ИНФОРМАЦИОННО ОБСЛУЖВАНЕ АД

1504 София
ул. Панайот Волов 2
тел.: 02/ 9420340
факс: 02/ 943 66 07
e-mail: office@is-bg.net

СОФИЯ ЕИК: 831641791 ISO 9001:2008, ISO/IEC 27001:2005 Certified

www.is-bg.net

Условия и ред за използване на универсален електронен подпис

Версия: 2.2
Дата на публикуване: 14.12.2010 г.

Одобрени с решение №1627 от 14.12.2010 г. на Комисията за регулиране на съобщенията

Съдържание

1 Общ преглед 9
1.1 Доставчик на удостоверителни услуги 9
1.2 Удостоверения за универсален електронен подпис 9
1.3 Взаимодействие с потребителите за избор на удостоверителни услуги 10
1.4 Абонати 10
1.5 Доверяващи се страни 10
1.6 Условия и ред за използване на универсален електронен подпис 10
1.7 Практика на доставчика при предоставяне на удостоверителни услуги-ПДПУУ (Certification Practice Statement - CPS) 11
2 Технология на използване на електронния подпис 12
2.1 Предварителна подготовка 12
2.2 Подписване 12
2.3 Идентификация 13
2.4 Проверка на електронен подпис 13
3 Изисквания за съхранение на частния ключ 14
3.1 Физическо съхранение 14
3.2 Възпроизвеждане 14
3.3 Оперативно съхранение на частния ключ 14
3.4 Ключова дума и персонален идентификационен номер (ПИН) 14
3.5 Ползване на частния ключ 14
3.6 Изгубване или унищожаване 15
3.7 Подписване 15
3.8 Криптиране и декриптиране 15
3.9 Криптографски алгоритми 15
3.10 Приложен софтуер 15
4 Статус на УУНЕП 16
4.1 Издаване и валидност на УУНЕП 16
4.2 Приемане на УУНЕП от Абоната 16
4.3 Публикуване на издадени УУНЕП 16
4.4 Доверяване на електронни подписи 16
4.5 Временно спиране и прекратяване на УУНЕП 16
5.1 Административен ред и условия за използване на електронен подпис 18
5.2 Идентичност 18
5.3 Изисквания към заявителите на УУНЕП 19
5.4 Публикуване на данните от УУНЕП 19
5.5 Задължение относно предоставената информация 19
5.6 Публикуване на информация 19
5.7 Стандарти 20
5.8 Избор на криптографски методи 20
5.9 StampIT директории, хранилище и списък с прекратени и спрени удостоверения 20
5.10 Доверяване на непроверени електронни подписи 20
5.11 Списък с прекратени и спрени УУНЕП (CRL) 20
5.12 Задължения на абоната 21
5.13 Точност, вярност и пълнота на информацията 22
5.14 Отговорност на абоната пред доверяващата се страна 22
5.15 Доверяване на собствен риск 22
5.16 Задължения на StampIT 22

5.17 Други гаранции 23
5.18 Права върху интелектуалната собственост 23

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. "Лъчезар Станчев" 13, ж.к. Изгрев,
1797 София, България
Тел.: + 359 2 9656 291
Факс: + 359 2 9656 212
E-mail:support@mail.stampit.org

ТЕРМИНИ

Автор	Автор на електронното изявление - физическото лице, което в изявлението се сочи като негов извършител
Електронен подпис	Електронен подпис е всяка информация, свързана с електронното изявление по начин, съгласуван между автора и адресата, достатъчно сигурен, който: а) разкрива самоличността на автора; б) разкрива съгласието на автора с електронното изявление, и в) защитава съдържанието на електронното изявление от последващи промени
ЗЕДЕП	Закон за електронния документ и електронния подпис
КРС	Комисия за регулиране на съобщенията
НДДУУ	Наредба за дейността на доставчиците на удостоверителни услуги
НИАУУНЕП	Наредба за изискванията към алгоритмите за усъвършенстван електроенен подпис
НРДДУ	Наредба за регистрация на доставчиците на удостоверителни услуги
Наръчник	Документ, съдържащ Практика на доставчика за предоставяне на удостоверителни услуги и Политика на доставчика при предоставяне на удостоверителни услуги
Практика	Практика на предоставяне на удостоверителни услуги за универсален електронен подпис
Политика	Политика на предоставяне на удостоверителни услуги за универсален електронен подпис
РО	Регистриращ орган
УО	Удостоверяващ орган
Титуляр	Титуляр на електронното изявление - лицето, от името на което е извършено електронното изявление.
УЕП	Универсален електронен подпис – има значението на саморъчен подпис по отношение на всички.
УУнЕП	Удостоверение за универсален електронен подпис – електронен документ, издаден и подписан от „Информационно обслужване” АД в качеството му на доставчик на удостоверителни услуги, който

