“СИСТЕМА ЗА ЕЛЕКТРОННИ ПЛАЩАНИЯ БЪЛГАРИЯ/ СЕП БЪЛГАРИЯ” АД

eSign Наръчник за потребителя

Версия 2.1

21.06.2013

СЪДЪРЖАНИЕ

Глава Първа

„Общи положения”

„Система за електронни плащания България/СЕП България” АД (наричано за краткост по-долу СЕП България) е акредитиран доставчик на удостоверителни услуги (ДУУ) съгласно §41 от Закона за изменение и допълнение на Закона за електронния подпис и електронния документ, обн. в Държавен вестник бр. 100 от 2010г.

Този „Наръчник за Потребителя” (Наръчник) обединява “Практиката при предоставяне на удостоверителни услуги” на СЕП България (тук и по-долу споменавана като „Практика”) и „Политиката по предоставяне на удостоверителни услуги” на СЕП България (тук и по-долу споменавана като „Политика”), и детайлизира правилата по отношение на удостоверителната практика на СЕП България, както и описва процесите по предоставяне на удостоверителни услуги и областта на приложение на удостоверенията за електронен подпис, резултат от тези услуги.

I. Характер на документа

Този Наръчник, в едно с Договора, сключен от клиента, формират договорните отношения между СЕП България и съответния клиент, в рамките на които последният получава правото да използва удостоверителните услуги, предоставяни от СЕП България. Наръчникът има характер на Общи условия и е обвързващ за СЕП България, а за съответния клиент – след подписване на конкретния договор за предоставяне на удостоверителни услуги.

Наръчникът е публичен документ за ДУУ и се представя на Комисията за регулиране на съобщенията и на всички заинтересовани страни. Наръчникът, както и всички документи от публичен характер, са достъпни в електронна форма на електронната страницата на СЕП България.

II. Съдържание и детайлност на документа

В качеството си на ДУУ СЕП България, опериращ на територията на Република България, е разработил настоящият „Наръчник за потребителя”, който включва:

- „Практика при предоставяне на удостоверителни услуги”;
- „Политика за предоставяне на удостоверителни услуги”;

Наръчникът е разработен в съответствие със ЗЕДЕП, подзаконовите актове по неговото прилагане и общоприетия международен стандарт RFC 3647 Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework.

Документът „Практика при предоставяне на удостоверителни услуги” описва подробно:

- Обхвата и приложимостта на предлаганите от СЕП България удостоверителни услуги, включително удостоверения за време;
- Технологията за издаване и управление на Удостоверенията за КЕП;
- Формата, сроковете на действие и валидност на издаваните Удостоверения за КЕП;
- Необходимите документи при приемане и проверка на искания за предоставяне на удостоверителни услуги;
- Документите и данните, които се съхраняват от ДУУ при предоставяне на удостоверителни услуги;
- Поддържаните алгоритми за електронен подпис и защита на данните;

- Задълженията и отговорностите на всички страни, участващи в дейността по издаване и управление на Удостоверения за КЕП;
- Правилата и процедурите, които се изпълняват от ДУУ при издаване на Удостоверения за КЕП;
- Правилата и процедурите, които се изпълняват от ДУУ при спиране, прекратяване и възобновяване на Удостоверения за КЕП.

Документът „Политика за предоставяне на удостоверителни услуги" описва политиката на издаване на удостоверения от ДУУ и видовете удостоверителни услуги, предоставяни от СЕП България, включително услугите по издаване на удостоверения за време.

Политиката на СЕП България описва общите правила при изпълнение на дейността на СЕП България по предоставяне на удостоверителни услуги, като определя детайлността и характера на дейността, участниците в удостоверителния процес, техните задължения и отговорности, процедурите по проверка на клиентската информация, областта на приложение на КЕП.

Политиката определя нивото на доверие в издаваните от СЕП България Удостоверения за КЕП Практиката на СЕП България показва по какъв начин се достига и гарантира това ниво на доверие.

III. Срок на действие и прекратяване на действието на документа

1. Срок на действие

Разпоредбите на Наръчника, както и включените в него „Практика при предоставяне на удостоверителни услуги" и „Политика за предоставяне на удостоверителни услуги" са валидни до тяхната промяна или публикуване на информация за невалидността им от СЕП България.

2. Прекратяване действието на документа

Действието на Наръчника се прекратява с прекратяване на дейността на СЕП България като ДУУ.

3. Последствия от прекратяване действието на документа

След прекратяване на действието на Наръчника остават в сила разпоредбите за задълженията на СЕП България за поддържане на архив на документите и удостоверенията в обема и за периода, описани в Практиката.

IV. Уведомяване и комуникация

Съобщения до СЕП България във връзка с дейностите по предоставяне на удостоверителни услуги се отправят писмено на адрес:

„Система за електронни плащания България/СЕП България" АД

ул. „Златовръх" № 1

1164, гр. София

или по електронен път на адрес: esign@sep.bg.

Уведомления до клиентите на СЕП България се изпращат на предоставения от тях в Договора електронен адрес.

В случаите, в които се налага изпращане на писмено съобщение или документи, СЕП България, в зависимост от характера на съобщението или документа, го изпраща по пощата, като писмо с обратна разписка или по куриер.

V. Изменения и допълнения

СЕП България, при необходимост, променя и допълва Наръчника, като информира Комисията за регулиране на съобщенията за всяка настъпила промяна.

Всяка промяна в Наръчника влиза в сила в срок от 7 (седем) дни от нейното публикуване на електронната страница на СЕП България. Промените в Наръчника имат обвързващо действие спрямо всички клиенти и потребители, които към момента на влизане в сила на промените използват предоставени от СЕП България удостоверителни услуги и не заявят тяхното отхвърляне по реда предвиден по-долу.

Всеки клиент има право да иска прекратяване на предоставените от СЕП България удостоверителни услуги с изрично писмено известие в срок от 7 (седем) дни от влизане в сила на промените в Наръчника. Последното не се прилага, когато промените произтичат от приложимото законодателство, от акт на компетенетен орган или предвиждат по-благоприятни клаузи за клиентите.

VI. Разрешаване на спорове

При възникване на спорове във връзка с предоставянето на удостоверителни услуги от СЕП България, заинтересованите лица подават жалби в писмена форма до Изпълнителния директор на СЕП България на следния адрес:

„Система за електронни плащания България/СЕП България" АД

ул. „Златовръх" № 1

1164, гр. София

Жалби от потребителите на СЕП България се подават и по електронен път на адрес: esign@sep.bg. За целта потребителят следва надлежно да подпише своята жалба с валиден КЕП. За получени се считат само жалби, подписани по надлежния ред.

В срок от 30 (тридесет) дни от нейното получаване, жалбата се разглежда и на жалбоподателя се изпраща писмен отговор от Изпълнителния директор.

VII. Приложимо законодателство

За неуредените в настоящия Наръчник въпроси по отношение на предоставяне на удостоверителни услуги се прилага референтното европейско и действащото българско законодателство.

VIII. Допълнителни разпоредби

1. Правоприемство

Правата и задълженията на СЕП България, посочени в този Наръчник, могат да бъдат прехвърляни по взаимно съгласие на страните, по силата на закона, в резултат на преобразуване или по друг начин, при положение, че такова прехвърляне се предприема в съответствие с условията на Наръчника.

2. Тълкуване

При предоставяне на удостоверителни услуги този Наръчник следва да се тълкува в съответствие с референтното действащо законодателство, общоприетите бизнес практики при дадените обстоятелства и ползването на услугите по предназначение.

В случай че някоя от клаузите на настоящия Наръчник се окаже недействителна, това няма да влече недействителност на други клаузи или части от Практиката и Политиката, или да доведе до недействителност на Договора за предоставяне на удостоверителни услуги с клиента. Недействителната клауза ще бъде заместена от съответната норма на ЗЕДЕП и подзаконовите нормативни актове по прилагането му.

3. Форсмажор

Потребителите на удостоверителни услуги, както и СЕП България не носят отговорност за неизпълнение на задълженията си, произтичащи от настоящия Наръчник (доколкото друго не е предвидено в действащото законодателство), дължащо се на непреодолима сила. Страната, за която е възникнала непреодолимата сима, е длъжна незабавно да уведоми другата страна, както и да положи максимална грижа да намали последиците от неизпълнението.

4. Юрисдикция

Всички спорове, възникнали при или по повод осигуряването на удостоверителните услуги от СЕП България, които не могат да бъдат решени по преговорен път между страните, ще бъдат отнасяни за разрешаване пред компетентния съд в гр. София.

5. Нормативна уредба

Отношенията между СЕП България и клиентите на ДУУ, са уредени с настоящия Наръчник в съответствие с/със:

[1] ЗЕДЕП: „Закон за електронния документ и електронния подпис";

[2] НРРДУУ: „Наредба за реда за регистрация на доставчиците на удостоверителни услуги";

[3] НДДУУРНПИПУУ: „Наредба за дейността на доставчиците на удостоверителни услуги, реда за нейното прекратяване и за изискванията при предоставяне на удостоверителни услуги";

[4] НИАСПКЕП: „Наредба за изискванията към алгоритмите за създаване и проверка на квалифициран електронен подпис";

[5] НРУВСДРДУУ: „Наредба №1 от 10.03.2011г. за реда и условията за водене, съхраняване и достъп до регистъра на доставчиците на удостоверителни услуги";

[6] Директива: „Directive 1999/93/EC of the European Parliament and OF the Council, of 13 December 1999, on a Community framework for electronic signatures";

[7] Решение: „Commission Decision of 14 July 2003, On the Publication of Reference Numbers of Generally Recognised Standards for Electronic Signature Products in Accordance with Directive 1999/93/EC of the European Parliament and of the Council"

[8] RFC 3280: „Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile";

[9] RFC 3628: "Requirements for Time-Stamping Authorities";

[10] RFC 3647: „Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework";

[11] RFC 3739: „Internet X.509 Public Key Infrastructure: Qualified Certificates Profile";

[12] ETSI TS 101 456 V1.4.3: "Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates" technical specification (2007-05);

[13] ETSI TS 101 862 V1.3.3: "Qualified Certificate profile" technical specification (2006-01);

[14] ETSI TS 102 023 v.1.2.1: "Policy Requirements for time-stamping authorities"(2003-01);

[15] ANSI X9.79: "Public Key Infrastructure (PKI) - Practices and Policy Framework";

[16] CWA 14167-1: "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1 System Security Requirements".

IX. Определения и съкращения

1. Определения

Използваните в този Наръчник понятия ще имат следното значение:

Автор/Автор на електронно изявление	Физическото лице, което се сочи като извършител на електронно изявление.
Автор/Титуляр на електронен подпис/квалифициран електронен подпис	Авторът/Титулярът, вписан в удостоверението за електронен подпис/квалифициран електронен подпис.
Данни за проверка на подписа	Данни, като кодове и публични криптографски ключове, използвани за проверка на електронния подпис.
Действителен подпис	Електронен подпис, който може да бъде автентикиран чрез валидно Удостоверение за КЕП.
Доверяваща се страна	Получатели на документи, подписани с квалифициран електронен подпис, които предприемат действия, доверявайки се на Удостоверението за съответния квалифициран електронен подпис и/или на електронните подписи, проверени чрез публичния ключ от това удостоверение.

