удостоверителна услуга.
3. Подписано искане за издаване.
4. Попълнена на латиница и подписана бланка за регистрация.
5. Документ, удостоверяващ заплащането на услугата.

7.4.3 Процедура по издаване на сертификат

Следните стъпки описват процеса по заявяване и издаване на сертификат:

1. Заявителят се явява лично пред Регистриращия орган и подава **"Искане за издаване"**, придружено с подписана регистрационна бланка и документите за издаване на сертификат.
2. Проверява се самоличността на заявителя и комплектността на представените документи.
3. Операторът на Регистриращия орган генерира двойката ключове върху смарт картата, в присъствието на абоната и подава заявка за издаване на сертификат до Удостоверяващия орган.
4. Удостоверяващият орган след формален контрол на данните за абоната, издава сертификат, който се изпраща обратно в Регистриращия орган.
5. Сертификатът се записва върху смарт карта и тя се предава на абоната.
6. Абонатът получава софтуер за достъп до смарт картата и се задължава преди първата употреба на сертификата да промени PIN кода за достъп до смарт картата.
7. Данните за активиране на смарт картата (PIN кода) се изпращат на абоната по алтернативен канал – чрез куриер или с препоръчано писмо с обратна разписка на адреса, посочен от заявителя.
8. Издаденият сертификат се публикува в поддържаната от StampIT публична LDAP директорийна структура.

7.4.4 Профил на сертификата:

StampIT Doc Certificate			
Signature Algorithm	Sha1/RSA		
Issuer	CN	StampIT Domestic CA	
	C	BG	
	O	Information Services Plc.	
	OU	StampIT	
Validity	1 Year		
Subject	C	Country	
	L	Locality	
	CN	Common Name	
	E	E-Mail	
	POC	Postal Code	
	STA	Address	
	S	State	EGN:[ЕГН]
	PN	Phone	
Public Key Length/Type	RSA 1024 bits		
Key Usage (Critical)	Digital Signature, Non-Repudiation, Key Encipherment, Data Encipherment		
Issuer Alternative Name (Non Critical)	/OU=Doc Certificate		
Extended Key Usage Field (Non Critical)	Client Authentication, E-Mail Protection		
Authority Key Identifier (Non Critical)	[Issuing Authority Key ID]		
Subject Key Identifier (Non Critical)	[Subject Key ID]		
Basic Constrains (Critical)	No (End Entity)		
CRL Distribution Point (Non Critical)	Custom DP: URL http://www.stampit.org/crl/stampit.crl		
Certificate Policies (Non Critical)	PolicyIdentifier = OID 1.3.6.1.4.1.11290.1.1.1.5 Policy Qualifier Info: Policy Qualifier ID = 1.3.6.1.5.5.7.2.1 Qualifier = http://www.stampit.org/repository/		

7.5 Персонални StampIT DocPro сертификати

StampIT DocPro Сертификати се издават на физически лица, които са упълномощени да представляват юридически лица. Сертификатите могат да бъдат използвани за идентифициране, защитено изпращане на електронни съобщения и защитени комуникации, достъп до лична финансова информация и онлайн Интернет транзакции от всякакъв вид, като например Интернет абонаментни услуги.

7.5.1 Съдържание

Съдържанието на информацията, публикувана в сертификата може да включва, но не е ограничено до следните елементи:

- e-mail адрес на упълномощения представител;
- име на упълномощения представител;
- публичен ключ;
- код на страната;
- наименование на юридическото лице;
- адрес по седалище на юридическото лице;
- данни за юридическото лице;
- издаващ Удостоверяващ орган (StampIT);
- електронен подпис на StampIT;
- вид на алгоритъма;
- срок на валидност на сертификата;
- сериен номер на сертификата.

7.5.2 Документи за издаване на StampIT DocPro сертификати:

1. Съдебно решение за регистрация-оригинал и копие, заверено от заявителя.