	съдържа: 1. наименованието, адреса, единния идентификационен код на доставчика на удостоверителни услуги, както и указание за националността му; 2. името или фирмата, адреса, данни за регистрацията на титуляра на усъвършенствания електронен подпис; 3. основанието на овластяването, името и адреса на физическото лице (автора), което е овластено да извършва електронни изявления от името на титуляра на усъвършенствания електронен подпис; 4. публичния ключ, който съответства на частния ключ на титуляра на усъвършенствания електронен подпис; 5. идентификаторите на алгоритмите, с помощта на които се използват публичните ключове на титуляра на усъвършенствания електронен подпис и на доставчика на удостоверителни услуги; 6. датата и часа на издаването, спирането, възобновяването и прекратяването на действието; 7. срока на действие; 8. ограниченията на действието на подписа; 9. уникалния идентификационен код на удостоверението; 10. отговорността и гаранциите на доставчика на удостоверителни услуги; 11. препратка към удостоверението за усъвършенствания електронен подпис на доставчика на удостоверителни услуги, както и към регистрацията на доставчика в Комисията за регулиране на съобщенията
УсЕП	Усъвършенстван електронен подпис е преобразувано електронно изявление, включено, добавено или логически свързано със същото електронно изявление, преди преобразуването. Преобразуването се извършва чрез алгоритми, включващи използването на частния ключ на асиметрична криптосистема.
УУсЕП	Удостоверение за усъвършенстван електронен подпис – електронен документ, издаден и подписан от „Информационно обслужване” АД в

	качеството му на доставчика на удостоверителни услуги, удостоверяващ връзката между титуляра/автора на електронния подпис и неговия публичен ключ
RSA Rivers-Shamir-Adelman	Криптографски алгоритъм (асиметричен)
SHA Secure Hash Algorithm	Хеш функция
URL Uniform Resource Locator	Указател на ресурс/уеб адрес
Автор	Автор на електронното изявление - физическото лице, което в изявлението се сочи като негов извършител
Електронен подпис	Електронен подпис е всяка информация, свързана с електронното изявление по начин, съгласуван между автора и адресата, достатъчно сигурен, който: а) разкрива самоличността на автора; б) разкрива съгласието на автора с електронното изявление, и в) защитава съдържанието на електронното изявление от последващи промени
ЗЕДЕП	Закон за електронния документ и електронния подпис
КРС	Комисия за регулиране на съобщенията
НДДУУ	Наредба за дейността на доставчиците на удостоверителни услуги
НИАУУНЕП	Наредба за изискванията към алгоритмите за усъвършенстван електроенен подпис
НРДДУ	Наредба за регистрация на доставчиците на удостоверителни услуги
Наръчник	Документ, съдържащ Практика на доставчика за предоставяне на удостоверителни услуги и Политика на доставчика при предоставяне на удостоверителни услуги
Практика	Практика на предоставяне на удостоверителни услуги за универсален електронен подпис
Политика	Политика на предоставяне на удостоверителни услуги за универсален електронен подпис
РО	Регистриращ орган
УО	Удостоверяващ орган
Титуляр	Титуляр на електронното изявление - лицето, от името на което е извършено електронното изявление.
УУНЕП	Универсален електронен подпис – има значението на саморъчен подпис по отношение на всички.