Договор	Договор за удостоверителни услуги между СЕП България и Клиент.
Електронната страница на СЕП България	Електронната страница http://eSign.bg/
Електронно изявление	Изявление в словесна или несловесна форма, представено в цифрова форма чрез общоприет стандарт за преобразуване, разчитане и визуално представяне на информацията.
Заявител	Физическо лице, което подава Искане за удостоверителна услуга.
Идентификаторът на обект (OID)	Уникална поредица от цели числа, която се присвоява на регистриран обект.
Квалифициран електронен подпис (КЕП)	Квалифициран електронен подпис е усъвършенстван електронен подпис, който: • е придружен от издадено от доставчик на удостоверителни услуги удостоверение за квалифициран електронен подпис, отговарящо на изискванията на чл. 24 от ЗЕДЕП и удостоверяващо връзката между автора и публичния ключ за проверка на подписа, и • е създаден посредством устройство за сигурно създаване на подписа.
Клиент	Физическо или юридическо лице, което има сключен със СЕП България Договор за предоставяне на удостоверителни услуги.
Механизъм за проверка на подписа	Конфигуриран софтуер или хардуер, използван за прилагане на данните за проверка на подписа.
Наръчник	„Наръчник за потребителя“
Онлайн	Режим, при който лицето е свързано към мрежа или към сървъра на Интернет доставчик.
Персонален идентифициращ номер (ПИН/PIN)	Поредица от символи, която служи като идентификатор на притежателя на средството за идентификация.
Потребител	Клиент и/или заявител и/или доверяваща се страна.
Пълномощник	Лице, упълномощено от Титуляра/Автора да подаде Искане за удостоверителни услуги, или да предприема други действия, свързани с Договора за удостоверителни услуги или промяна на статуса на издадените Удостоверения за КЕП.
Титуляр/Титуляр на електронно изявление	Физическото/Юридическото лице, от името на което е извършено електронно изявление.
Удостоверение за квалифициран електронен подпис	Удостоверението е електронен документ, издаден и подписан от доставчика на удостоверителни услуги, който може да съдържа: • указание, че удостоверението е издадено за квалифициран

(Удостоверение за КЕП/Удостоверение)	електронен подпис; • наименованието и адреса на ДУУ, както и указание за държавата, в която е установил своята дейност; • името или псевдонима на Автора на електронния подпис; • особени атрибути, свързани с Автора, ако удостоверението се издава за конкретна цел, както и ако доставчикът поддържа политика за издаване на удостоверения с вписване на такива атрибути; • публичния ключ, съответстващ на държания от автора частен ключ за създаване на квалифицирания електронен подпис; • усъвършенстваният електронен подпис на „СЕП България"АД в качеството му на ДУУ; • срока на действие на удостоверението; • ограниченията на действието на подписа по отношение на целите и/или на стойността на сделките, ако удостоверението е издадено с ограничения на удостоверителното действие; • уникалния идентификационен код на удостоверението; • указание за акредитацията на доставчика.
Удостоверителен процес	Действията по издаване и управление на удостоверение за квалифициран електронен подпис, услугите по валидация на удостоверения за квалифицирани електронни подписи, както и действията на доверяващите се страни във връзка с удостоверенията за квалифицирани електронни подписи.
Удостоверителни услуги	Услугите по издаване, подновяване, модификация, спиране, възобновяване, прекратяване и поддръжка на удостоверение за квалифициран електронен подпис, както и услугите по валидация на удостоверение за квалифициран електронен подпис и услугите по удостоверяване на време.
Устройство за сигурно създаване на електронен подпис (SSCD)	Механизъм за създаване на електронен подпис, който отговаря на изискванията на чл. 17, ал. 1 ЗЕДЕП.
Усъвършенстван електронен подпис	Усъвършенстван електронен подпис е електронен подпис, който: • дава възможност за идентифициране на автора; • е свързан по уникален начин с автора; • е създаден със средства, които са под контрола единствено на автора, и • е свързан с електронното изявление по начин, който осигурява установяването на всякакви последващи промени.
Online Certificate Status Protocol (OCSP)	Интернет протокол за on-line проверка на статуса на издадено удостоверение за електронен подпис.

2. Съкращения

Използваните в настоящия Наръчник съкращения ще имат следното значение:

ДУУ	Доставчик на удостоверителни услуги
ЕП	Електронен подпис
КЕП	Квалифициран електронен подпис
Политика	Политика за предоставяне на удостоверителни услуги
Практика	Практика при предоставяне на удостоверителни услуги
РО	Регистриращ орган
УД	Удостоверителна дейност
УЕП	Удостоверение за електронен подпис
УО	Удостоверяващ орган
УсЕП	Усъвършенстван електронен подпис
УУ	Удостоверителни услуги
OID	Object Identifier
OCSP	Online Certificate Status Protocol
SEP ROOT CA	Базов удостоверяващ орган на СЕП България
eSign QES CA	Оперативен удостоверяващ орган на СЕП България
SSCD	Устройство за сигурно създаване на електронен подпис
TSA	Time Stamp Authority

Глава Втора

„Практика при предоставяне на удостоверителни услуги„

I. Общ преглед

„Практиката при предоставяне на удостоверителни услуги“ е основна част от документите за дейностите на Удостоверяващия орган и регистриращите органи, клиентите и доверяващите се страни.

Удостоверителните услуги на СЕП България се предоставят чрез йерархия от Удостоверяващи органи, подписващи типовете издавани Удостоверения за КЕП, обектите за удостоверяване на време и резултата от онлайн проверката за статуса на Удостоверенията за КЕП.

СЕП България има един оперативен удостоверяващ орган, йерархично разположен под базовия удостоверяващ орган. Оперативният удостоверяващ орган подписва различните типове Удостоверения за КЕП, издавани от ДУУ

– СЕП България и удостоверението за онлайн валидация. Базовият удостоверяващ орган подписва оперативния удостоверяващ орган и удостоверението за валидация на удостоверено време.

Удостоверения за КЕП, издадени от СЕП България, включват в съдържанието си идентификатор на политиката, според която са издадени.

II. Страни в удостоверителния процес

„Практиката при предоставяне на удостоверителни услуги“ е общ регламентиращ документ по отношение на всички участници в процеса по предоставяне на удостоверителни услуги от СЕП България и описва процеса по предоставяне на удостоверителни услуги, взаимодействието между РО, УО, клиенти и доверяващи се страни. Практиката е водещ документ и при осъществяване на проверки на дейността на ДУУ и се отнася до дейността на Удостоверяващите органи – SEP Root CA, eSign QES CA и Регистриращите органи – от една страна, а от друга – до отношенията с Авторите/Титулярите, вписани в Удостоверения за КЕП и с Доверяващите се страни.

СЕП България предоставя удостоверителни услуги на всички юридически и физически лица, приемащи правилата и практиките, описани в този документ. Прилагането на тези правила и практики има за цел да осигури декларираните нива на сигурност при предоставяне на удостоверителни услуги.

1. Удостоверяващи органи

СЕП България предоставя удостоверителни услуги чрез йерархия от удостоверяващи органи и мрежа от регистриращи органи, като издава и управлява Удостоверения за КЕП.

СЕП България, в качеството си на ДУУ, публикува информация за статуса на Удостоверенията за КЕП и я предоставя на доверяващите се страни за целите на проверка на КЕП.

1.1.Базов удостоверяващ орган

SEP Root CA издава базов усъвършенстван електронен подпис (УсЕП) на себе си и оперативни усъвършенствани електронни подписи на други УО, принадлежащи на йерархията от УО на СЕП България. SEP Root CA функционира на база на УсЕП, издаден от самия него. В този УсЕП не се включва OID за политиката, спрямо която се издават и управляват УсЕП. Липсата на идентификатор на политиката следва да се тълкува като липса на ограничения по отношение на политиката, спрямо която УО – SEP Root CA издава удостоверения.

SEP Root CA е изходната точка на доверие за всички потребители на удостоверителни услуги на СЕП България. Това означава, че удостоверителния път за всеки издаден КЕП в йерархията на ДУУ започва от УсЕП на УО – SEP Root CA.

Базовият УО на СЕП България – SEP Root CA издава УсЕП за:

- Себе си – SEP Root CA;
- Оперативния УО – eSign QES CA;
- SEP TSA – удостоверението за проверка на обекти с удостоверено време (TimeStamp).

1.2. Оперативен удостоверяващ орган

Оперативен УО на СЕП България е eSign QES CA. Оперативният УО издава Удостоверения за КЕП в съответствие с „Политика за предоставяне на удостоверителни услуги” на СЕП България на физически или юридически лица.

Оперативният УО включва в издадените Удостоверения за КЕП идентификатори на обекти, за да идентифицира издадените удостоверения от определен тип, в съответствие с тази политика. Идентификаторите на обекти са:

SEP Bulgaria JSC	SEP Root CA	eSignQES CA	Обект/Типове удостоверения	
1.3.6.1.4.1.30299	2	5	1	eSign Qualified Private
			2	eSign Qualified Organization
			3	eSign Qualified Profession
			5	eSign OCSP

Удостоверенията за КЕП, издавани от оперативния УО, съдържат идентификатор на политиката, спрямо която са издадени.

- Оперативният УО издава Удостоверението за проверка на онлайн отговора за статуса на издадено удостоверение за електронен подпис (OCSP)s.

SEP TimeStamp удостоверения за време се издават на физически и на юридически лица – потребители на УУ. Удостоверението за време има официална удостоверителна сила след вписването му във воденият от СЕП България Регистър, достъпен на адрес http://tsa.sep.bg

Удостоверението включва идентификатор на политика посочен в таблицата:

Обект	идентификатор на политика
SEP TSA	1.3.6.1.4.1.30299.2.1.5

Оперативният удостоверяващ орган eSign QES CA, издава удостоверение за електронен подпис, което се използва за проверка на обекти за онлайн проверка на статуса на Удостоверение за КЕП. Удостоверението включва идентификатор на политика посочен в таблицата:

Обект	идентификатор на политика
eSign OCSP	1.3.6.1.4.1.30299.2.5.5

2. Регистриращи органи

Регистриращите органи са част от инфраструктурата на СЕП България в качеството му на ДУУ. РО представляват СЕП България при контакт с клиентите и функционират според правата, делегирани им от УО по отношение на проверка на идентичността съответно самоличността на Автора/Титуляра и регистриране на постъпилите искания за издаване или управление на Удостоверенията за КЕП.

ДУУ издава Удостоверения за КЕП след извършване на проверка на самоличността, съответно идентичността на заявителите на удостоверителни услуги. В тази връзка СЕП България предоставя услугите си чрез мрежа от Регистриращи органи, които имат следните функции:

- Приемат, проверяват, одобряват или отхвърлят Исканията за издаване на Удостоверения за КЕП;
- Приемат, проверяват, одобряват или отхвърлят Исканията за управление на Удостоверения за КЕП;
- Участват във всички етапи при идентифицирането на Заявителите, Авторите и Титулярите на удостоверителни услуги и проверка на самоличността, съответно на тяхната идентичност;
- Сключват договори за предоставяне на УУ по издаване, поддръжка и управление на удостоверения за КЕП с Титулярите от името на СЕП България;
- Извършват други дейности, свързани с предоставяне на удостоверителни услуги описани в политиките, практиките и процедурите на ДУУ.

Регистриращите органи действат от името на СЕП България, в съответствие с неговите политики, практики и процедури.

РО приема, проверява и одобрява или отхвърля Искания за издаване на Удостоверения за КЕП, модификация, подновяване, спиране/възобновяване и прекратяване на Удостоверенията за КЕП.

При проверка на идентичността, съответно самоличността на Титуляра/Автора, операторите на РО пряко или непряко идентифицират лицата, на които ще се издават Удостоверения за КЕП, като използват методи за идентификация, даващи същата степен на сигурност като при физическата идентификация.

СЕП България сключва договор с РО (в случаите, когато конктетният РО е звено извън правно-организационната структура на СЕП България), по силата на който се извършват дейностите, описани по-горе, като „Наръчника за потребителя“ на ДУУ е част от този договор.

Всяко лице може да функционира като РО на ДУУ – СЕП България, след като заяви това и изпълни условията, произтичащи от регламентиращите документи на ДУУ.

Списъкът на РО, които са оторизирани от СЕП България, е публичен и е достъпен на електронната страница на СЕП България.

3. Потребители

Потребители на удостоверителните услуги на СЕП България са клиенти и доверяващи се страни.

1.1. Автор

Автор на електронното изявление - физическото лице, което в изявлението се сочи като негов извършител.

1.2. Титуляр

Титуляр на електронното изявление - лицето, от името на което е извършено електронното изявление.

1.3. Разграничаване на Титуляр и Автор

При издаване на Удостоверение за КЕП на физическо лице, Авторът и Титулярът, вписани в Удостоверението съвпадат.

При издаване на Удостоверение за КЕП на юридическо лице, в Удостоверението като Титуляр се вписва юридическото лице, а като Автор – съответното лице, което е овластено да използва издаденото Удостоверение.

1.4. Доверяващи се страни

Доверяващи се страни са получатели на документи, подписани с КЕП, които предприемат действия, доверявайки се на Удостоверението за съответния КЕП. Доверяващата се страна е отговорна за проверката на валидността на Удостоверението за КЕП. Решението за приемане на автентичността на електронно изявление, подписано с КЕП се взима от доверяващата се страна всеки път при получаване на такова.

Доверяващите се страни преценяват дали типът на Удостоверението за КЕП и гаранциите, свързани с него, са достатъчни за целите, за които се използва. Отговорност на Титуляра е познаването на изискванията на доверяващата се страна и ползването на съответстващ на съответните изисквания тип Удостоверение за КЕП.

III. Предоставяни удостоверителни услуги от СЕП България – обхват и приложимост

СЕП България издава удостоверения за квалифициран електронен подпис, удостоверения за време и удостоверения за електронен подпис, използвани за проверка на обекти.

1. Удостоверения за квалифициран електронен подпис

Удостоверенията за квалифициран електронен подпис могат да се използват за установяване авторството на електронни изявления, като придават на електронния подпис значението на саморъчен подпис по отношение на всички, включително и държавен орган или орган на местното самоуправление

Удостоверенията за квалифицирани електронни подписи, издавани от СЕП България, са следните видове: eSignQualified Private, eSign Qualified Organization и eSign Qualified Profession.