2. Документ за данъчна регистрация – оригинал и копие, заверено от заявителя.
3. Документ за регистрация по БУЛСТАТ - оригинал и копие, заверено от заявителя.
4. Удостоверение за актуално състояние, издадено не по-рано от един месец преди подаване на искането за издаване на сертификат – оригинал.
5. Документ за самоличност (лична карта) на физическото лице, което се вписва в съдържанието на сертификата и е упълномощено да представлява юридическото лице – оригинал и копие, заверено от заявителя.
6. Нотариално заверено пълномощно, от което произтича представителната власт на физическото лице спрямо юридическото лице – оригинал и копие, заверено от заявителя. Този документ е необходим в случай, че основанието за овластяване не е включено в другите документи за статуса на юридическото лице.
7. Подписан договор за удостоверителна услуга.
8. Подписано искане за издаване на сертификат.
9. Попълнена на латиница и подписана бланка за регистрация.
10. Документ, удостоверяващ заплащането на услугата.

7.5.3 Процедура по издаване на сертификат

Следните стъпки описват процеса по заявяване и издаване на сертификат:

1. Заявителят се явява лично пред Регистриращия орган и подава "Искане за издаване", придружено с подписана регистрационна бланка и документите за издаване на сертификат.
2. Проверява се самоличността, съответно идентичността на заявителя и комплектността на представените документи.
3. Операторът на Регистриращия орган генерира двойката ключове върху смарт картата, в присъствието на абоната и подава заявка за издаване на сертификат до Удостоверяващия орган.
4. Удостоверяващият орган след формален контрол на данните за абоната, издава сертификата, който се изпраща обратно в Регистриращия орган.
5. Сертификатът се записва върху смарт карта и тя се предава на абоната.
6. Абонатът получава софтуер за достъп до смарт картата и се задължава преди първата употреба на сертификата да промени PIN кода за достъп до смарт картата.
7. Данните за активиране на смарт картата (PIN кода) се изпращат на абоната по алтернативен канал – чрез куриер или с препоръчано писмо с обратна разписка на адреса, посочен от заявителя.
8. Издаденият сертификат се публикува в поддържаната от StampIT публична LDAP директорийна структура.

7.5.4 Профил на сертификата:

StampIT DocPro Certificate			
Signature Algorithm	Sha1/RSA		
Issuer	CN	StampIT Domestic CA	
	C	BG	
	O	Information Services Plc.	
	OU	StampIT	
Validity	1 Year		
Subject	C	Country	
	L	Locality	
	O	Organisation	
	OU	Organisation Unit	
	CN	Common Name	
	E	E-Mail	
	POC	Postal Code	
	STA	Address	
	T	Job Function	
	S	State	B:[БУЛСТАТ] T:[Данъчен номер] C:[Съдебна регистрация] F:[овластяване] EGN:[ЕГН]
	PN	Phone	
Public Key Length/Type	RSA 1024 bits		
Key Usage (Critical)	Digital Signature, Non-Repudiation, Key Encipherment, Data Encipherment		
Issuer Alternative Name (Non Critical)	/OU=DocPro Certificate		
Extended Key Usage Field (Non Critical)	Client Authentication, E-Mail Protection		
Authority Key Identifier (Non Critical)	[Issuing Authority Key ID]		
Subject Key Identifier (Non Critical)	[Subject Key ID]		
Basic Constrains (Critical)	No (End Entity)		
CRL Distribution Point (Non Critical)	Custom DP: URL http://www.stampit.org/crl/stampit.crl		
Certificate Policies (Non Critical)	Policy Identifier = OID 1.3.6.1.4.1.11290.1.1.1.1 Policy Qualifier Info: Policy Qualifier ID = 1.3.6.1.5.5.7.2.1 Qualifier = http://www.stampit.org/repository/		

7.6 Персонални StampIT Enterprise сертификати

StampIT Enterprise сертификати се издават по заявка на корпоративни клиенти на StampIT за физически лица, които са служители на корпоративния клиент. В съдържанието на сертификата е вписано наименованието на юридическото лице, но служителите нямат пълномощия да правят електронни изявления от негово име.