УУнЕП	Удостоверение за универсален електронен подпис – електронен документ, издаден и подписан от „Информационно обслужване” АД в качеството му на доставчика на удостоверителни услуги, който съдържа: 1. наименованието, адреса, единния граждански номер или единния идентификационен код на доставчика на удостоверителни услуги, както и указание за националността му; 2. името или фирмата, адреса, данни за регистрацията на титуляра на усъвършенствания електронен подпис; 3. основанието на овластяването, името и адреса на физическото лице (автора), което е овластено да извършва електронни изявления от името на титуляра на усъвършенствания електронен подпис; 4. публичния ключ, който съответства на частния ключ на титуляра на усъвършенствания електронен подпис; 5. идентификаторите на алгоритмите, с помощта на които се използват публичните ключове на титуляра на усъвършенствания електронен подпис и на доставчика на удостоверителни услуги; 6. датата и часа на издаването, спирането, възобновяването и прекратяването на действието; 7. срока на действие; 8. ограниченията на действието на подписа; 9. уникалния идентификационен код на удостоверението; 10. отговорността и гаранциите на доставчика на удостоверителни услуги; 11. препратка към удостоверението за усъвършенствания електронен подпис на доставчика на удостоверителни услуги, както и към регистрацията на доставчика в Комисията за регулиране на съобщенията
УсЕП	Усъвършенстван електронен подпис е преобразувано електронно изявление, включено, добавено или логически свързано със същото електронно изявление, преди преобразуването. Преобразуването се извършва чрез

	алгоритми, включващи използването на частния ключ на асиметрична криптосистема.
УУсЕП	Удостоверение за усъвършенстван електронен подпис – електронен документ, издаден и подписан от „Информационно обслужване” АД в качеството му на доставчик на удостоверителни услуги, удостоверяващ връзката между титуляра/автора на електронния подпис и неговия публичен ключ
RSA Rivers-Shamir-Adelman	Криптографски алгоритъм (асиметричен)
SHA Secure Hash Algorithm	Хеш функция
URL Uniform Resource Locator	Указател на ресурс/уеб адрес

1 Общ преглед

Този раздел прави общ преглед на практиките по предоставяне на удостоверителни услуги от „Информационно обслужване” АД.

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 удостоверения за универсален електронен подпис (УУнЕП) на физически или юридически лица. Удостоверяващият орган извършва дейности, които включват издаване, подновяване, спиране и възобновяване, прекратяване на УУнЕП, водене на регистър и осигуряване на достъп до него.

1.1.2 Регистриращи органи

Удостоверяващият орган издава УУнЕП 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 УУнЕП;
- регистрират подадените искания за удостоверителни услуги на StampIT;
- участват във всички етапи при идентифицирането на абонатите, както е определено от StampIT, в зависимост от типа УУнЕП, които 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 УУнЕП;
- регистрират подадените заявки за подновяване, прекратяване, временно спиране и възобновяване на действието на УУнЕП.

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 универсален електронен подпис

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

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

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 удостоверителни услуги

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

1.4 Абонати

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

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

Абонатът е титуляр на електронния подпис, когато УУнЕП е издадено 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 удостоверителните услуги с УУнЕП, издадени от StampIT и се доверяват на тези УУнЕП и/или електронни подписи, които могат да бъдат проверени чрез публичния ключ, записан в УУнЕП на абоната.

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

1.6 Условия и ред за използване на универсален електронен подпис

Настоящият документ "Условия и ред за използване на универсален електронен подпис" дава информация за технологията, условията и реда за използване на електронния подпис и УУНЕП, включително изискванията за съхранение на частния ключ.

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 ПДПУУ, е публично изявление за практиките на StampIT и условията на издаване, временно спиране, прекратяване и т.н. на УУнЕП издадени в йерархията от УУнЕП на StampIT. В съответствие с дейностите на Удостоверяващия орган, тази ПДПУУ е разделен най-общо на следните раздели: Технически, Организационен и Правен.

ПДПУУ е разработен в съответствие с изискванията на общоприетата международна спецификация RFC 3647 и българското законодателство.

2 Технология на използване на електронния подпис

В този раздел е разгледана технологията на получаване, инсталиране и използване на УУНЕП и електронните подписи. Персоналните УУНЕП се издават от StampIT върху смарт карта.