2. eSign Qualified Private удостоверение (eSign за физически лица)

Удостоверение от типа eSign Qualified Private се издава само и единствено на физически лица и се използва за потвърждаване съгласието/самоличността на физическо лице при участие в електронен обмен, като Web-базирани приложения, подписване на електронни документи и/или договори, банкови транзакции и извършване на изявления по смисъла на ЗЕДЕП. При този вид удостоверения за КЕП Авторът и Титулярът са едно и също лице.

3. eSign Qualified Organization удостоверение (eSign за юридически лица)

Удостоверение от типа eSign Qualified Organisation се издава на юридически лица и се използва за потвърждаване на съгласието/самоличността, съответно на идентичността, на юридическо лице при участие в електронен обмен, като Web-базирани приложения, подписване на електронни документи и/или договори, банкови транзакции и извършване на изявления по смисъла на ЗЕДЕП. Титулярът и авторът се различават, като авторът е физическо лице (овластено от закона или чрез съответно изрично пълномощно от юридическото лице да извършва изявленията от името и за сметка на Титуляра), а Титулярът - юридическо.

Авторът върши изявленията от името и за сметка на Титуляра.

4. eSign Qualified Profession удостоверение (eSign за свободни професии)

Удостоверение от типа eSignQualified Profession се издава на физически лица и се използва за потвърждаване на съгласието/самоличността и професионална принадлежност на лице, извършващо услуги с личен труд или упражняващо свободна професия, при участие в електронен обмен, като Web-базирани приложения, подписване на електронни документи и/или договори, банкови транзакции и извършване на изявления по смисъла на ЗЕДЕП. Титулярът и Авторът на изявленията са едно и също лице.

5. SEP TSA удостоверение (Удостоверяване на време)

Удостоверение от типа SEP TSA се използва за потвърждаване времето на представяне на електронен подпис, създаден за определен електронен документ.

Удостоверението за време е подписан от ДУУ електронен документ, който съдържа:

- Идентификатора на политиката за издаване на удостоверения за време, съдържаща се в този Наръчник;
- Представения на доставчика електронен подпис на подписания електронен документ;
- Идентификаторите на алгоритмите, използвани за създаването на електронния подпис;
- Времето на представяне на електронния подпис;
- Уникалния идентификационен номер на удостоверението за време;
- Удостоверението за квалифицирания електронен подпис на ДУУ.

IV. Използвани приложения

Удостоверения за КЕП, издадени в съответствие с Наръчника, могат да се използват с приложения, които отговарят най-малко на следните изисквания:

- Приложенията по подходящ начин управляват частните и публичните ключове, както и тяхното използване;
- Удостоверението за КЕП и асоциираните публични ключове, се използват в съответствие с определеното предназначение, одобрено от СЕП България;
- Имат вграден механизъм за проверка статуса на Удостоверението за КЕП, удостоверителната верига и контрол на валидността (например на подписи, на време и др.);
- Използват алгоритми, определени в „Наредба за изискванията към алгоритмите за създаване и проверка на квалифициран електронен подпис";
- Предоставят подходяща информация за Удостоверенията за КЕП и самото приложение на автора.

Информация за приложенията, с които могат да се използват Удостоверенията за КЕП, издадени от СЕП България, се публикува на електронната страница на СЕП България.

СЕП България не носи отговорност за използване на издадените Удостоверения за КЕП с приложения, неотговарящи на изискванията, описани по-горе.

V. Публичен регистър и информация

СЕП България в качеството си на Доставчик на удостоверителни услуги води публичен електронен регистър (Регистър), в който публикува удостоверенията на УО от своята йерархия, издадените удостоверения за КЕП и информация, необходима на страните, ползващи удостоверителните услуги.

1. Публикувана информация

СЕП България публикува следната информация:

- Списък с Удостоверения за електронен подпис от своята йерархия;
- Списък на издадените Удостоверения за КЕП;
- Списък на издадените удостоверения за време;
- Списък на прекратените Удостоверения за КЕП (CRL);
- Предишни и актуални версии на документите, регламентиращи дейността на ДУУ;
- Наръчник за потребителя;
- Инструкции, описващи начина на използване на електронен подпис;
- Ценови листи за услугите, предоставяни от ДУУ;
- Друга информация, която може да се променя и модифицира в реално време.

2. Периодичност на публикуване на информацията

СЕП България поддържа информацията, посочена по-горе, като я актуализира със следната периодичност:

- Наръчник за потребителя – съобразно, описаното в Глава Първа, раздел V, изискванията на ЗЕДЕП и подзаконовите му нормативни актове;
- Списъците на издадените и прекратените удостоверения на базовия УО – при всяко настъпило събитие или автоматично, най-малко веднъж годишно, когато в рамките на този период не е настъпило събитие по издаване, спиране, възобновяване или прекратяване;
- Списъците на издадените и прекратените Удостоверения за КЕП на оперативния УО – при всяко настъпило събитие или автоматично, на всеки всеки 3 часа, когато в рамките на този период не е настъпило събитие по издаване, спиране, възобновяване или прекратяване;
- Друга информация – при промяна.

3. Достъп до публичния регистър

СЕП България води публичен електронен регистър (Регистър) на издадените от него Удостоверения с X.500 и LDAP базиран достъп.

Достъпът до Регистъра и съдържащата се в него информация е публичен.

Авторът, вписан в Удостоверение за КЕП има правото да ограничи достъпа до информацията в издаденото му Удостоверенеие, като посочи това при подаване на Искане за удостоверителни услуги. Когато достъпът е ограничен, СЕП България предоставя само следната информация от съдържанието на удостоверението:

- Сериен номер на Удостоверението;
- Срок на действие на Удостоверението;
- Статус на удостоверението.

Достъпът до информацията за Удостоверенията от списъка на прекратени удостоверения не се ограничава по никакъв начин.

4. Пазене на публичния регистър

СЕП България пази своя Регистър по начин, който осигурява следното:

- Въвеждането на данни да се извършва само от надлежно овластени служители;
- Извършването на промени на данните да не е възможно;
- Възможността за непозволена намеса да е сведена до минимум.

VI. Използвани имена

1. Тип на имената

Удостоверенията за КЕП, издавани от СЕП България, отговарят на стандарт X.509 v3 и следващите версии. ДУУ проверява и одобрява имената на Титуляра/Автора в съответствие със стандарта X.509 v3. Базовото име на Титуляра/Автора, включено в удостоверението, съответства на нотацията за Distinguished Name, според препоръки X.500 и X.520.

За да осигури лесна комуникация по електронен път с Титуляра/Автора, СЕП България включва в съдържанието на Удостоверението за КЕП електронен адрес в съответствие с RFC822.

Имената на директориите, където се съхраняват удостоверенията за електронен подпис, "Списъкът на прекратените удостоверения" и „Политиката по предоставяне на удостоверителни услуги", както и имената на CRL's distribution points, са в съответствие с RFC1738 и схема за имена според протокола LDAP – RFC 1778.

Издаваните от СЕП България Удостоверения за КЕП съдържат информация, както е определено в чл. 24 от ЗЕДЕП.

Списъкът с данните, които се включват в Удостоверенията за КЕП и тяхната интерпретация е в съответствие с X.509 v3 и е представена в глава „Профили на удостоверения, "Списък на прекратените удостоверения" и OCSP".

2. Смисъл на имена

Удостоверенията за КЕП, издавани от СЕП България съдържат уникални имена с общоразбираема семантика, позволяваща определянето на Доставчика (Issuer Distinguished Name)и идентичността на клиента (Subject Distinguished Name).

Удостоверенията на удостоверяващите органи на Доставчика съдържат уникални имена, идентифициращи Доставчика, субект на удостоверението.

Имената, включени в клиентския Distinguished Name, съдържат идентифициращата информация за Автора/Титуляра.

Съдържанието на Distinguished Name се одобрява/присвоява и проверява от РО в зависимост от Автора/Титуляра и типа удостоверение и се одобрява от УО.

Distinguished Name съдържа набор от полета, чието описание и абревиатури на имената е в съответствие с препоръките RFC 3280 и X.520.

Distinguished Name на Титуляра/Автора се потвърждава от оператора на РО.

Детайлна спецификация и описание на информацията и съответните полета за различните типове удостоверения се съдържат по-долу в настоящия Наръчник.

3. Правила за интерпретиране на различните именни форми

Интерпретацията на имената на полетата в Удостоверенията за КЕП, издадени от СЕП България, е в съответствие с различните типове на Удостоверенията (профили на Удостоверенията). При създаването и

интерпретирането на различните Distinguished Name се прилагат общите правила, посочени по-долу в раздел VI на настоящия Наръчник.

4. Уникалност на имената

За да осигури уникалност на издадените Удостоверения за КЕП, СЕП България присвоява уникален шестнадесетцифрен сериен номер за всяко издадено удостоверение. Серийният номер в комбинация с Issuer Distinguished Name, прецизно и по уникален начин го идентифицира. Също така СЕП България гарантира уникалност на имената и за публичния електронен регистър.

5. Търговски марки

Клиентите нямат право да заявяват издаване на удостоверения с използване на имена, които са обект на авторски или сродни права на трети лица, нито да нарушават чужди имуществени или неимуществени права. Притежателите на такива права удостоверяват това свое право с представяне на съответния надлежен документ пред РО в процеса по представяне на Искане за издаване на съответното Удостоверение. СЕП България не носи отговорност, когато използвани имена в издадените Удостоверения за КЕП нарушават чужди права върху търговско име, търговска марка, домейни, авторски права и др. Клиентите носят отговорност пред ДУУ за всички претърпени от последния вреди във връзка с нарушения на изискванията на тази т.5.

VII. Правила и процедури при предоставяне и използване на удостоверителни услуги

1. Идентификация и автентикация

Този раздел представя общите правила за проверка на самоличността, съответно на идентичността, на Автора и на Титуляра, прилагани от ДУУ, при предоставяне на удостоверителни услуги. Правилата се различават в зависимост от типа информация, която се включва в Удостоверенията. ДУУ е задължен да осигури точността и верността на тази информацията в момента на издаване на Удостоверение за КЕП (първоначална идентификация/автентикация) и при постъпване на Искане за управление на Удостоверение за КЕП (последваща идентификация/автентикация).

1.1. Първоначална идентификация и автентикация на лицето

Първоначална проверка на идентичността, съответно на самоличността на Титуляра и на Автора се осъществява при:

- Първоначално подаване на Искане за удостоверителни услуги пред РО;
- Регистрация за заявяване на удостоверителни услуги през електронната страница на СЕП България.

1.1.1. Първоначална идентификация и автентикация на лицето пред РО

1.1.1.1. Проверка на идентичността на юридически лица – Титуляри на КЕП

РО изисква представянето на подходящи документи, които по категоричен начин и без никакво съмнение потвърждават идентичността на юридическото лице, посочено в съответното Искане за издаване на Удостоверение, което ще бъде вписвано като Титуляр в Удостоверението и на физическото лице, което представлява юридическото, вписвано като Автор в Удостоверението. Документите по предходното изречение включват:

- Документ за самоличност на Автора (оригинал и заверено от Автора копие, като копието остава при РО);
- Документ за съдебна регистрация на юридическото лице (оригинал и заверено от Титуляра копие, като копието остава при РО) – доколкото такъв е приложим с оглед вида на юридическото лице;
- Документ за регистрация по идентификационен номер (БУЛСТАТ) (оригинал и заверено от Титуляра копие, като копието остава при РО) – доколкото такъв е приложим с оглед вида на юридическото лице;
- Удостоверение за актуалното състояние на юридическото лице, издадено в срок до един месец от датата на подаване на заявка за удостоверителни услуги (оригинал и заверено от Титуляра копие, като копието остава при РО);
- Документ по образец на ДУУ за изрично упълномощаване на Автора с представителна власт от Титуляра, в случай че основанието на представителната власт не следва от закона (оригинал, който остава при РО);
- Нотариално заверено пълномощно на заявителя на удостоверителни услуги, в случай че Титулярът упълномощи свой представител, различен от Автора, да заяви удостоверителни услуги.

РО може да провери необходимите данни за идентификация на Титуляра сам, като използва публични регистри, като това право не отменя задължението на лицата за представяне на посочените по-горе документи.

Проверката на идентичността на юридическото лице може да се осъществи като:

- Упълномощен представител на юридическото лице лично посети офис на РО;
- Оператор на РО посети седалището на юридическото лице;
- Оператор на РО използва непряк метод на идентификация, даващ същата степен на сигурност, както при пряка физическа идентификация.

Ако проверката на идентичността е успешна, оператор на РО преминава към обработка на данните на юридическото лице и съответните дейности по предоставяне на удостоверителни услуги.