Корпоративният клиент упълномощава свой представител, който подготвя документите за издаване на сертификати, проверява самоличността на служителите и представлява корпоративния клиент пред StampIT.

7.6.1 Съдържание

Съдържанието на информацията, публикувана в сертификата може да включва, но не е ограничено до следните елементи:

- e-mail адрес на служителя;
- име служителя;
- публичен ключ;
- код на страната;
- наименование на юридическото лице;
- адрес по седалище на ЮЛ;
- издаващ Удостоверяващ орган (StampIT);
- електронен подпис на StampIT;

- вид на алгоритъма;
- срок на валидност на сертификата;
- сериен номер на сертификата.

7.6.2 Документи за издаване на StampIT Enterprise сертификати:

1. Съдебно решение за регистрация-оригинал и копие, заверено от заявителя.
2. Документ за данъчна регистрация – оригинал и копие, заверено от заявителя.
3. Документ за регистрация по БУЛСТАТ - оригинал и копие, заверено от заявителя.
4. Удостоверение за актуално състояние, издадено не по-рано от един месец преди подаване на искането за издаване на сертификат – оригинал.
5. Подписан и подпечатан списък с данните за служителите на абоната на хартиен носител и електронен носител, съдържащ данните от бланките за регистрация.
6. Нотариално заверено пълномощно, с което корпоративният клиент е упълномощил свой представител да го представлява пред StampIT за всички действия, свързани с издаването и управлението на сертификатите, издадени на служителите на корпоративния клиент – оригинал.
7. Документ за самоличност (лична карта) на физическото лице по т.6., което е упълномощено да направи заявка за издаване на сертификати – оригинал и копие, заверено от заявителя.
8. Подписан договор за удостоверителна услуга.
9. Подписано искане за издаване.
10. Попълнени на латиница,подписани и подпечатани бланки за регистрация за всеки от служителите, на който се издава сертификат.
11. Документ, удостоверяващ заплащането на услугата.

7.6.3 Процедура по издаване на сертификат

Следните стъпки описват процеса по заявяване и издаване на сертификат:

1. Подписване на договор/споразумение за издаване на сертификати на корпоративен клиент.
2. Упълномощеният представител на корпоративния клиент (заявителят) подава "Искане за издаване", придружено с бланки за регистрация – на електронен и хартиен носител. Всяка страница на хартиеният носител е подписана и подпечатана, а за електронен носител се използва CD ROM (с възможност за еднократен запис).
3. В уговорения срок, след подаване на искането, StampIT издава сертификати на служителите на корпоративния клиент в условията на пакетна обработка на предоставените файлове и списъци с данни за служителите.
4. Сертификатите са с дата на издаване, следваща уговорената дата на предаване на готовите смарт карти на упълномощения представител на корпоративния клиент.
5. Издадените сертификати се публикуват в поддържаната от Удостоверяващия орган публична LDAP директорийна структура.
6. С приемо-предавателен протокол упълномощеният представител на клиента получава издадените на смарт карти сертификати и данните за активиране на смарт картите в именовани и запечатани пликове.

7. Пликовете се предават персонално от упълномощения представител на корпоративния клиент на съответните служители, които са вписани в съдържанието на сертификатите.
8. Корпоративният клиент, чрез неговия упълномощен представител получава софтуер за достъп до смарт картата и задължава служителите си преди първата употреба на сертификата да променят PIN кода за достъп до смарт картата.

7.6.4 Профил на сертификата:

StampIT Enterprise Certificate			
Signature Algorithm	Sha1/RSA		
Issuer	CN	StampIT Domestic CA	
	C	BG	
	O	Information Services Plc.	
	OU	StampIT	
Validity	1 Year		
Subject	C	Country	
	L	Locality	
	O	Organisation	
	OU	Organisation Unit	
	CN	Common Name	
	E	E-Mail	
	POC	Postal Code	
	STA	Address	
	S	State	EGN:[ЕГН]
	PN	Phone	
Public Key Length/Type	RSA 1024 bits		
Key Usage (Critical)	Digital Signature, Non-Repudiation, Key Encipherment, Data Encipherment		
Issuer Alternative Name (Non Critical)	/OU=Enterprise Certificate		
Extended Key Usage Field (Non Critical)	Client Authentication, E-Mail Protection		
Authority Key Identifier (Non Critical)	[Issuing Authority Key ID]		
Subject Key Identifier (Non Critical)	[Subject Key ID]		
Basic Constrains (Critical)	No (End Entity)		
CRL Distribution Point (Non Critical)	Custom DP: URL http://www.stampit.org/crl/stampit.crl		
Certificate Policies (Non Critical)	PolicyIdentifier = OID 1.3.6.1.4.1.11290.1.1.1.4 Policy Qualifier Info: Policy Qualifier ID = 1.3.6.1.5.5.7.2.1 Qualifier = http://www.stampit.org/repository/		

7.7 Сертификат за защитен сървър StampIT Server Certificate

StampIT Server сертификатите са предназначени за защитени комуникации с даден уеб сайт. Заявителят е юридическо лице, което има уеб сайт. Server сертификатите се използват, за да гарантират идентичността на уеб сайта пред посетители и да осигурят конфиденциалност на комуникациите с този уеб сайт. Сертификатите за защитен сървър се издават на юридически лица.

За да осъществи издаването на StampIT Server сертификат, Регистриращият орган работи в пакетен режим. Това е автоматизиран процес за четене на заявките за сертификати и издаване на сертификати.

7.7.1 Съдържание

Съдържанието на информацията, публикувана в сертификата може да включва, но не е ограничено до следните елементи:

- име на сървъра;
- публичен ключ;
- код на страната;
- наименование на юридическото лице;
- издаващ Удостоверяващ орган (StampIT);

- електронен подпис на StampIT;
- вид на алгоритъма;
- срок на валидност на сертификата;
- сериен номер на сертификата.

7.7.2 Документи за издаване на StampIT Server сертификати:

1. Съдебно решение за регистрация-оригинал и копие, заверено от заявителя.
2. Документ за данъчна регистрация – оригинал и копие, заверено от заявителя.
3. Документ за регистрация по БУЛСТАТ - оригинал и копие, заверено от заявителя.
4. Удостоверение за актуално състояние, издадено не по-рано от един месец преди подаване на искането за издаване на сертификата – оригинал.
5. Доказателство за правото на ползване на името на домейн – копие, заверено от заявителя.
6. Нотариално заверено пълномощно, с което юридическото лице е упълномощило свой представител да го представлява пред StampIT за всички действия, свързани с издаването и управлението на сертификата – оригинал.
7. Документ за самоличност (лична карта) на физическото лице, което е упълномощено да представлява юридическото лице пред StampIT – оригинал и копие, заверено от заявителя.
8. Подписан договор за удостоверителна услуга.
9. Подписано искане за издаване.
10. Попълнена на латиница и подписана бланка за регистрация.
11. Документ, удостоверяващ заплащането на услугата.

7.7.3 Процедура по издаване на сертификат

Следните стъпки описват процеса по заявяване и издаване на сертификат:

1. Заявителят, който заявява StampIT Server Certificate от името на юридическо лице, трябва да генерира CSR файл (заявка за подписване на сертификат - Certificate Signing Request) с подходящото приложение. Този процес включва генерирането на ключовата двойка, като се използва съответното програмно осигуряване, предоставяно от софтуера на сървъра.
2. Заявителят съхранява CSR файла, съдържащ публичния ключ от генерираната двойка ключове, на дискета.
3. Заявителят трябва лично да се яви в Регистриращия орган на StampIT.
4. Заявителят предоставя лична информация и информация за юридическото лице, която доказва неговата идентичност и връзката му с юридическото лице
5. След проверка на документите Регистриращият орган на StampIT обработва CSR файла на заявителя и го изпраща в Удостоверяващия орган на StampIT.
6. Удостоверяващият орган на StampIT прави формален контрол на данните, издава и публикува сертификата.
7. Удостоверяващият орган на StampIT изпраща подписания сертификат обратно на Регистриращия орган на StampIT.

