



“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

Правила за издаване на удостоверения за електронен подпис

Версия: 1.02

Дата на публикуване: 17 Март 2003 г.

Съдържание

1	Общ преглед	4
1.1	Доставчик на удостоверителни услуги	4
1.2	Удостоверения за електронен подпис (Електронни сертификати)	4
1.3	Взаимодействие с потребителите за избор на сертификационни услуги	5
1.4	Абонати	5
1.5	Доверяващи се страни	5
1.6	Правила за издаване на удостоверения за универсален електронен подпис (сертификати)	5
1.7	Практика на доставчика при предоставяне на удостоверителни услуги-ПДПУУ (Certification Practice Statement - CPS)	5
2	Технология	7
2.1	Издаване и управление на сертификатите	7
2.2	StampIT директории, хранилище и списък с прекратени сертификати	7
2.3	Надеждни системи	7
2.4	Типове StampIT сертификати	7
3	Правила и процедури	9
3.1	Изисквания към заявителите на сертификати	9
3.2	Идентифициране на заявителите	9
3.3	Изисквания за потвърждаване на заявките за сертификати	9
3.4	Време за издаване на сертификат	10
3.5	Удовлетворяване и отхвърляне на заявки за сертификат	10
3.6	Издаване на сертификат и съгласие на абоната	10
3.7	Валидност на сертификата	10
3.8	Приемане на сертификата от Абоната	10
3.9	Публикуване на издадени сертификати	11
4	Правни условия за издаване на сертификат	12
4.1	Представяне на услуги	12
4.2	Ограничения и отговорности	12
4.3	Публикуване на данните от сертификата	12
4.4	Задължение относно предоставената информация	12
4.5	Публикуване на информация	12
4.6	Стандарти	13
4.7	Отказ да бъде издаден сертификат	13
4.8	Точност, вярност и пълнота на информацията	13
4.9	Задължение за наблюдение на представителите на абоната	13
4.10	Използване на представители	13
4.11	Условия за използване на хранилището и уеб сайта на StampIT	13
4.12	Пропуски при спазване на условията	14
4.13	Нарушения и вреди	14
4.14	Уведомяване	14
4.15	Такси	14
5	Правила за издаване на сертификати	15
5.1	Общи положения	15
5.2	Предоставяни документи за идентифициране на заявителя	15
5.3	Време за потвърждаване на предоставените данни	15

5.4	Персонални StampIT Doc сертификати	15
5.5	Персонални StampIT DocPro сертификати	16
5.6	Персонални StampIT Enterprise сертификати	18
5.7	Сертификат за защитен сървър StampIT Server Certificate	20
5.8	Сертификати за подписване на обекти StampIT Object Certificate	21

Вие можете да изпращате Вашите коментари по този документ 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

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 форматиранни 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 сертификационни 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 (CRL), всеки път преди да вземат решение дали да се доверят на информацията посочена в сертификата.

1.6 Правила за издаване на удостоверения за електронен подпис (сертификати)

Настоящият документ "Правила за издаване на удостоверения за електронен подпис" дава описание на технологията, правните аспекти и правилата и процедурите при издаване на сертификати, включително правилата за установяване на идентичността на титуляра на електронен подпис.

1.7 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.

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

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 трансакции.

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.

3 Правила и процедури

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

3.1.3 Защита на ключовата двойка

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

3.1.4 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.

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 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.

3.4 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.

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.

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

Доставчикът незабавно публикува издаденият сертификат в поддържания от него регистър.

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 Правни условия за издаване на сертификат

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

4.1 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.

4.2 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.

4.3 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.

4.4 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.

4.5 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.

4.6 Стандарти

StampIT приема, че софтуерът на абонатите е съвместим със стандарта X.509v3 и другите приложими стандарти и изпълнява изискванията поставени от 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.

4.7 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.

4.8 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.

4.9 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.

4.10 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.

4.11 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 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.

4.12 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.

4.13 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, объркваща 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.

4.14 Уведомяване

StampIT приема съобщения 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

4.15 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.

5 Правила за издаване на сертификати

5.1 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.

5.2 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 др.

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 представят 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.

5.3 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.

5.4 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 трансакции от всякакъв вид, като например Интернет абонаментни услуги.

5.4.1 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.

5.4.2 Документи за издаване на StampIT Doc сертификати:

1. Документ за самоличност (лична карта) на физическото 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.

5.4.3 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.

5.5 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 трансакции от всякакъв вид, като например Интернет абонаментни услуги.

5.5.1 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.

5.5.2 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.

5.5.3 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.

5.6 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.

5.6.1 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.

5.6.2 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.б., 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.

5.6.3 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 пликосе.

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.

5.7 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.

5.7.1 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.

5.7.2 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.

5.7.3 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.

5.8 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.

5.8.1 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.

5.8.2 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.

5.8.3 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.