1.1.1.2. Проверка на самоличността/идентичността на физически лица – Титуляри на КЕП

РО изисква представянето на подходящи и надлежни документи, които по категоричен и безспорен начин потвърждават съществуването и самоличността на физическото лице, което се вписва като Автор и съответно Титуляр в Удостоверението, както и принадлежността му към определена категория лица, упражняващи свободна професия, ако исканото Удостоверение изисква това. Документите по предходното изречение включват:

- Документ за самоличност на Автора (оригинал и заверено от Автора копие, като копието остава при РО);
- Нотариално заверено изрично пълномощно по образец на ДУУ на заявителя на удостоверителни услуги, в случай, че Авторът упълномощи свой представител да заяви удостоверителни услуги;
- Надлежен документ, доказващ по безпорен начин принадлежността на лицето, посочено като Титуляр към съответната професионална/браншова организация (когато исканите удостоверителни услуги са за ползването на Удостоверение от типа SEP Qualified Profession (оригинал и заверено от Автора копие, като копието остава при РО)

Проверката на самоличността на физическо лице може да се осъществи като:

- Физическото лице (упълномощен представител на лицето) лично посети РО;
- Представител на РО посети физическото лице посочено в Искането;
- Оператор на РО използва непряк метод даващ същата степен на сигурност на идентификацията, както при пряка физическа идентификация.

Ако проверката е успешна, оператор на РО преминава към обработка на данните на физическото лице и съответните дейности по предоставяне на удостоверителни услуги

1.1.2. Първоначална идентификация и автентикация на лицето при регистрация за заявяване на удостоверителни услуги по електронен начин

Регистрацията включва предоставянето на данни за заявителя на удостоверителни услуги по електронен начин, които позволяват на СЕП България да го индивидуализира. Данните по предходното изречение включват:

- Три имена и псевдоним, и/или
- Лични данни за заявителя, и/или
- Валиден електронен адрес, който да бъде използван впоследствие за комуникация със заявителя.

Предоставената информация при първоначалната регистрация се съхранява от СЕП България и може да се ползва при приемане на искания за удостоверителни услуги от ДУУ.

При валидация на събраните данни лицето може да премине към следващи стъпки по заявяване на удостоверителни услуги.

1.2. Последваща идентификация и автентикация на лицето

Последваща проверка на идентичността, съответно на самоличността на Титуляра и на Автора се осъществява при:

- Подаване на последващи искания за удостоверителни услуги към РО;
- Иницииране на процес по заявяване на удостоверителни услуги по електронен начин, след извършена първоначална регистрация.

1.2.1. Последваща идентификация и автентикация пред РО

Последваща идентификация и автентикация пред РО се извършва при заявяване на управление на съществуващи удостоверителни услуги.

За извършване на идентификация и автентикация, РО прави проверка на първоначално автентикираните данни за клиента по реда на т. 1.1.1. от този раздел и данните, посочени в новото Искане.

1.2.2. Последваща идентификация и автентикация при регистрация по електронен начин

Последваща идентификация и автентикация на лицето се извършва от PKI на СЕП България при заявяване на удостоверителни услуги. Искане за удостоверителни услуги може да се подаде от първоначално регистриран заявител по реда на т.1.1.2 на този раздел.

В случай, че регистрираният заявител притежава валидно Удостоверение за КЕП, издадено от ДУУ, последният попълва по електронен начин Искането за съответните услуги и го подава, използвайки валидното Удостоверение. Заедно със заявлението, заявителят следва да изпрати по електронен път и по указания в електронния портал на ДУУ начин и необходимите документи за установяване на самоличността/идентичността на Автора/Титулята, както и останалите изискуеми документи, посочени по-горе в т.1.1. „Първоначална идентификация и автентикация пред РО".

В случай, че регистрираният заявител не притежава валидно Удостоверение за КЕП, издадено от ДУУ, подаването на Искането и съпътстващите документи в този случай се извършва към РО по реда предвиден в т.1.1.1.

2. Непотвърдена официално информация

СЕП България прави проверка по реда на раздел VII на тази глава по отношение на предоставените от заявителя данни, съгласно изискванията на чл. 5, ал.1, т.1, б). на НДДУУРНПИПУУ.

ДУУ може да включи в съдържанието на предоставяните Удостоверения за КЕП и данни, които не могат да бъдат потвърдени по официален начин. Такива данни могат да бъдат, без да се ограничават само до:

- Електронен адрес за кореспонденция;
- Специфични за Автора/Титуляра идентификатори.

Непотвърдената официално информация се включва в съдържанието на Удостоверението на база декларация от страна на подалия Искане Автор/Титуляр.

СЕП България не носи отговорност за включената непотвърдена информация в съдържанието на Удостоверението, включително и при невъзможност от страна на Титуляра/Автора да ползва издаденото му Удостоверение.

3. Потвърждаване на представителството

При предоставяне на удостоверителни услуги ДУУ проверява представителната власт на лицата, носители на представителството или упълномощени от Титуляра, съответно Автора, преди да предприеме действия по извършване на заявените услуги.

Представителството се проверява на база предоставените от Титуляра/Автора официални документи, от които е виден факта и обема на представителната власт.

ДУУ може да събере необходимите данни за потвържадване на представителството, когато същото се основава на законова разпоредба, от публично достъпни регистри.

ДУУ не носи отговорност/не проверява правото на Титуляра за използване на лични данни на Автора. Отговорността за неправомерно използвани лични данни на Автора се носи от Титуляра. Титулярът е длъжен да декларира правото си да използва, съхранява и предоставя личните данни на Автора.

4. Контрол над двойката ключове

Ако лице контролира частния ключ, когато заявява издаване на Удостоверение за КЕП, УО и/или РО трябва да се убедят, че предоставеният за удостоверяване публичен ключ съответства на държания от лицето частен ключ.

Проверката за държане на частния ключ се извършва чрез процедура за доказване притежаване на частния ключ. Процедурата потвърждава, че публичният ключ на автора съответства на частния ключ и се намира под неговия изключителен контрол.

При заявяване на издаване на Удостоверение за КЕП, клиентският криптомодул SSCD генерира двойка ключове и съвместно с разработения от СЕП България PKI софтуер формира електронна заявка във формат PKCS #10, чрез която при създаване на Удостоверението се гарантира съответствието между публичния ключ и държания от Автора частен ключ. Електронната заявка се обработва от УО и УО издава исканото Удостоверение за КЕП.

По време на генериране на двойката ключове клиентският криптомодул се контролира от Автора.

При заявяване на издаване на Удостоверение за КЕП при РО клиентският криптомодул се предава на Автора. В този случай ДУУ гарантира, че криптомодулът и ключовете са предоставени по сигурен начин на Автора, за който са предназначени.

При получаване на удостоверителни услуги по електронен път Авторът управлява генерирането на двойката ключове от притежания от него криптомодул.

5. Процедури при предоставяне на удостоверителни услуги от СЕП България

СЕП България предоставя на клиентите си удостоверителни услуги по издаване и управление на Удостоверения за КЕП при стриктно спазване на описаните по-долу правила и процедури.

Всяка процедура стартира с подаване на съответно Искане от Автора/Титуляра или надлежно упълномощено за процедурата лице. Подаденото Искане съдържа данни за съответната услуга и необходимата информация за идентификация/автентикация на Автора/Титуляра и надлежни декларации за референтни факти и права.

5.1. Подаване на Искания

Исканията за съответната услуга се подават:

- Към оператор на РО.
- Към СЕП България, посредством електронната страница на СЕП България;

Исканията се подават съответно в електронна форма или на хартиен носител.

5.1.1. Искания на хартиен носител

Исканията на хартиен носител се подават към РО по някой от следните начини:

- Лично на оператор на РО;
- По непряк метод, даващ същата степен на сигурност, както при личното подаване.

При необходимост, в зависимост от съответната процедура, РО изисква представянето на допълнителните данни и документи за получаване на удостоверителната услуга

5.1.2. Искания в електронна форма

Исканията в електронна форма се подават посредством електронната страница на СЕП България и се попълват като се спазват указанията на всяка стъпка от процеса.

За подаване на искания по електронен път чрез електронната страница на СЕП България се използват мрежови протоколи като HTTPS, S/MIMME или TCP/IP.

При необходимост, в зависимост от съответната процедура, се посочва РО, пред който ще се представят допълнителните данни и документи (съпътстващи Искането документи), необходими за получаване на исканата удостоверителната услуга. Съпътстващите Искането документи могат да бъдат подадени по електронен път заедно с конкретното Искане, като в този случай се изисква същите да бъдат нотариално заверени.

Искането се обработва от оператор на РО като се проверяват и сравнят данните от подаденото Искане с данни от други източници и допълнително представените данни и документи за получаване на удостоверителната услуга по реда на раздел VII на тази глава.

5.2. Обработване на Исканията от РО

Исканията се обработват от оператор на РО по следния начин:

- Операторът проверява данните, посочени в Искането и, когато е приложимо, проверява доказателствата относно държането на частен ключ от Автора;
- Данните се сверяват с данни от публични регистри и/или допълнително предоставени документи;
- РО може да провери и други данни при необходимост;
- При успешна проверка, операторът одобрява Искането, като го подписва. При грешни и неверни данни Искането се отхвърля;
- На база на одобреното Искане се подава електронна заявка към УО посредством специализирания софтуер, като операторът на РО гарантира съответствието между данните в електронната заявка към УО с данните, съдържащи се в съответното Искане.

РО комплектова и предава на ДУУ събраните документи с оглед исканата от Клиента удостоверителна услуга по издаване и управление на Удостоверение за КЕП.

5.3. Обработка на заявките от Удостоверяващ орган

УО обработва получените по реда на т.5.2. от този раздел електронни заявки по следния начин:

- Проверява дали заявката е получена от упълномощен РО и автентикира оператора на РО, подал съответната заявка;
- Свързва данните от Искането с наличните данни за Автор/Титуляр от своята база данни;
- Води записи за обработката в базата данни, системните журнали на PKI и Регистъра.

5.4. Процедура за издаване на Удостоверение за КЕП

Издаване на ново Удостоверение за КЕП представлява вписване на съответното Удостоверение в „Списъка на издадените удостоверения“ в публичния електронен регистър на ДУУ.

Издаването се извършва въз основа на подадено Искане за издаване на Удостоверение за КЕП. Информацията, която се попълва в Искането следва да е изчерпателна и коректна, в зависимост от типа на искано Удостоверение за КЕП. Информацията по предходното изречение включва:

- Пълното име на Автора, както и псевдонима му, ако се иска вписването на такъв в съответното удостоверение;
- Пълното име на Титуляра;

- Пълно име на лицето, упълномощено да представлява Титуляра/Автора при заявяване на услугата (заявител);
- Идентификатори на Автора: ЕГН, ЛНЧ, номер на документ за самоличност, дата на издаване и валидност на документа, орган, издател на документа за самоличност;
- Идентификатори на Титуляра: ЕИК, БУЛСТАТ, ИН по ДДС
- Идентификатори на заявителя: ЕГН, ЛНЧ
- Постоянен адрес/ седалище и адрес на управление на Титуляра;
- Постоянен/служебен адрес на Автора;
- Тип на искано Удостоверение за КЕП;
- Електронен адрес на Автора за целите на ползване на Удостоверението за КЕП;
- Допълнителна информация, необходима за получаване на искания тип Удостоверение за КЕП;
- Данни за представителната власт на Автора – вид, номер и дата на документа, удостоверяващ представителната власт, индивидуализиращи белези на органа, издал/удостоверил документа.
- Данни и информация за принадлежността на лицето към съответната браншова/съсловна организация.

Заедно с предоставянето на посочената по-горе информация, лицето, подаващо Искането за издаване на Удостоверение за КЕП, следва да представи и следните декларации относно:

- Пълнота, коректност и точност на представените с Искането данни;
- Съхраняване и обработка на личните данни, съдържащи се в Искането;
- Наличието или липсата на желание за ограничаване на публичния достъп до исканото Удостоверение за КЕП.

При получаване на Искане за издаване на Удостоверение за КЕП, ДУУ, чрез съответен РО:

- Извършва съответната идентификация/автентикация на лицето по реда на раздел VII, т. 1 на тази глава;
- Обработва Искането по реда на т.5.2 на този раздел;
- Сключва договор за Удостоверителни услуги (ако съответният договор е обвързан с конкретно удостоверение);
- Издава фактура за заплатена цена;
- РО подава електронна заявка по реда на т.5.3 на този раздел към сървъра на УО за издаване на Удостоверение за КЕП, спазвайки изискванията:
    - Алгоритмите за проверка на Удостоверения за КЕП да съставляват логическо цяло с алгоритмите за създаването им;
    - Алгоритмите и параметрите за квалифициран електронен подпис да отговарят на съответни изисквания по отношение на хеш-функциите и асиметричните алгоритми съгласно изискванията на НИАСПКЕП;
- Ако процедурата е успешна, сървърът генерира Удостоверението и го подписва като използва хардуерен криптомодул. Генерираното удостоверение се съхранява в базата данни на УО и се публикува в публичния електронен регистър на УО;
- УО подготвя отговор, съдържащ генерираното Удостоверение за КЕП и го представя на клиента чрез РО, или по електронен път.