8. Операторът на Регистриращия орган на StampIT записва сертификата на носителя, предоставен от заявителя и го предава на упълномощения представител на юридическото лице.

7.7.4 Профил на сертификата:

StampIT Server Certificate		
Signature Algorithm	Sha1/RSA	
Issuer	CN	StampIT Domestic CA
	C	BG
	O	Information Services Plc.
	OU	StampIT
Validity	1 Year	
Subject	C	Country
	L	Locality
	O	Organisation
	OU	Organisation Unit
	CN	Common Name
Public Key Length/Type	RSA 1024 bits	
Key Usage (Critical)	Digital Signature, Non-Repudiation, Key Encipherment, Data Encipherment	
Issuer Alternative Name (Non Critical)	/OU=Server Certificate	
Extended Key Usage Field (Non Critical)	Server Authentication	
Authority Key Identifier (Non Critical)	[Issuing Authority Key ID]	
Subject Key Identifier (Non Critical)	[Subject Key ID]	
Basic Constrains (Critical)	No (End Entity)	
CRL Distribution Point (Non Critical)	Custom DP: URL http://www.stampit.org/crl/stampit.crl	
Certificate Policies (Non Critical)	PolicyIdentifier = OID 1.3.6.1.4.1.11290.1.1.1.2 Policy Qualifier Info: Policy Qualifier ID = 1.3.6.1.5.5.7.2.1 Qualifier = http://www.stampit.org/repository/	

Поради спецификата на издаване на сертификатите за защитен сървър те се издават само от Регистриращия орган в гр. София.

7.8 Сертификати за подписване на обекти StampIT Object Certificate

StampIT Object сертификатите се използват за подписване на обекти, като например софтуер. Сертификатите за подписване на обекти се издават на юридически лица.

7.8.1 Съдържание

Съдържанието на информацията, публикувана в сертификата може да включва, но не е ограничено до следните елементи:

- наименование на юридическото лице;
- данни за юридическото лице;
- публичен ключ;
- код на страната;
- издаващ Удостоверяващ орган (StampIT);
- електронен подпис на StampIT;
- вид на алгоритъма;
- срок на валидност на сертификата;
- сериен номер на сертификата.

7.8.2 Документи за издаване на StampIT Object сертификати:

1. Съдебно решение за регистрация-оригинал и копие, заверено от заявителя.
2. Документ за данъчна регистрация – оригинал и копие, заверено от заявителя.

3. Документ за регистрация по БУЛСТАТ - оригинал и копие, заверено от заявителя.
4. Удостоверение за актуално състояние, издадено не по-рано от един месец преди подаване на искането за издаване на сертификата – оригинал.
5. Нотариално заверено пълномощно, с което юридическото лице е упълномощило свой представител да го представлява пред StampIT за всички действия, свързани с издаването и управлението на сертификата – оригинал.
6. Документ за самоличност (лична карта) на физическото лице, което е упълномощено да представлява юридическото лице пред StampIT – оригинал и копие, заверено от заявителя.
7. Подписан договор за удостоверителна услуга.
8. Подписано искане за издаване.
9. Попълнена на латиница и подписана бланка за регистрация.
10. Документ, удостоверяващ заплащането на услугата.

7.8.3 Процедура по издаване на сертификат

Следните стъпки описват процеса по заявяване и издаване на сертификат:

1. Заявителят се явява лично пред Регистриращия орган и подава "Искане за издаване", придружено с подписана регистрационна бланка и документите за издаване на сертификат.
2. Проверява се самоличността, съответно идентичността на заявителя и комплектността на представените документи.
3. Операторът на Регистриращия орган генерира двойката ключове върху смарт картата в присъствието на абоната и подава заявка за издаване на сертификат до Удостоверяващия орган.
4. Удостоверяващият орган след формален контрол на данните за абоната, издава сертификата, който се изпраща обратно в Регистриращия орган.
5. Сертификатът се записва върху смарт картата и тя се предава на абоната срещу подпис.
6. Абонатът получава софтуер за достъп до смарт картата и се задължава преди първата употреба на сертификата да промени PIN кода за достъп до смарт картата.
7. Данните за активиране на смарт картата (PIN кода) се изпращат на абоната по алтернативен канал – чрез куриер или с препоръчано писмо с обратна разписка на адреса, посочен от заявителя.
8. Издаденият сертификат се публикува в поддържаната от StampIT публична LDAP директорийна структура.