2.1 Предварителна подготовка

Процесът на предварителната подготовка за получаване и инсталиране на УУНЕП и използване на електронния подпис включва следните основни стъпки:

- Подаване на искане за издаване на УУНЕП;
- Проверка на идентичността на заявителя;
- Издаване на УУНЕП от StampIT;
- Получаване на УУНЕП и данните за достъп до смарт картата;
- Инсталиране на УУНЕП на StampIT на персоналния компютър на автора на електрнния подпис;
- Инсталиране на УУНЕП на автора на електронния подпис на персоналния компютър;
- Осигуряване на условия за защита на частния ключ и УУНЕП;
- Избор и инсталиране на приложен софтуер, за ползване на частния ключ и УУНЕП;
- Настройка на приложния софтуер.

2.2 Подписване

В настоящият параграф е разгледан най-често срещания вариант на използване на електронния подпис - за подписване на електронна поща. В общия случай, това става по следния начин:

- въвежда се електронния адрес на адресата на електронното изявление;
- въвежда се темата (Subject) на електронното изявление;
- въвежда се съдържанието на електронното изявление;
- в случай, че е необходимо, към съобщението се добавят избраните от автора файлове;
- авторът избира УУнЕП, за който разполага със съответния частен ключ и с който подписва електронното изявление (при наличие на повече от един персонален УУнЕП);
- подписаното електронно изявление се изпраща на електронния адрес, въведен в началото.

Във всички случаи на подписване на електронни изявления, авторът на електронния подпис трябва стриктно да следва указанията, дадени от разработчика на приложния софтуер и да се съобразява с ограниченията и условията за използване, посочени в нормативната уредба, този документ и CPS на StampIT.

2.3 Идентификация

УУНЕП, издавани от StampIT, могат да се използват за идентификация на клиента при отдалечен достъп до уеб сървър по следния начин:

- С помощта на използвания от абоната браузър се избира мястото, което е обект на отдалечен достъп (най-често URL);
- При осъществяване на връзката със сървъра, от абонатът се изисква да избере и потвърди съответния персонален УУНЕП, които ще използва, за да получи достъп до отдалечените ресурси;
- След успешно приключване на сесията по идентифициране, абонатът получава възможност за достъп до отдалечените ресурси, в съответствие с предоставените му за това права.

2.4 Проверка на електронен подпис

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 УУНЕП на подписващия;
- съобщението не е било променяно след като е било електронно подписано.

При получаване на подписано електронно изявление, преди да вземе решение, дали да се довери на този електронен подпис, адресатът (доверяващата се страна) трябва да извърши най-малко следните действия:

- Да се запознае с принципите и правилата на StampIT за издаване и управление на УУНЕП;
- Да провери (с помощта на приложния софтуер) състоянието на електронния подпис - дали електронното изявление не е променяно след като е подписано от автора;
- Да провери периода на валидност, вписан в УУНЕП на автора на електронното изявление;
- Да провери дали УУНЕП, който е използван за подписване на електронното изявление, е публикуван от StampIT;
- Да изтегли от сайта на StampIT последното копие на публично предоставения Списък с прекратени и спрени УУНЕП (CRL);
- Да инсталира CRL и да актуализира базата данни с прекратени и спрени удостоверения върху локалния компютър, на който се извършва проверката;
- Визуално или автоматично (посредством приложния софтуер) да направи проверка за статуса на УУНЕП - дали в актуалния CRL е включен УУНЕП на автора/титуляра на полученото електронно изявление.

След извършване на посочените стъпки, ако счете за необходимо, адресатът може да предприеме и други, допустими от закона действия, с цел допълнителна проверка, преди да вземе окончателното решение дали да се довери на електронния подпис и УУНЕП. Във всички случаи адресатът трябва да се доверява на електронния подпис и УУНЕП само до степен, разумна за дадените обстоятелства.

3 Изисквания за съхранение на частния ключ

Частният ключ на асиметричната криптографска система трябва да се съхраня- ва в условията на висока степен на сигурност. В настоящия раздел са разгле- дани основните изисквания за съхранение на частния ключ на автора на елект- ронен подпис.