Издаденото Удостоверение за КЕП се смята за валидно от момента на публикуването му в публичния електронен регистър на ДУУ.

Публикуването на Удостоверението за КЕП в Регистъра е равносилно на уведомяване на доверяващите се страни за това, че е издадено Удостоверение на лицето, вписано в него, и това лице може да се идентифицира чрез този КЕП.

5.4.1. Отказ за издаване на Удостоверение за КЕП

ДУУ има право да откаже издаване на Удостоверение за КЕП в следните случаи:

- Авторът/Титулярът не е представил изискуемите документи за издаване на удостоверение за КЕП;
- Заявителят не може да докаже наличието на изрична представителна власт относно извършването на фактическите и правни действия по снабдяване с Удостоверение за КЕП;
- При наличие на съмнения, че при провеждане на процедурата по издаване на Удостоверение за КЕП са използвани неверни данни и/или неистински или подправен документ;
- При неспазване на изискванията на чл.25, ал.2, т.3 от ЗЕДЕП
- Достигнат е предварително договорен лимит за брой издадени Удостоверения за КЕП на конкретен Титуляр/Автор;
- При наличие на други основания за отказ, регламентирани в действащото законодателство.

Информацията за отказа за издаване на Удостоверение за КЕП и причините свързани с това се съобщават на заявителя. Лицето, на което е отказано издаването на Удостоверение за КЕП може да подаде жалба в 3 (три) дневен срок по реда, предвиден в Глава Първа, раздел VI.

5.4.2. Приемане на съдържанието на издадено Удостоверение за КЕП

Авторът/Титулярът, може да възрази, ако издаденото му Удостоверение съдържа грешки или непълноти в 3 (три) дневен срок от публикуването му в публичния електронен регистър на ДУУ.

ДУУ издава ново Удостоверение за КЕП без допълнително заплащане, освен в случаите, когато грешките се дължат на предоставяне на неверни данни от страна на Автора/Титуляра или упълномощеното лице.

В случай, че Авторът/Титулярът не подаде възражение в посочения по-горе срок, се смята, че съдържанието на издаденото Удостоверение е прието.

5.5. Процедура за подновяване на Удостоверение за КЕП

Подновяване на валидно Удостоверение за КЕП представлява издаване на ново Удостоверение за КЕП, заявено преди изтичане на срока на действието на валидното Удостоверение за КЕП. Подновяват се само валидни Удостоверения, които не са прекратени и информацията, съдържаща се в тях не е променена.

Подновяването се извършва чрез подаване на Искане за издаване на Удостоверение за КЕП на основание подновяване. Информацията, която се попълва в Искането следва да съдържа идентична информация на тази, подадена от лицето при Искането за издаване на подновяваното Удостоверение, както е посочено в т.5.4 на този раздел.

При получаване на Искане за подновяване на Удостоверение за КЕП, ДУУ, чрез съответен РО:

- Извършва съответната идентификация/автентикация на лицето по реда на раздел VII, т.1;
- РО обработва Искането по реда на т.5.2 на този раздел;

- Сключва договор за Удостоверителни услуги (ако съответният договор е обвързан с конкретно удостоверение);
- Издава фактура за заплатена цена;
- РО подава електронна заявка по реда на т.5.3 на този раздел към сървъра на УО за издаване на Удостоверение за КЕП;
- Ако процедурата е успешна сървърът генерира Удостоверението и го подписва като използва хардуерен криптомодул. Новото Удостоверение за КЕП е с нови сериен номер и срок на действие. Генерираното удостоверение се съхранява в базата данни на УО и се публикува в публичния електронен регистър на УО;
- УО подготвя отговор, съдържащ генерираното подновено Удостоверение за КЕП и го представя на клиента чрез РО, или по електронен път.

СЕП България публикува информация за подновеното Удостоверение за КЕП в публичния си електронен регистър. Публикуването на инфромацията за Удостоверението за КЕП е равносилно на уведомяване на доверяващите се страни за това, че лицето, вписано в него, притежава валидно Удостоверение и може да се идентифицира чрез съответния КЕП.

СЕП България има право да откаже подновяването на Удостоверение за КЕП в описаните по-горе в т5.4.1. на този раздел хипотези.

Авторът/Титулярът, може да възрази, ако издаденото му подновено Удостоверение съдържа грешки или непълноти в 3 (три) дневен срок от публикуването му в публичния електронен регистър на ДУУ.

ДУУ издава ново Удостоверение за КЕП без допълнително заплащане, освен в случаите, когато грешките се дължат на предоставяне на неверни данни от страна на Автора/Титуляра или упълномощеното лице.

В случай, че Авторът/Титулярът не подаде възражение в посочения по-горе срок, се смята, че съдържанието на издаденото подновено Удостоверение е прието.

5.6. Процедура за модификация на удостоверение за КЕП

Модификация на Удостоверение за КЕП представлява издаване на ново удостоверение на база на издадено преди това валидно удостоверение при промяна на информация, вписана в Удостоверението.

Обхвата на допустимата промяна е вписване на ново съдържание или попълване на нова информация.

Модифицират се само валидни удостоверения, които не са прекратени.

Модификацията се извършва чрез подаване на Искане за издаване на Удостоверение за КЕП на основание модификация. Информацията, която се попълва в Искането следва да съдържа информацията, подадена от лицето при предхождащото Искане за издаване на Удостоверение, както е посочено в т.5.4 от този раздел и съответното ново съдържание от допустимия обхват.

Искането се подава към ДУУ по реда предвиден в т.5.1 на настоящия раздел.

При получаване на Искане за модификация на Удостоверение за КЕП, ДУУ:

- Извършва съответната идентификация/автентикация на лицето по реда на раздел VII, т.1.2;
- РО обработва Искането по реда на т5.2 на настоящия раздел;
- Сключва договор за удостоверителни услуги (ако съответният договор е обвързан с конкретно Удостоверение);

- Издава фактура за заплатена цена;
- РО подава електронна заявка към УО за издаване на Удостоверение за КЕП по реда на т. 5.3 на този раздел;
- Обработената по реда на т. 5.3 на този раздел електронна заявка се подава към сървъра на УО за издаване на Удостоверение;
- Ако процедурата е успешна сървъра генерира Удостоверението и го подписва като използва хардуерен криптомодул. Новото Удостоверение за КЕП е с нови сериен номер и срок на действие. Генерираното удостоверение се съхранява в базата данни на УО и се публикува в публичния електронен регистър на УО, а модифицираното Удостоверение се прекратява;
- УО подготвя отговор, съдържащ генерираното ново Удостоверение за КЕП и го предоставя на Клиента чрез РО или по електронен път.

СЕП България публикува информация за модифицираното Удостоверение за КЕП в публичния си електронен регистър. Публикуването на информацията за Удостоверението за КЕП е равносилно на уведомяване на доверяващите се страни за това, че лицето, вписано в него, притежава валидно Удостоверение и може да се автентикира чрез съответния КЕП.

Модифицираното Удостоверение за КЕП се прекратява с причина за прекратяване affiliationChanged. По този начин се показва, че Удостоверението е заменено от друго с модифицирани данни и информира доверяващите се страни, че частният ключ, съответстващ на публичния от замененото Удостоверение, не е бил компрометиран.

СЕП България има право да откаже модифицирането на Удостоверение за КЕП в описаните по-горе в т5.4.1. на този Раздел хипотези.

Авторът/Титулярът, може да възрази, ако издаденото му в хода на процедурата по модифициране ново Удостоверение съдържа грешки или непълноти в 3 (три) дневен срок от публикуването му в публичния електронен регистър на ДУУ.

ДУУ издава ново Удостоверение за КЕП без допълнително заплащане, освен в случаите, когато грешките се дължат на предоставяне на неверни данни от страна на Автора/Титуляра или упълномощеното лице.

В случай, че Авторът/Титулярът не подаде възражение в посочения по-горе срок, се смята, че съдържанието на издаденото модифицирано Удостоверение е прието.

5.7. Процедура за спиране на Удостоверение за КЕП

Спиране на Удостоверение за КЕП представлява временно включване на Удостоверението в „Списъка на прекратените удостоверения“. За времето на спиране на Удостоверението, последното се счита за невалидно и всички електронни подписи, автентикирани с това Удостоверение са недействителни.

Действието на валидно Удостоверение може да бъде спряно при наличие на съответните основания, за необходимия според обстоятелствата срок, но за не повече от 48 часа.

Спиране на Удостоверение за КЕП се осъществява в следните случаи:

- По искане, отправено към ДУУ от Автора или Титуляра, или упълномощено от него лице, без ДУУ да е длъжен да се увери в самоличността или в представителната му власт;
- 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.;
- По искане на Комисията за регулиране на съобщенията;

- С решение на председателя на Комисията за регулиране на съобщенията.

Искането за спиране (представляващо вид Искане за управление) се подава към ДУУ по реда предвиден в т5.1 на този раздел, като следва да съдържа и информация за причината за спиране.

При получаване на Искане за спиране на Удостоверение за КЕП, ДУУ го обработва по следния ред:

- РО обработва Искането по реда, предвиден в т.5.2 на настоящия раздел.
- РО подава електронна заявка към УО за спиране на Удостоверение за КЕП по реда на т.5.3 на настоящия раздел;
- УО проверява валидността на Удостоверението, чието спиране се иска и съответствието между данните в Искането и данните, вписани в Удостоверението;
- УО спира действието на удостоверението, като го включва в „Списъка на прекратените удостоверения“ с причина за прекратяване „hold“;
- УО незабавно уведомява Титуляра/Автора за спирането на действието на удостоверението.

СЕП България публикува информация за спряното Удостоверение за КЕП в публичния си електронен регистър. Публикуването на информацията за Удостоверението за КЕП е равносилно на уведомяване на доверяващите се страни за това, че съответното Удостоверение не е валидно и лицето, вписано в него, не може да бъде автентикирано чрез съответния КЕП.

5.8. Процедура за възобновяване на Удостоверение за КЕП

Възобновяване на Удостоверение за КЕП представлява изключване на Удостоверението от „Списъка на прекратени удостоверения“. След възобновяване на Удостоверението последното се счита за валидно.

Възобновяването на спряно Удостоверение се осъществява в следните случаи:

- След изтичане на максималният срок за спиране от 48 часа – автоматично;
- Преди изтичане на максималния срок за спиране – от доставчика на удостоверителни услуги - при отпадане на основанието за спиране или по Искане на Автора или Титуляря, след като ДУУ, съответно Комисията за регулиране на съобщенията, се е уверил/а, че той е узнал причината за спирането, както и че Искането за възобновяване е направено вследствие на узнаването.

Искането за възобновяване (представляващо вид Искане за управление) от страна на Автора/Титуляра се подава към ДУУ по реда предвиден в т5.1 на настоящия раздел.

Информацията, която се съдържа в Искането е следната:

- Информация за възобновяваното Удостоверение;
- Пълното име на Автора;
- Пълното име на Титуляра;
- Пълно име на лицето, упълномощено да представлява Титуляра/Автора при заявяване на услугата;
- Идентификатори на Автора/Титуляра: ЕГН, ЛНЧ, ЕИК, БУЛСТАТ;
- Постоянен адрес/ седалище и адрес на управление на Титуляра;
- Постоянен/служебен адрес на Автора;
- Причина за възобновяване;

- Декларация, че Авторът/Титулярът е узнал причината за спирането и Искането за възобновяване е направено вследствие на узнаването.

При получаване на Искане за възобновяване на Удостоверение за КЕП от страна на Автора/Титуляра, ДУУ го обработва по следния ред:

- Извършва съответната идентификация/автентикация на лицето по реда на раздел VII, т.1.2;
- РО обработва Искането по реда на т.5.2 на настоящият раздел;
- РО подава електронна заявка към УО за възобновяване на Удостоверение за КЕП по реда на т.5.3 на настоящият раздел;
- УО проверява валидността на Удостоверението, чието възобновяване се иска, както и наличието на основания за Искането и съответствието между данните в Искането и данните, вписани в Удостоверението;
- УО възобновява спряното Удостоверение като го изключва от „Списъка на прекратените удостоверения";
- УО незабавно уведомява Титуляра/Автора за възобновяването на действието на удостоверението.