7.8.4 Профил на сертификата:

StampIT Object Certificate		
Signature Algorithm	Sha1/RSA	
Issuer	CN	StampIT Domestic CA
	C	BG
	O	Information Services Plc.
	OU	StampIT
Validity	1 Year	
Subject	C	Country
	L	Locality
	O	Organisation
	OU	Organisation Unit
	CN	Common Name
Public Key Length/Type	RSA 1024 bits	
Key Usage (Critical)	Digital Signature, Non-Repudiation	
Issuer Alternative Name (Non Critical)	/OU=Object Certificate	
Extended Key Usage Field (Non Critical)	Code signing	
Authority Key Identifier (Non Critical)	[Issuing Authority Key ID]	
Subject Key Identifier (Non Critical)	[Subject Key ID]	
Basic Constrains (Critical)	No (End Entity)	
CRL Distribution Point (Non Critical)	Custom DP: URL http://www.stampit.org/crl/stampit.crl	
Certificate Policies (Non Critical)	PolicyIdentifier = OID 1.3.6.1.4.1.11290.1.1.1.3 Policy Qualifier Info: Policy Qualifier ID = 1.3.6.1.5.5.7.2.1 Qualifier = http://www.stampit.org/repository/	

Поради спецификата на издаване на сертификатите за подписване на обекти те се издават само от Регистриращия орган в гр. София.

7.9 Удостоверяване на време

StampIT предоставя на абонатите си услугата по удостоверяване на датата и часа на представяне на електронен документ, който е подписан с частен ключ, съответстващ на публичния ключ в сертификата, издаден от StampIT.

7.9.1 Уверение за абонатите и трети страни

Ползвайки услугата по удостоверяване на датата и часа на представяне на електронен документ, абонатите и трети страни получават уверение за това, че този електронен документ е съществувал в този вид към удостовереното от StampIT време.

7.9.2 Технология

Удостоверяването на датата и часа на представяне на електронен документ се извършва в съответствие с IETF RFC 3161 Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP), след като абонатът подаде електронна заявка на посочен от StampIT IP адрес. Заявката се подава към "Информационно обслужване" АД, като доставчик на удостоверителни услуги и той изпълнява дейностите по удостоверяване на време.

7.10 Списък с прекратени сертификати (CRL)

StampIT поддържа и актуализира на всеки три часа списъка с прекратените сертификати (CRL), които е публично достъпен на адрес http://www.StampIT.org/crl/StampIT.crl.

7.10.1 Профил на списъка с прекратени сертификати:

StampIT CRL		
Version	Version 2	
Issuer Name	CN	StampIT Domestic CA
	C	BG
	O	Information Services Plc.
	OU	StampIT
Effective date	[Date of CRL issuance]	
Next Update	[Next update]	
Signature algorithm	Sha1/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)

7.10.2 Кодове за спиране/прекратяване на сертификати:

1. **Key Compromise** – компрометиран е частния ключ, съответстващ на публичния ключ, включен в съдържанието на сертификата, следователно няма основания за доверяване на този сертификат.
2. **CA Compromise** – компрометиран е частния ключ на Удостоверяващия орган, който се използва за подписване на сертификати на абонатите.
3. **Affiliation Changed** – промени в дружеството/сдружението – субектът, вписан в сертификата вече е с променен статут по отношение на юридическото лице.
4. **Superseded** – сертификатът е заместен от друг сертификат.
5. **Cessation of Operation** – прекратени са дейностите, свързани с първоначалното издаване на сертификата.
6. **Certificate Hold** – действието на сертификата е спряно (сертификатът е невалиден в момента).