3.1 Физическо съхранение

След генерирането на ключовата двойка върху смарт картата и предоставяне на данните за активиране на смарт картата на абоната, отговорността за физическото опазване на частния ключ се носи изцяло от него. Същото се отнася и за случаите при съхранение на частния ключ във файл. Абонатът трябва да вземе съответните мерки за възпрепятстване на неоторизиран физически достъп до носителя (файла или смарт картата), съдържащ частния ключ. Достъп до носителя трябва да има само автора на електронния подпис, което ще предпази частния ключ и УУНЕП от неоторизиран достъп, издаване или ползване на електронен подпис от друго лице, различно от автора.

3.2 Възпроизвеждане

Съхраняването на частните ключове и УУНЕП във файлове създава предпоставки за бързото им и лесно възпроизвеждане от лице, различно от автора. При съхранение на частния ключ върху смарт карта, той не може да бъде експортиран, но авторът на електронния подпис не трябва да предоставя на други лица възможността за достъп до частния ключ, смарт картата или пре- доставеният му от StampIT електронен файл, съдържащ УУНЕП.

3.3 Оперативно съхранение на частния ключ

В случаите на оперативна работа, когато файлът или смарт картата, върху която се намира частния ключ и УУНЕП не се използва временно, те не трябва да се оставят без надзор на публично достъпно място. Неспазването на това изискване създава предпоставки за компрометиране на частния ключ на абоната.

3.4 Ключова дума и персонален идентификационен номер (ПИН)

Достъпът до частния ключ и предоставения от StampIT УУнЕП е ограничен, посредством ключова дума (парола) или ПИН код. Само и единствено авторът на електронния подпис трябва да знае и да използва ключовата дума за достъп до файла или ПИН кода за достъп до смарт картата. След трикратно въвеждане на погрешен ПИН код, смарт картата се блокира. Авторът на електронния подпис трябва да предприеме необходимите действия, за да предотврати възможността всяко друго лице да получи информация за ключовата дума или ПИН кода.

3.5 Ползване на частния ключ

При всеки случай на ползване на частния ключ и УУНЕП се изисква смарт картата да е поставена в карточетящото устройство. За да се предотврати опасността от неоторизирано ползване на частния ключ и УУНЕП от други лица, картата не трябва да се оставя без надзор в карточетящото устройство. В случай, че персоналният компютър няма да се използва за по-продължителен период от време, смарт картата не трябва да се оставя в четящото устройство и персоналния компютър трябва да се изключи и/или да се вземат адекватни мерки за предотвратяване на възможността за неоторизиран достъп до него със средствата на хардуера и на операционната система.

3.6 Изгубване или унищожаване

При изгубване или унищожаване на частния ключ, авторът загубва възможността за използване на УУНЕП. StampIT не е в състояние да възстанови изгубената или унищожена ключова двойка, тъй като не разполага с възможност за копирането ѝ. Когато тя се генерира върху смарт карта, частният ключ не може по никакъв начин да бъде експортиран от нея. В случаите, когато частният ключ и УУНЕП се съхраняват във файл, StampIT не получава достъп до частния ключ, тъй като електронната заявка за подписване на УУНЕП, която получава от абоната, не съдържа частен ключ. Загубата или унищожаването на частния ключ или смарт картата, върху която е съхранен частния ключ води до невъзможност за по-нататъшно използване на електронния подпис.

3.7 Подписване

При подписване, авторът на електронния подпис ползва частния си ключ и УУНЕП, за да подпише електронното изявление, за съдържанието на което той носи лична отговорност. Авторът на електронния подпис трябва да предприеме необходимите мерки, за да предотврати възможността други лица да получат възможност за достъп до носителя, съдържащ частния ключ, тъй като това ще доведе до компрометиране на частния ключ.

3.8 Криптиране и декриптиране

При криптиране се използва публичния ключ на абоната, а при декриптиране съответстващият на него частен. При осъществяване на операцията по декриптиране на криптиран електронен документ, абонатът ползва за целта частния си ключ. Абонатът и всички заинтересовани лица, трябва да са наясно, че при загуба или унищожаване на частния ключ, с който се декриптират, обработените по този начин електронни документи стават недостъпни.