УО възобновява спряно Удостоверение и след получаване на писмено разпореждане от Комисията за регулиране на съобщенията или председателя на Комисията за регулиране на съобщенията за възобновяване, или незабавно след изтичане на максималния период за спиране (48 часа).

От момента на възобновяване на Удостоверението, същото се счита за валидно. СЕП България публикува информация за възобновеното Удостоверение за КЕП в публичния си електронен регистър. Публикуването на информацията за Удостоверението за КЕП е равносилно на уведомяване на доверяващите се страни за това, че лицето, вписано в него, притежава валидно Удостоверение и може да се автентикира чрез съответния КЕП.

5.9. Процедура за прекратяване на удостоверение

Прекратяване на Удостоверение за КЕП представлява включване на Удостоверението в „Списъка на прекратените удостоверения" (CRL). От момента на включване на Удостоверението в „Списъка на прекратените удостоверения", същото се счита за невалидно и всички електронни подписи, автентикирани с това Удостоверение са недействителни.

Прекратяване на Удостоверение би могло да се осъществяви в следните случаи:

- Смърт или поставяне под запрещение на Автора;
- Прекратяване на представителната власт на Автора по отношение на Титуляра, когато удостоверението е издадено с вписване на Титуляр;
- Прекратяване на юридическото лице на Титуляра, когато удостоверението е издадено с вписване на Титуляр;
- Установяване, че Удостоверението е издадено въз основа на неверни данни;
- Компрометиране (или съмнения за компрометиране) на частния ключ, съответстващ на публичния от Удостоверението или носителя използван за съхранението му;
- Искане на Титуляра или Автора за прекратяване на Удостоверението и/или за прекратяване на договорните отношения със СЕП България, подадено по реда на т.5.1 на този раздел;
- При компрометиране на частния ключ на ДУУ;
- При неизпълнение (пълно или частично) на задължение за заплащане на определените цени за ползване на удостоверителни услуги;

- При прекратяване на дейността на ДУУ. В този случай се прекратяват всички издадени Удостоверения, както и удостоверенията на ДУУ;
- При неизпълнение от страна на Титуляра/Автора на задълженията му според този Наръчник или сключен договор за удостоверителни услуги;
- С изтичане на срока на действие на Удостоверението;
- Искането за прекратяване се подава по следния начин:
- От страна на Титуляра/Автора, или упълномощено за целта лице;
- По искане на посочени в нормативен акт органи.

Когато прекратяването се извършва по искане от страна на Автора/Титуляра, то Искането за прекратяване (представляващо вид Искане за управление) се подава към ДУУ по реда предвиден в т.5.1 на настоящия раздел.

Информацията, която се съдържа в Искането за прекратяване е следната:

- Информация за прекратяваното Удостоверение;
- Пълното име на Автора;
- Пълното име на Титуляра;
- Пълно име на лицето, упълномощено да представлява Титуляра/Автора при заявяване на услугата;
- Идентификатори на Автора/Титуляра: ЕГН, ЛНЧ, ЕИК, БУЛСТАТ;
- Постоянен адрес/ седалище и адрес на управление на Титуляра;
- Постоянен/служебен адрес на Автора;
- Причина за прекратяване.

При получаване на Искане за прекратяване на Удостоверение за КЕП, ДУУ го обработва по следния ред:

- РО извършва идентификация/автентикация на Автора/Титуляра по реда на раздел VII, т.1;
- РО обработва Искането по реда, предвиден в т.5.2 на този раздел;
- УО обработва Искането по реда, предвиден в т.5.3 на този разде;
- УО публикува информация за прекратяването на Удостоверението в CRL заедно с информация относно причината за прекратяване;
- УО изпраща потвърждение за прекратяване на Удостоверението до заявителя на Искането за прекратяване;
- УО незабавно уведомява Титуляра/Автора за прекратяване на действието на Удостоверението.

СЕП България публикува информация за прекратеното Удостоверение за КЕП в публичния си електронен регистър. Публикуването на Удостоверението за КЕП в „Списъка на прекратените удостоверения“ е равносилно на уведомяване на доверяващите се страни за това, че съответното Удостоверение не е валидно и лицето, вписано в него, не може да бъде автентикирано чрез съответния КЕП.

5.10. Поддръжка на Удостоверение за КЕП

Поддръжка на Удостоверение за КЕП представлява осигуряването на възможността за използване на следните услуги за определен период в рамките на срока на действие на издадено валидно Удостоверение:

- Услуги по управление (спиране, възобновяване и прекратяване) на издадено валидно Удостоверение за КЕП;

- Услуга за Удостоверяване на време на представяне на КЕП, създаден за определен електронен документ;
- Услуги по публикуване на актуална информация за Удостоверението за КЕП в публичния електронен регистър на ДУУ съобразно искането на Клиента;
- Услуги по валидация - извършването на проверка на валидността на издаденото Удостоверение от доверяващите се страни.

Поддържат се само валидни Удостоверения, които не са прекратени и информацията, съдържаща се в тях не е променена.

С оглед извършване на ежегодната поддръжка през периода на валидност на удостоверението, Клиентът подава Искане за поддръжка. Искането за поддръжка следва да бъде подавано до края на съответния едногодишен период.

Информацията, която се съдържа в Искането е следната:

- Информация за поддържаното Удостоверение;
- Пълното име на Автора;
- Пълното име на Титуляра;
- Пълно име на лицето, упълномощено да представлява Титуляра/Автора при заявяване на услугата;
- Идентификатори на Автора/Титуляра: ЕГН, ЛНЧ, ЕИК, БУЛСТАТ;
- Постоянен адрес/ седалище и адрес на управление на Титуляра;
- Постоянен/служебен адрес на Автора;
- Декларация за непроменени данни.

Искането се подава към ДУУ по реда предвиден в т.5.1 на този раздел.

При получаване на Искане за поддръжка на Удостоверение за КЕП, ДУУ:

- Извършва съответната идентификация/автентикация на лицето по реда на раздел VII, т.1;
- Издава фактура за заплатена цена;
- Обработва Искането за поддръжка на Удостоверение за КЕП по реда на т.5.2 на настоящия раздел.

В случай че Клиентът не подаде Искане за поддръжка на Удостоверение за КЕП в предвидения за това срок, то последното ще бъде прекратено.

6. Използване на Удостоверението и ключовата двойка

Титулярът/Авторът могат да използват частния ключ и Удостоверението за КЕП:

- Съобразно тяхното предназначение, както е посочено в този документ и в съответствие със съдържанието на Удостоверението за КЕП (полета keyUsage, EnhancedKeyUsage);
- Съобразно Договора за удостоверителни услуги, сключен между тях и СЕП България;
- В срока на валидност на Удостоверението, освен за целите на декриптиране на документи и проверка на електронен подпис;
- До прекратяване на Удостоверението за КЕП;

- Когато Удостоверението е спряно и Титулярът/Авторът е използвал частния ключ за поставяне на електронен подпис, то подписите ще се смятат за действителни само, ако Удостоверението бъде възобновено.

Доверяващите се страни могат да ползват публичния ключ и Удостоверението за КЕП:

- Съобразно тяхното предназначение, както е посочено в този документ и в съответствие със съдържанието на Удостоверението за КЕП (полета keyUsage, enchansedKeyUsage);
- Само за проверка статуса на издадено Удостоверение за КЕП и проверка на електронен подпис;
- До момента на прекратяване за публични ключове за key exchange, data encryption или key agreement;
- Когато Удостоверението е спряно, доверяващата се страна не следва да ползва публичния ключ от това Удостоверение.

7. Необходимост от проверка статуса на Удостоверението за КЕП

Отговорност на доверяващите се страни, при получаване на документ, подписан с КЕП, е да проверят дали публичният ключ от Удостоверението, който съответства на частния ключ на Автора, използван при електронния подпис, не е публикуван в CRL. Доверяващата се страна следва да направи проверката онлайн в актуалния текущ CRL или по OCSP.

Ако проверяваното Удостоверение за КЕП (съответно публичен ключ) е включено в CRL, доверяващата се страна следва да отхвърли документа, асоцииран с Удостоверението, ако причината за включване в CRL е една от следните:

Причина	**Описание**
Unspecified	Не е посочена причина за включване на удостоверението в CRL
keyCompromise	Нарушена е сигурността на частния ключ
caCompromiced	Нарушена е сигурността на ключа на УО
cessationOfOperation	Основанието за издаване на Удостоверението вече не съществува
certificateHold	Удостоверението е спряно
affiliationChanged	Модифицирани са данните, вписани вУдостоверението
Superseded	Удостоверението е заменено с друго удостоверение

Крайното решение относно приемане на валидността на Удостоверението се взема от доверяващата се страна. ДУУ не носи отговорност за действията на доверяващата се страна при неизпълнение на посочените по-горе изисквания.

7.1. Онлайн проверка на валидността на Удостоверения за КЕП

СЕП България предоставя възможност за проверка в реално време, онлайн, на статуса на издадените Удостоверения за КЕП. Тази услуга се предоставя чрез OCSP протокол, описан в RFC 2560. Моделът на предоставяне на OCSP услугата се базира на процеса „запитване – отговор“. Отговорите, които се получават от OCSP сървъра, осигуряващ услугата, са следните:

Отговор	**Значение**
good	Удостоверението е валидно
revoked	Удостоверението е прекратено
unknown	Статусът на Удостоверението не е установен или Удостоверението не е издадено от съответния УО.

7.2. Услуги по валидация

Доверяващите се страни могат да проверят статуса на издадено от СЕП България Удостоверение за КЕП по един от следните начини:

- В „Списъка на прекратените удостоверения“, публикуван в публичния електронен регистър на СЕП България;
- Чрез OCSP протокол.

Необходимите действия за осъществяване на проверката са съответно:

- Изтегляне на CRL и инсталиране в приложението на доверяващата се страна. Електронният адрес, от който може да се изтегли CRL се посочва във всяко издадено Удостоверение;
- При OCSP – изпращане на заявка за валидация до сървъра на СЕП България. Протокола за обмен е дефиниран в RFC 2560.

7.3. Достъпност на услугата

Услугата за валидация е достъпна 24 часа 7 дни в седмицата. При аварии и природни бедствия, СЕП България взема незабавни мерки, за да се възстановят първо услугите по валидация.

8. Издаване на удостоверение за време

СЕП България издава удостоверение за времето на представяне на електронен подпис, създаден за определен електронен документ.

Удостоверението за време има официална удостоверителна сила след вписването му Регистъра на ДУУ за издадените удостоверения за време.

Системата на СЕП България за удостоверяване на време приема обръщения в съответствие с IETF RFC 3161 Internet X.509 Public Key Infrastructure Time-Stamp Protocol.

8.1. Процедура по Удостоверяване на време

Системата на СЕП България, осигуряваща Удостоверяването на време, приема заявки и връща отговори във формат, дефиниран от RFC 3161 - „Internet X.509 Public Key Infrastructure - Time-Stamp Protocol“.

В заявката е необходимо да се съдържа хеш на електронния подпис на документа, чието време на поставяне се удостоверява и версия на заявката.

Заявката за удостоверяване на време се изпраща на електронен адрес: http://tsa.sep.bg и може да се генерира чрез специализиран клиентски софтуер.

Постъпващите заявки се обработват последователно. Точността, с която се издават удостоверенията за време от СЕП България, е една секунда. Удостоверението за време, съдържа следните елементи:

- Статус;
- Версия на удостоверението за време;
- Идентификатор на удостоверения документ;
- Последователен уникален сериен номер;
- Време на подписване по ZULU;
- Идентификация на доставчика на удостоверено време – СЕП България.

Удостоверенията за време се подписват с частен ключ, предназначен само и единствено за тази дейност.

9. Прекратяване ползване на удостоверителни услуги

СЕП България няма ангажимент към Титуляра по отношение на предоставяне на услуги по управление на Удостоверения за КЕП, след като Договорът, сключен между тях, е прекратен или изтекъл.

Клиентът на удостоверителните услуги на СЕП България, може по всяко време да прекрати ползваните от него удостоверителни услуги.

При Искане за прекратяване на ползването на удостоверителни услуги, СЕП България, прекратява договорните отношения с Титуляра/Автора и прекратява издадените Удостоверения, в които Титулярът/Авторът е вписан.

СЕП България не обезщетява Титуляра/Автора, при прекратяване на ползването на удостоверителни услуги по негово искане.

VIII. Съоръжения, ръководство и оперативни контроли

В тази глава се представят общите правила относно управлението на ДУУ и реализираните контроли по отношение на физическата и организационна сигурност и дейностите на персонала, при предоставяне на удостоверителни услуги от СЕП България.