8 Ограничение на действието на сертификатите

Този раздел определя специфичните ограничения на действието на сертификатите, във връзка с размера на обезщетенията, дължими от доставчика на удостоверителни услуги, респ. застрахователя, за вреди, настъпили вследствие на издаване и ползване на електронния подпис със сертификати, издадени от StampIT.

Доставчикът отговаря за вреди пред титуляра на усъвършенствания електронен подпис и пред всички трети лица в съответствие с разпоредбата на чл. 29 от ЗЕДЕП.

8.1 Лимити за обезщетение и лимити за транзакции

Посочените максимални лимити на обезщетение в т. 8.8 са и максимални лимити за транзакциите при използване на сертификати на StampIT.

8.2 Абонати

Абонатите на StampIT са физически и/или юридически лица, на които е издаден сертификат от някой от следните видове:

- StampIT Doc Certificate
- StampIT DocPro Certificate
- StampIT Enterprise Certificate
- StampIT Object Certificate
- StampIT Server Certificate

8.3 Безплатни и тестови сертификати

StampIT не носи отговорност за начина на ползване на безплатни и тестови сертификати, които могат да бъдат предоставяни за цели включващи демонстрации, обучение и тестване.

8.4 Предмет на застраховката

Предмет на застраховката на доставчика е отговорността на "Информационно обслужване" АД в качеството му на доставчик на удостоверителни услуги в съответствие с чл. 29 от Закона за електронния документ и електронния подпис.

8.5 Ограничение на действието на сертификатите

StampIT ограничава действието на сертификатите и 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 заявка за прекратяване действието на сертификат 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 удостоверителни услуги" (CPS);
- 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 сертификатите за опериране 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.

8.6 Срок

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.

8.6.1 Период на застраховката

Претенциите по предходната точка трябва да бъдат доведени до знанието на StampIT по време на периода на застраховката. Периодът на застраховката е времето между началната и крайна дата на валидност на сертификата.

8.6.2 Удължаване на периода на застраховката

Застраховката на StampIT покрива също и писмени претенции, които са предявени в StampIT в период от 15 (петнадесет) дни след крайната дата на валидност на сертификата и се основават на вреди, настъпили по време на валидността на сертификата.

8.7 Задължения на абонатите

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.

8.8 Максимален лимит на обезщетение

С цел ограничаване на действието на сертификатите, StampIT определя максимален лимит на обезщетение за претърпени вреди, причинени от използването

на сертификат, издаден от него. Ограниченията са определени според типа на сертификата, както е указано в таблицата по-долу:

Максимален лимит на обезщетение	
StampIT Doc Certificate	40 000 лева
StampIT DocPro Certificate	40 000 лева
StampIT Enterprise Certificate	3 000 лева
StampIT Object Certificate	40 000 лева
StampIT Server Certificate	40 000 лева

При наличие на вреди, превишаващи определения лимит на обезщетение, за който и да е сертификат, на първо място се обезщетяват най-рано постъпилите претенции, докато се постигне окончателното разпределяне. StampIT има право да откаже да изплати сума, надвишаваща максималния лимит на обезщетение за вредите от един сертификат.

Максималният лимит на обезщетение остава непроменен, независимо от броя на абонатите, доверяващите се страни, електронните подписи, размера на транзакциите или претенциите, свързани със сертификата. Максималният лимит на обезщетение се отнася до вреди, причинени на всички абонати, заявители, получатели или доверяващи се страни, които са резултат от доверяване на потвърдена със сертификат на StampIT информация.

8.9 Приложима застраховка

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.

8.10 Форсмажорни обстоятелства

Наличието на форсмажорни обстоятелства, води до отмяна на правата, произтичащи от този CPS.

8.11 Юрисдикция

Уреждането на всички възникнали спорове, които могат да произлизат от или са във връзка с осигуряването на удостоверителните услуги на StampIT, ще бъде отнесено за разрешаване пред компетентния съд в гр. София.

8.12 Приложимо законодателство

За неуредените в настоящият раздел въпроси се прилага българското законодателство.