3.9 Криптографски алгоритми

Ползването на криптографски алгоритми, които не предоставят достатъчно ниво на сигурност за нуждите на абонатите е нарушение на изискванията за сигурност. Към настоящия момент в световната практика се считат за сигурни и се препоръчват за използване RSA алгоритъм за подписване, SHA1 (160bit) за хеширане и 3DES алгоритъм за криптиране на данни. Абонатите трябва да използват само алгоритми с висока степен на сигурност и в съответствие с нормативната уредба, регламентираща тяхната употреба.

3.10 Приложен софтуер

Използването на електронен подпис се извършва посредством софтуерни приложения. Абонатът и доверяващите се страни трябва да използват само лицензиран софтуер с доказан произход, който отговаря на общоприетите в практиката стандарти за информационна сигурност. Ползването на нелицензиран софтуер е нарушение на изискванията за сигурност.

4 Статус на УУНЕП

Този раздел представя правилата за актуализиране и проверка на статуса на УУНЕП, издадени от StampIT.

4.1 Издаване и валидност на УУНЕП

StampIT издава УУНЕП след удовлетворяване на заявката за УУНЕП. УУНЕП са валидни при издаването им от StampIT и приемането им от страна на абонатите.

4.2 Приемане на УУНЕП от Абоната

Приема се, че УУНЕП е приет от абоната при наличието на някоя от следните предпоставки:

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

4.3 Публикуване на издадени УУНЕП

StampIT публикува копие от издадените УУнЕП в хранилището си. StampIT може да публикува УУНЕП 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 своите УУНЕП, издадени от StampIT в други хранилища.

4.4 Доверяване на електронни подписи

Крайното решение, дали да се довери на електронния подпис изцяло трябва да бъде взето от проверяващия при наличието на следните предпоставки:

- електронният подпис е създаден в период, когато УУНЕП е бил валиден, което може да бъде проверено като се направи справка за валидността на УУНЕП;
- проверяващият приема реда и условията, при които е издадено удостоверението на подписващия;
- доверяването е разумно за дадените обстоятелства.

4.5 Временно спиране и прекратяване на УУНЕП

Временното спиране на УУНЕП цели да бъде временно спряна неговата употреба. Прекратяването на УУНЕП спира за постоянно действието на УУНЕП. StampIT временно спира или прекратява действието на електронните УУНЕП, 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 УУНЕП (независимо, дали това е StampIT или абонатът) нарушил задълженията си по CPS;
- изпълнението на някое задължение по 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 компрометира-

на;
- има промяна в информацията, която се съдържа в УУНЕП на абоната;
- по искане на посочени в нормативен акт органи.

4.5.1 Заявка за временно спиране или прекратяване

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

4.5.2 Ефект от временното спиране или прекратяване

За периода на временното спиране или при прекратяването на УУНЕП валидността му незабавно се счита за прекратена. Действието на УУНЕП се възобновява с изтичане на срока на спиране, при отпадане на основанието за спиране или по искане на абоната в съответствие с нормативната уредба. Максималният срок за спиране на едно удостоверение е 48 часа.

4.5.3 Уведомяване при спиране и прекратяване на УУНЕП

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

4.5.4 Прекратяване на УУНЕП

Прекратяване на действието на УУНЕП се извършва от StampIT след пода- ване на заявка за прекратяване от страна на Регистриращия орган. За да нап- рави тази заявка операторът на Регистриращия орган е длъжен да се увери в самоличността и представителната власт на заявителя.

4.5.4.1 Основания за прекратяване

Основанията за прекратяване на действието на УУНЕП 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. Прекратена е представителната власт на физическото лице спрямо юридическото лице, вписано в съдържанието на УУНЕП;
3. Прекратено е дейността на юридическото лице на абоната;
4. При смърт или поставяне под запрещение на абонат - физическото лице.
5. При установяване, че УУНЕП е издаден въз основа на неверни данни.
6. При промяна в информацията, която е подадена първоначално и се съ- държа в УУНЕП на абоната;
7. При неизпълнение на задълженията на абоната по договора за удостоверителна услуга;
8. По искане на абоната, след проверка на самоличността и представител- ната власт на заявителя.