1. Съоръжения на доставчика

1.1. Физическа сигурност при УО

Мрежовите компютърни системи, терминалите на операторите и информационните ресурси на СЕП България са разположени в обособени места, физически, защитени срещу неоторизиран достъп, разрушаване и

прекъсване на операциите. Тези места се наблюдават и охраняват денонощно. Водят се записи за всяко влизане и излизане в журнал. Следят се параметрите на електрозахранването, температурата и влажността на въздуха.

СЕП България разполага с помещения със съответна степен на физическа защита срещу проникване. Помещенията са климатизирани, с контролиран физически достъп, осигурено основно и резервно електрозахранване, осигурен основен и запасен комуникационен канал.

1.1.1. Физически достъп

Сградата се охранява от 24 часова физическа охрана. Изградена е техническа система, следяща за проникване на територията на обекта и в защитените помещения. Прилежащата територия и помещенията са под 24 часово видео наблюдение.

Физическият достъп се наблюдава и контролира от интегрирана система за сигурност, следяща за наличието или отсъствието на служители в помещенията на ДУУ.

Реализирана е противопожарна система и са взети мерки срещу наводнение на помещенията.

Системите са осигурени срещу отпадане на електрическото захранване на обекта, взети са мерки срещу краткотрайни прекъсвания и колебания в захранващата електрическа мрежа (UPS) и срещу дълготрайни прекъсвания на електрозахранването (генератор).

В зависимост от дейностите, които се извършват в съответните помещения, част от тях са публично достъпни, а достъпът до други се контролира или е възможен само за упълномощени служители. До определени помещения се изисква едновременно присъствие на двама упълномощени служители.

Посетители и одитори се допускат само ако те се придружават от служител/ли на СЕП България, имащ/и право на достъп до посетеното помещение.

Всички служители и посетители носят бадж с информация за зоната за физически достъп и режима на достъп.

Защитените зони са оборудвани със системите за физически контрол и наблюдение и системи за известяване при пожар и гасене на пожар. Достъп до тези зони имат само упълномощени служители на СЕП България. Влизането и излизането от зоните и движението в помещенията от зоните се следи и записва от система за контрол на достъпа. Придружителите могат да преминават само след потвърждение от упълномощен служител.

1.1.2. Електрозахранване и климатизация

При отпадане на основното захранване системите превключват на резервно захранване.

При кратковременни прекъсвания и колебания се използва UPS. В случай, че прекъсването е продължително се включва генератор.

Всички работни помещения са вентилирани и климатизирани. Вентилацията е проектирана и изпълнена по такъв начин, че да не се компрометира физическата сигурност на обекта.

1.1.3. Наводнение

Взети са мерки са предотвратяване наводняването на помещенията на СЕП България. Реализирана е процедура за реагиране при проблеми, свързани с природно бедствие или промишлена авария.

1.1.4. Противопожарни мерки

Взети са мерки по откриване и гасене на пожар в помещенията, използвани за дейността на СЕП България. Реализирана е процедура за действие при възникване на пожар. Всички помещения, в зависимост от типа им, са оборудвани със средства за гасене на пожар в съответствие с нормативната регулация. В защитените помещения и архивите е изградена автоматична система за гасене, която се включва автоматично при откриване на огън.

1.1.5. Съхраняване на носители

В зависимост от чувствителността на съхраняваната върху носителите информация, носителите с архиви и резервни копия се съхраняват в огнеупорни сейфове, разположени в защитените помещения. Достъпът до сейфовете се осъществява чрез два ключа, държани от упълномощени лица. Копия от тази информация се съхранява при същите условия извън основните помещения.

Носителите използвани за архивиране на текущата информация и резервни копия, и хартиените документи се съхраняват в сейфове разположени при ДУУ. Периодът на съхранение е 10 (десет) години от получаване на информацията и сключване на договор с клиента.

1.1.6. Депозиране на отпадъци

Хартиени и електронни носители с чувствителни данни, след изтичане на периода за съхранение, се унищожават по подходящ начин, така, че да не е възможно узнаване на информацията, която е била върху тях.

1.1.7. Съхранение на резервните копия

СЕП България съхранява резервни копия от всички необходими данни, с чиято помощ може да възстанови своите операции в рамките на 48 часа. Това са копия на актуалните данни и резервни копия на информационните системи.

1.2. Съоръжения на РО

Компютърните системи в РО се разполагат в подходящо оборудвани помещения и работят в онлайн режим по приемане и обработка на исканията на клиентите. Достъпът е физически ограничен. Взети са мерки системите да се ползват само от упълномощени лица.

Актуален списък с адресите на действащите регистриращи органи е публикуван на електронната страница на СЕП България.

1.2.1. Сигурност на Титуляра/Автора

Титулярът/Авторът е отговорен за съхранението и опазване тайната на паролите за достъп, идентификационни кодове, ПИН и деблокиращ ПИН.

1.2.2. Контрол на процедурите

Всички процедури се изпълняват в съответствие със ЗЕДЕП, регламентиращите документи разработени от ДУУ и вътрешните процедури и правила, от служители на съответни длъжности и в съответствие с делегирани права и задължения.

2. Ръководство и персонал

2.1. Доверени длъжности

СЕП България разработва длъжностни характеристики в съответствие с раздел IV на „Наредба за дейността на доставчиците на удостоверителни услуги, реда за нейното прекратяване и за изискванията при предоставяне на удостоверителни услуги".

ДУУ обособява в своята организационна структура различни длъжности за изпълнение на следните видове дейности:

- Генериране и поддържане на инфарструктурата на публичния ключ на ДУУ;
- Администриране и осигуряване сигурност на системите;
- Създаване и управление на удостоверения за квалифициран електронен подпис, включително създаване на двойка ключове - частен и публичен, за квалифициран електронен подпис;
- Съхранение на данни и архивиране.

2.2. Управление на персонала

СЕП България предприема мерки, които да гарантират високо ниво на персонала при изпълнение на задълженията му по предоставяне на удостоверителни услуги. Мерките при назначаване, са както следва:

- Лицата са завършили минимум средно образование (доколкото не се изисква друго за съответната длъжност);
- Представят свидетелство за съдимост;
- Подписват трудов договор с приложена длъжностна характеристика, описваща преките задължения и отговорности;
- Подписват декларация за конфиденциалност;
- Преминават обучение за съответната длъжност;
- Обучават се за работа с клиенти и защита на лични данни.

2.3. Квалификация и опит

СЕП България назначава на съответните длъжности лица, които имат познания в следните области:

- Технологии за сигурност, криптография, инфраструктура на публични ключове (PKI);
- Технически норми за оценка на сигурността;
- Информационни системи.

СЕП България, преди да назначи лице на съответните длъжности, проверява познанията и квалификацията му.

2.4. Обучение на персонала

Персоналът на Доставчика на удостоверителни услуги – СЕП България, се обучава в следните области:

- Регулация, свързана със ЗЕДЕП и подзаконовите актове по приложението му;
- Регулация, свързана с „Политика за предоставяне на удостоверителни услуги";
- Регулация, свързана с „Практика при предоставяне на удостоверителни услуги";
- Регулация, свързана с вътрешни процедури и документация за съответната длъжност;
- Процедурите и контролите, свързани с информационната сигурност;

- Системен софтуер на УО и РО;
- Работа с клиенти и защита на личните данни.

Обучението на персонала се повтаря:

- При необходимост от опресняване и затвърждаване на знанията и уменията свързани с изпълнение на задълженията за заеманата длъжност;
- През определени периоди от време;
- При съществени промени в регламентиращите документи;
- При необходимост от разбор на критична ситуация или инцидент.

2.5. Дисциплинарни мерки

При неизпълнение на задълженията за съответната длъжност, СЕП България налага дисциплинарни санкции в зависимост от вида и размера на нарушението и в съответствие с действащото трудово законодателство.

2.6. Договори с външни лица

При сключване на договори с външни лица (външни услуги, разработка на софтуер и др.) те подлежат на същите процедури, както собствения персонал.

2.7. Документи, предоставяни на персонала

Ръководството на СЕП България, предоставя достъп на служителите от УО и РО до следните документи:

- ЗЕДЕП и подзаконовите актове по приложението му;
- „Политика за предоставяне на удостоверителни услуги";
- „Практика при предоставяне на удостоверителни услуги";
- Форми на искания и шаблони за всякаки използвани документи;
- Вътрешни процедури и документация за съответната длъжност;
- Процедурите и контролите, свързани с информационната сигурност;
- Ръководства на ползване на системния софтуер на УО и РО;
- Процедури за действие при извънредни ситуации, повреди, аварии и природни бедствия.

IX. Водене на записи и преглеждане на журналите

За ефективен контрол върху дейностите и персонала, СЕП България води записи за всички дейности, имащи съществено влияние върху сигурността.

Задължително всяка група или екип, свързан с предоставянето на удостоверителни услуги, води записи за своята дейност и отговаря за управлението им в съответствие с позицията и задълженията, които има.

Информационните записи от всеки журнал се съхраняват и достъпват само от оторизирани лица за получаване на информация, необходима за решаване на спорове или за откриване и проследяване на нарушения по информационната сигурност. Всички записи се архивират. Архивните копия се пазят извън основните помещения на ДУУ.

Генерирането на записи в журналите става автоматично. Ако това е невъзможно събитията се записват на хартиен носител. Всички записи – автоматични и на хартия, се предоставят при провеждане на проверки на дейността на ДУУ.

Мениджър ИТ Сигурност е задължен да осъществява регулярни проверки за съответствие на реализираните механизми и процедури с действащото законодателство и тази практика, и да оцени ефективността на съществуващите процедури по сигурността.

1. Тип на записваните събития

Всяка критична дейност по отношение на сигурността на СЕП България се записва в журнал и се архивира. Архивите може да се криптират и съхраняват върху носители за еднократен запис, за да се предотврати тяхната кражба или модифициране.

Запазват се всичките журнали, генерирани от софтуерните компоненти на информационната система на СЕП България. Записите се разделят на следните категории:

- Системни записи – записите съдържат информация относно системните събития;
- Записи за грешки – записите съдържат информация за грешките на ниво протокол и приложение;
- Записи от наблюдение – записите съдържат информация, свързана с удостоверителните услуги, като подаване на искания за издаване на удостоверения, приемане на удостоверения, издаване на удостоверения и списъци с прекратени удостоверения.

Горните журнали са общи за всеки компонент, инсталиран на приложните сървъри или работните станции. Размера на журналите предварително е определен и е предвиден достатъчен капацитет за нормална работа на системите. При достигане на определен размер се създават нови журнали. Старите се архивират и изтриват от оперативните системи.

Всеки запис независимо дали е на хартия или автоматично генериран, съдържа следната информация:

- Тип на събитието;
- Идентификатор на събитието;
- Дата и час на събитието;
- Идентификатор или други данни, които позволяват да се определи лицето, отговорно за събитието;
- Решението, което съответства на успешна или грешна операция.

Записите могат да бъдат:

- Аларми от защитни стени и мрежови сензори;
- Операции, съответстващи на регистрация, удостоверяване/издаване, смяна на ключове и подновяване, прекратяване, спиране/възобновяване и други услуги предоставяни от УО;
- Всяка промяна на хардуера или софтуера;
- Физическо посещение на защитените периметри и нарушаване на защитените периметри;
- Смаяна на ПИН, пароли и права за достъп на персонала;
- Успешни и неуспешни опити за достъп до базите данни на ДУУ;
- Генерация на ключове за УО и други елементи от инфраструктурата за доставка на удостоверителни услуги;
- Всяко получено искане в електронна форма.
- Цялата кореспонденция в електронна форма между ДУУ и другите участници в удостоверителния процес;
- История на архивните копия на журналите, системите и бази данни.

Достъп до журналите имат само Мениджър ИТ Сигурност и лица, осъществяващи проверка на дейността на ДУУ.

2. Преглед на журналите

Поне веднъж месечно се прави детайлен преглед на журналите, включително за цялостност и автентичност. Веднъж седмично подробно се преглеждат журналите от произволно избрана операция.

При инцидент или съмнение за инцидент по сигурността, се преглеждат всички журнални файлове.

3. Период на съхранение

Журналите се съхраняват на дисковете на информационните системи, докато се достигне определен размер. През това време те са достъпни онлайн за всички упълномощени лица.

При достигането на определен размер, журналите се архивират. Архивите се пазят най-малко 10 (десет) години от получаване на информацията и сключване на договор с клиента.

4. Защита на журналните файлове

Журналните файлове се криптират при архивиране, като ключа за архивиране е под изключителния контрол на Мениджър ИТ Сигурност.

Журналните файлове могат да се преглеждат само от упълномощени лица и лица, за които прегледа и анализа на тези файлове е пряко задължение. Достъпът до журналните файлове е конфигуриран по начин, позволяващ:

- Само упълномощени лица – проверяващи и служители на ДУУ, да имат право да преглеждат файловете;
- Само Мениджър ИТ Сигурност да има право да архивира и изтрива файлове, съдържащи регистрирани събития;
- Откриване на всяко нарушение на целостта на данните и гарантиране, че всеки запис е автентичен (не е фалшифициран).

