“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"**

Политика за предоставяне на удостоверителни услуги - StampIT Server Certificate

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

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 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.

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

Доверяващите се страни са физически или юридически лица, които използват удостоверителните услуги 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 Списък с Прекратените Сертификати (CRL), всеки път преди да вземат решение дали да се доверят на информацията посочена в сертификата.

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

Документът "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.

Този документ е публично достъпен и може да бъде намерен на
http://www.StampIT.org/repository/

1.6 Политика за предоставяне на удостоверителни услуги (Certificate policy)

Настоящият документ "Политика за предоставяне на удостоверителни услуги", наричан за по-кратко Certificate policy е публично изявление за политиката на StampIT при издаване на сертификати и видовете услуги предоставяни от него.

Този документ е разработен в съответствие с изискванията на общоприетите международни спецификации и българското законодателство.

Този документ е публично достъпен и може да бъде намерен на
http://www.StampIT.org/repository/

2 Технология

Този раздел описва определени технологични аспекти на услугите предоставяни от StampIT.

2.1 Типове StampIT сертификати

StampIT предлага набор от сертификати и свързани с тях услуги, които могат да бъдат използвани по такъв начин, че да бъдат удовлетворени 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.

2.2 Разширения

2.2.1 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.

2.2.2 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.

2.3 Профили на Сертификатите на StampIT

Профилът на Сертификата може да съдържа полетата, посочени по-долу:

2.3.1 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).

2.3.2 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.

2.3.3 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.

2.4 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

2.5 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

2.6 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

3 Правила за издаване на сертификати

Тази част на документа представя правилата за издаване на сертификати от страна на StampIT.

3.1 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 CPS;
- предоставят доказателства за тяхната идентичност според стандартно определените процедури на StampIT.

3.1.1 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.

3.1.2 Защита на ключовата двойка

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

3.1.3 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.

3.2 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.

3.3 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.

3.4 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, е 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.

3.5 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.

3.6 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.

3.7 Валидност на сертификата

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

3.8 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.

3.9 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.

4 Продукти и услуги, предоставяни от StampIT

4.1 Подновяване на действието на сертификат

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.

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 момента на подновяване. Заявителят подписва декларация, че данните предоставени при първоначално издаване и тези, вписани в сертификата са точни, верни и непроменени към настоящия момент. 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.

За да бъде запазена възможността на потребителите на електронни сертификати да се подписват електронно, StampIT ще направи всичко възможно да уведоми абонатите по електронна поща, приблизително 30 (тридесет) дни преди предстоящото изтичане на срока на валидност сертификата.

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

4.2 Прекратяване на сертификат

Прекратяване на действието на 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.

4.3 Спиране на действието на StampIT сертификати

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

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

4.4 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 ис-

кането за възобновяване е направено вследствие на узнаването. Удостоверяващият орган възобновява действието на сертификата, като го изважда от списъка с прекратените сертификати.

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.

5 Условия за издаване и ползване на сертификати

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

5.1 Представяне на услуги

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

5.2 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.

5.3 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.

5.4 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.

5.5 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.

5.6 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.

5.7 Задължения на абоната

Освен ако в 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 в 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 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 те 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.

5.8 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 CPS.

5.9 Задължения на StampIT

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

- спазва 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 CPS и изпълнява задълженията си посочени в него;
- при получаване на заявка от Регистриращия орган, издава и подновява сертификати, в съответствие с CPS;
- при получаване на заявка за прекратяване на сертификат от Регистриращия орган прекратява сертификата, в съответствие с CPS;
- публикува сертификатите, в съответствие с CPS;
- осигурява поддръжка на абонатите и доверяващите се страни, както е описано в CPS;
- прекратява, спира и възобновява сертификатите в съответствие с CPS;
- осигурява информация за изтичането на срока на валидност и подновяването на сертификатите в съответствие с CPS;
- предоставя копия от CPS и действащите си документи за публичен достъп.

5.10 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.

5.11 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 CPS;
- използването на сертификат, който не е валиден;
- използването на сертификат, при което са надвишени определените ограничения, посочени в него или в CPS;
- сигурността, използването, целостта на продуктите, включително хардуера и софтуера, които абонатът използва;
- компрометиране на частния ключ на абоната.

5.12 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 документа "Практика на доставчика при предоставяне на удостоверителни услуги" (CPS).

5.13 Приложение на Certificate policy

Когато документът Certificate policy противоречи на CPS, ще се прилагат условията на CPS и той ще има задължителна сила за абоната.

5.14 Уведомяване

StampIT приема съобщения, касаещи неговата дейност 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, Изгрев,
1797 София, България
Тел: + 359 2 9656 2044
Факс: + 359 2 9656 2012
E-mail адрес: support@mail.stampit.org

6 StampIT Server сертификати

StampIT Server сертификати се издават по заявка на юридически лица и са предназначени за осигуряване на защитени комуникации с техния уеб сайт. StampIT Server сертификатите се използват, за да гарантират идентичността на уеб сайта пред посетителите и да осигурят конфиденциалност на комуникациите с този уеб сайт. Сертификатите за защитен сървър се издават само 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.

StampIT Server сертификатите имат срок на валидност една година.

6.1 Съдържание

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

- име на сървъра;
- 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.

6.2 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	Organization
	OU	Organization 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/	

6.3 Документи за издаване на StampIT Server сертификати

Следните документи трябва да бъдат представени от заявителя при подаване на искане за издаване на StampIT Server сертификат:

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.

6.4 Издаване на сертификати

Заявителят на StampIT Server сертификат 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. Заявителят трябва да съхрани CSR файла, съдържащ публичния ключ от генерираната двойка ключове, на дискета.

За издаване на StampIT Server сертификат е необходимо упълномощеният представител на юридическото лице (заявителя) да се яви в Регистриращият орган и да представи необходимите документи, относно статуса на юридическото лице и представителната власт на упълномощеният представител.

След проверка на документите Регистриращият орган на StampIT обработва CSR файла на заявителя и го изпраща в Удостоверяващия орган на StampIT. Удостоверяващият орган на StampIT прави формален контрол на данните, издава и публикува сертификата. Операторът на Регистриращия орган на StampIT записва сертификата на носителя, предоставен от заявителя и го предава на упълномощения представител на юридическото лице.

6.5 Информация, вписана в сертификата

Абонатът е длъжен да съблюдава за верността на предоставената информация, да уведомява StampIT за всякакви промени, настъпили след издаване на сертификата и да подаде искане за прекратяване на сертификата при наличие на промени в данните и обстоятелствата, вписани в сертификата.

Абонатите носят пълната отговорност за предотвратяване на компрометиране, загуба, разкриване, модифициране или друго неоторизирано използване на

техния частен ключ. При наличие на съмнения относно настъпване на някое от посочените събития, свързани с компрометиране на частния ключ, абонатите са длъжни да подадат искане за прекратяване на сертификата.

6.6 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

6.6.1 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)

6.6.2 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).