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

4.5.5 Спиране на действието на StampIT УУНЕП

Действието на УУНЕП, издадени от StampIT, може да бъде спряно при наличие на съответните основания, за необходимия според обстоятелствата срок, но за не повече от 48 часа. За периода на временно спиране на УУНЕП, същият се счита за невалиден.

4.5.5.1 Основания за спиране

Действието на УУНЕП, издадени от StampIT може да бъде спряно:

1. По искане на титуляра, респективно автора. Искането може да бъде подадено както в Регистрираш орган на доставчика, така и чрез други средства за комуникация, включително телефон, факс, електронна поща.
2. По искане на лице, за което според обстоятелствата е видно, че може да знае за нарушения на сигурността на частния ключ, като представител, съдружник, служител, член на семейството и др.
3. 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.

4.5.6 Възобновяване на действието на УУНЕП

Действието на УУНЕП 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 УУНЕП, като го изважда от списъка с прекратените УУНЕП. От момента на възобновяване на действието на УУНЕП, същият се счита за валиден.

4.5.6.1 Основания за възобновяване на действието на УУНЕП

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 УУНЕП.
3. По искане от страна на абоната – в случай, че е узнал причината за спирането и искането за възобновяване е направено вследствие на узнаването.

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

5. Правни условия и ред за използване на електронен подпис

Тази част на документа описва правните гаранции, основания и ограничения, свързани със УУНЕП, издавани от StampIT и електронните подписи на абонатите на StampIT.

5.1 Административен ред и условия за използване на електронен подпис

StampIT издава персонални УУНЕП на физически и юридически лица. Физическите лица, които заявяват и ползват УУНЕП от типа StampIT Doc Certificate се ръководят от условията и реда за използване, посочени в този документ и в CPS на StampIT. За електронните подписи и УУНЕП, в съдържанието на които е включено наименованието на юридическото лице, е целесъобразно юридическото лице – титуляр да разработи вътрешен нормативен документ. В рамките на вътрешните правила на юридическото лице, този документ следва да регламентира приложното поле, правата, задълженията и отговорностите на служителите на юридическото лице по отношение на техните електронни изявления и използването от тях на електронния подпис.

5.2 Идентичност

Лицата, които използват електронен подпис и доверяващите се страни трябва да познават правилата и процедурите по определяне на идентичността на абонатите на УУНЕП, издадени от StampIT, което ще им позволи да вземат съответните решения за използване, проверка и доверяване на електронните подписи и УУНЕП.

5.3 Изисквания към заявителите на УУНЕП

Преди или по време на процеса по заявяване на УУНЕП, заявителите на УУНЕП извършват следното:

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

5.3.1 Упълномощаване

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

5.3.2 Генериране на ключовата двойка

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

5.3.3 Защита на ключовата двойка

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

5.3.4 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 пазене, съхранение или унищожаване на техните частни ключове.

5.4 Публикуване на данните от УУНЕП

StampIT си запазва правото, а абонатът приема, да публикува УУНЕП или данни от УУНЕП във всяко достъпно хранилище, като LDAP (Lightweight Directory Application Protocol) директории и списъци с прекратените и спрените УУНЕП -CRL (Certificate Revocation List). StampIT управлява директории от УУНЕП 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 и спрени УУНЕП всеки път, преди да вземат решение дали да се доверят на информацията, посочена в УУНЕП.

5.5 Задължение относно предоставената информация

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

5.6 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.

5.7 Стандарти

Софтуерът на абонатите задължително трябва да е съвместим със стандарта X.509v3 и другите приложими стандарти и да 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.

5.8 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.

5.9 StampIT директории, хранилище и списък с прекратени и спрени удостоверения

Директно или чрез услугите на трети страни, StampIT предоставя публичен достъп и управлява директории с издадени, временно спрени и прекратени УУНЕП. Списъкът с прекратени и спрени УУНЕП (CRL) е такава директория. CRL се актуализира при настъпване на събитие или автоматично на всеки три часа. Потребителите и доверяващите се страни винаги трябва да проверяват директориите с издадените, спрените и прекратените УУНЕП преди да решат, дали да се доверят на информацията, вписана в даден УУНЕП.

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 във връзка с предоставяните от него услуги.

5.10 Доверяване на непроверени електронни подписи

Доверяващите се страни трябва да проверяват електронния подпис, като всеки път проверяват валидността на УУНЕП в директорията на CRL или всяка друга налична директория, която е публикувана от StampIT. 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 CPS и други документи, публикувани в неговото публично хранилище.

5.11 Списък с прекратени и спрени УУНЕП (CRL)

StampIT поддържа и актуализира при настъпване на събитие или автоматично на всеки три часа списъка с прекратените и спрени УУНЕП (CRL), който е публично достъпен на адрес http://www.StampIT.org/crl/.

5.11.1 Профил на списъка с прекратени и спрени УУНЕП:

StampIT CRL		
Version	Version 2	
Issuer Name	CN	
	C	
	O	
	OU	
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	[Date and Time of Revocation]
	Reason code	[Revocation reason code]

5.11.2 Кодове за спиране/прекратяване на УУНЕП:

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

5.12 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 УУНЕП и на PKI;
- да предоставят вярна, точна и пълна информация на StampIT;
- да се запознаят и приемат сроковете и условията на CPS на StampIT и свързаните с него документи, публикувани в хранилището на StampIT;
- да използват УУНЕП, 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 УУНЕП, ако някаква част от информацията се окаже, че е остаряла, променена, неточна или невярна;
- да преустановяват използването на УУНЕП, ако същият е с изтекъл срок и да го деинсталират от приложенията или устройствата, в които той е бил инсталиран;
- да предприемат мерки за 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 УУНЕП в случай, че има съмнения относно целостта на издадение УУНЕП;
- да заявят прекратяване на УУНЕП в случай, че някаква част от информацията, включена в УУНЕП се окаже остаряла, променена, неточна или невярна;
- за действия и пропуски на представители, които използват, за да контролират, управляват или унищожават техния частен ключ;
- да се въздържат от предоставяне пред StampIT на материали, с клевет нически, нецензурен, порнографски, обиден, фанатичен или расистки характер.

5.13 Точност, вярност и пълнота на информацията

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

5.14 Отговорност на абоната пред доверяващата се страна

Абонатите са отговорни за всякакви неверни изявления, направени от тях в УУНЕП пред трети страни, които основателно се доверяват на информацията посочена там, след като са проверили един или повече електронни подписи със УУНЕП.

5.15 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 УУНЕП.

5.16 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 Закона за електронния документ и електронния подпис и подзаконова нормативна уредба, издадена по неговото прилагане;
- 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 механизъм за генериране 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 да предоставя процедурите за заявяване на различните типове УУНЕП;
- издава и подновява УУНЕП в съответствие с CPS и изпълнява задълбенията си посочени в него
- при получаване на заявка от Регистриращия орган, издава и подновява УУНЕП, в съответствие с CPS;
- при получаване на заявка за прекратяване на УУНЕП от Регистриращия орган прекратява УУНЕП, в съответствие с CPS;
- публикува УУНЕП, в съответствие с CPS;
- осигурява поддръжка на абонатите и доверяващите се страни, както е посочено в CPS;
- прекратява, спира и възобновява УУНЕП в съответствие с CPS;
- осигурява информация за изтичането на срока на валидност и подновяванети на УУНЕП в съответствие с CPS;
- уведомява КРС и потребителите си най-късно 4 месеца преди датата на прекратяване – в случай, че възнамерява да прекрати дейността си;
- предоставя копия от CPS и действащите си документи за публичен достъп;

5.17 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 УУНЕП или разпространява от StampIT или от негово име, както е посочено в съответното описание на продукта в CPS на StampIT;
- точността, автентичността, пълнотата или съответствието на всяка информация, която се съдържа в безплатни, тестови или демонстрационни УУНЕП, издадени от StampIT;
- представяне на информация в УУНЕП, освен ако не е посочено другов съответното описание на продуктитъе в CPS;
- въпреки, че StampIT има задължения за прекратяването на УУНЕП, 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 и спрени УУНЕП, поддържани от трети страни, освен ако това не е посочено изрично от StampIT.

5.18 Права върху интелектуалната собственост

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