Никой няма право да модифицира съдържанието на журналните файлове.

Горните правила за достъп важат и за архивирани и предадени за съхранение записи.

5. Архивиране на журналните файлове

СЕП България ежемесечно архивира журналите за събития и записите за дейностите по техния преглед, анализ и статистика, открити заплахи и предприети мерки. Архивите се пазят в основния и отдалечен офис на СЕП България. Архивните копия, които са в електронен вид, може да са с удостоверено време на създаването им.

X. Известяване за събития

СЕП България осъществява наблюдение и анализ на системните събития, като при откриване на подозрително събитие се известяват отговорните лица.

Уведомените лица предприемат съответните действия за защита на системата в зависимост от заплахата.

XI. Оценка на уязвимостите

СЕП България в качеството си на ДУУ и всички лица, предоставящи удостоверителни услуги от негово име и за негова сметка, периодично извършват оценка на уязвимостите, като се анализират вътрешните процедури, приложенията и информационните системи.

XII. Архивиране на записите

Всички данни и файлове, свързани с регистрацията на потребителите на удостоверителни услуги и сигурността на системите, информацията, предоставена от Титуляра/Автора, издадените удостоверения, генерираните CRL, ключовете, използвани от РО и цялата кореспонденция между СЕП България и Титуляра/Автора, или упълномощени представители се архивират. Архивират се документите и данните, използвани за идентификация на Титуляра/Автора и проверка на идентичността, съответно самоличността на Титуляра/Автора.

Документите, представени в хартиена форма, когато е възможно, се преобразуват в електронен формат и се архивират.

СЕП България поддържа електронни и хартиени архиви. Архивът се съхранява за срок от 10 (десет) години.

1. Типове архивни данни

Архивират се следните данни:

- Информацията от проверките и оценки на логическата и физическа защита на УО и РО и публичния електронен регистър;
- База данни с потребителите на удостоверителни услуги;
- База данни с удостоверенията;
- Генерираните CRL;
- История на управление на ключовете на УО на ДУУ;
- История на потребителските ключове, генерация, предоставяне, унищожаване на архивни копия след предоставянето им на автора;
- Вътрешна и външна кореспонденция, в хартиена или електронна форма, между СЕП България и потребителите на удостоверителни услуги и РО;
- Документи и данни, използвани в процеса на проверка на идентичността съответно самоличността на Титуляра/Автора.

2. Честота на архивиране

Данните се архивират на различни нива според следния времеви график:

- База данни с потребителските удостоверения и данните на Титуляра/Автора се съхраняват на сървърите на СЕП България до 10 (десет) години от момента на издаване на удостоверението или последното действие по неговото управление, след което се архивира на оптичен носител без възможност за добавяне или изтриване на записи.
- Носителите с данните се предават в документален архив за съхранение.

Списъкът с прекратени удостоверения, кореспонденцията и подадените искания, както и взетите решения, се съхраняват според по-горе описаната схема.

3. Период на съхраняване в архив

Архивираните данни в хартиена или електронна форма, се съхраняват за период от минимум 10 (десет) години. След изтичане на определения период, архивираните данни се унищожават. При унищожаване на ключове и удостоверения се прилагат съответни процедури.

4. Защита на архива

СЕП България поддържа средства и предприема мерки, позволяващи да се поддържа целостта и достъпността на данните от архива. Мерките включват следните основни правила:

- Само упълномощени лица, на доверени позиции имат право на достъп до архива;
- Архивът се защитава от модификация, като записите се подписват с електронен подпис и данните се архивират върху носители за еднократен запис;
- Поддържа се повече от едно копие на различни, физически отдалечени места с цел защита от унищожаване на архива;
- За да предпази архива от повреди поради стареене на носителите, на които е бил записан, архивът периодично се прехвърля на нови носители, а старите се унищожават. Периодично се подменят носителите, на които се правят ежедневните архиви;
- Формата на данните и носителите, на които се записва или прехвърля запис на архива, се променя при необходимост, за да се предпази от невъзможност за ползване поради промяна на технологиите, алгоритмите, форматите на данни и хардуера за архивиране;
- Поддържат се средства за достъп до архиви, създадени в минал период от време.

5. Резервни копия на архива – процедура

Резервните копия позволяват пълно възстановяване в случай на необходимост на основните данни, необходими за правилно функциониране на ДУУ. За да се обезпечи тази цел, на следните данни и файлове се прави резервно копие:

- Инсталационните дискове със системните приложения;
- Инсталационните дискове с приложенията на УО и РО;
- WWW сървър и дисковете с инсталация на публичния електронен регистър;
- Данните от публичния електронен регистър, бази данни с потребители на удостоверителни услуги и системни бази данни;
- Други данни, свързани с дейността на СЕП България, като ДУУ;
- Журналните файлове.

Методите за създаване на резервни копия, използвани от СЕП България са:

- Ежедневни резервни копия – правят се резервни копия на базите данни ежедневно и могат да се използват за възстановяване на загубени данни;
- Седмични резервни копия – използват се за възстановяване на системата при повреда на хардуера или необходимост от възстановяване на настройките на системния софтуер към определен момент от време. Тези копия отразяват изцяло текущото състояние на информационните системи.

СЕП България може да възстанови изцяло своите системи в рамките на 48 часа.

Подробно описание на данните и процедурите, по които се правят резервните копия е част от документацията за техническата инфраструктура на ДУУ. Тази документация няма публичен характер и е достъпна изключително за упълномощения персонал и проверяващи дейността на СЕП България.

6. Изискване за удостоверено време за записите

При възможност, за всички архивирани данни се удостоверява точното време, към което те са били създадени.

7. Процедура за проверка на архивираната информация

За да се провери целостта на архивираната информация, данните периодично се тестват и проверяват като се сверяват с оригиналните данни, ако те все още са налични в оперативните информационни системи.

Тази дейност се осъществява само от оторизирани длъжностни лица и се отразява в журнала на системата.

В случай, че се открие повреда в данните вземат незабавни мерки по възстановяване на целостта на архива.

XIII. Смяна на ключовете

УО на СЕП България подменя ключовете, с които подписва издаваните удостоверения и списък с прекратени удостоверения, като спазва следната процедура:

- Издава се специално удостоверение от УО, за потребителите, които притежават старото удостоверение на УО, с което се гарантира защитената обмяна на новото удостоверение. По този начин се позволява на новите потребители да получат по сигурен начин старото удостоверение за целите на проверката.
- Всяка смяна на ключовете се обявява предварително на сайта на ДУУ, уведомява се КРС всички Автори/Титуляри по надлежния ред.
- Периодичността на смяната на ключове се определя от периода на валидност на удостоверенията на базовия и оперативния УО.

От момента на смяна на ключа, УО на СЕП България използва само новия частен ключ за подписване на издадените удостоверения.

XIV. Компрометиране и възстановяване след бедствия и аварии

СЕП България следва строги процедури за случаите на компрометиране на частния ключ и/или възникване на авария, за да се гарантира възстановяване нивото на предоставяне на удостоверителните услуги. Тези процедури се изпълняват в съответствие с одобрен план за действие при аварии и извънредни обстоятелства.

1. Реакция при нарушения на сигурността

Нарушенията на сигурността на информационните системи се докладват незабавно след откриването им на ръководителя на звеното, който отговаря за тяхното отстраняване.

Служителите на СЕП България имат права и задължения да правят предложения и съответно да докладват за допускани нарушения относно сигурността.

Неизправности в софтуера се докладват на оперативния ръководител или на определен администратор.

Мерките и процедурите за действие при възникване на технически проблеми във връзка със сигурността са описани по-долу в този раздел.

2. Щети по компютърни ресурси, софтуер и/или данни

Политиката за сигурност, прилагана от СЕП България, определя следните основни заплахи по отношение на непрекъсваемостта на предлагане на услуги:

- Физическо разрушаване на системите на СЕП България, включително мрежови ресурси – тази заплаха включва разрушения от всякакъв най-често случаен характер;
- Неизправност в работата на софтуера и приложенията, липса/невъзможност за достъп до данните – тези неизправности са причинени от неправилно функциониране на операционни системи и потребителски приложения, в резултат на зловредни кодове;
- Загуба на важни мрежови услуги – загуба на захранване и физическо прекъсване на кабели;
- Повреда в използвания хардуер.

За да се предотврати и ограничи влиянието на горните заплахи, СЕП България използва следните практики и политики за сигурност:

2.1. План за възстановяване след авария или природно бедствие

Уведомяват се всички потребители на удостоверителни услуги по подходящ начин за текущата ситуация и всички ограничения при предлагане на услугите, свързани с функционирането на информационните системи и мрежовата инфраструктура. Планът включва редица действия в зависимост от това коя част от системата е неизправна или функционира с проблеми:

- Правят се огледални копия на дисковете на всички сървъри и работни станции. Всяко резервно копие се съхранява на две места, в СЕП България и резервен център за обработка на данни;
- Периодично се правят резервни копия на базите данни. Копията съдържат всички подадени искания, издадените, подновени и прекратени удостоверения. Копията се съхраняват на гореописаните места;
- Периодично се прави пълно резервно копие на всеки сървър. Това копие съдържа всички подадени искания, журнала на събитията, издадените, подновените и прекратените удостоверения. Копието се съхранява на сигурно място извън офис на СЕП България;
- Ключовете на СЕП България, разделени на части, се държат от лица на доверени позиции и се съхраняват от тях;
- Разполага се с резервно оборудване за подмяна на повредени сървъри, дискове и комуникационно оборудване;
- Процедурите се тестват по отношение на всеки компонент на системата поне веднъж годишно.

2.2. Управление на промените

Инсталацията и обновяване на софтуера до по-нови версии на оперативните системи се извършва само след провеждане на тестови инсталации и обновявания върху тестова система. Всяка модификация на системите се извършва след одобрение от Администратора по сигурността. Предварително се вземат мерки за възстановяване на системите към състоянието им преди инсталацията или обновяването в случай на проблеми при функционирането.

2.3. Резервни системи

В случай на авария или природно бедствие СЕП България активира в рамките на 24 часа резервни системи, които да подменят основните функции на ДУУ, докато основните системи бъдат възстановени. Поради наличието на резервни копия на системите и резервен хардуер СЕП България:

- Активира резервния център, за да се осигури предоставяне на удостоверителни услуги;
- Обработва натрупаните и необработените искания за прекратяване;
- Обработва други подадени искания от потребителите на удостоверителни услуги.

2.4. Създаване на резервни копия

СЕП България създава резервни копия на всички данни така, че да е възможно възстановяването на системата към произволен момент от време. Копия се правят и на всички данни, които имат определящо значение по отношение на информационната сигурност на СЕП България. Копията се правят периодично и се съхраняват извън офис на СЕП България. Копията се защитават с пароли и се криптират.

3. Допълнителни дейности

За да се предотврати спиране на дейностите на ДУУ поради отпадане на захранването, е осигурено резервно захранване. На всеки шест месеца се провеждат тестове на резервното захранване.

4. Компрометиране на частния ключ на УО

В случай, че частният ключ на УО на СЕП България се компрометира или има подозрение за компрометиране, се предприемат следните действия:

- УО генерира нова ключова двойка и ново удостоверение;
- Уведомява всички потребители на удостоверителни услуги;
- Уведомява Комисията за регулиране на съобщенията;
- Удостоверенията, подписани с компрометирания ключ, се прекратяват със съответната причина за прекратяване;
- Всички удостоверения в удостоверителния път на компрометираното удостоверение се прекратяват със съответната причина за прекратяване;
- Генерират се нови удостоверения за Титулярите/Авторите;
- Новите удостоверения се издават за сметка на СЕП България.

5. Продължаване на дейностите след възстановяване от бедствия и авария

След всяко възстановяване на системата от авария, Мениджър ИТ Сигурност и системният администратор извършват следните дейности:

- При необходимост сменят всички пароли;
- Преглеждат и дават/отнемат права за достъп до системни ресурси;
- Сменят всички кодове и ПИН, отнасящи се до физически достъп до системни компоненти;
- Преглеждат и анализират казуса свързан с аварията. Коригират и допълват плана за действие, политиката за сигурност и правилата за физически достъп до помещенията и системните компоненти;
- Информират потребителите на системата за възстановяване на системните дейности;
- Инициират прекратяване или прехвърляне на дейността на съответната система.

XV. Прекратяване или прехвърляне на дейността на УО

СЕП България уведомява КРС и потребителите за намерението си за прекратяване на дейността в законоустановените срокове, като изрично посочва дали прехвърля дейността си на друг доставчик на удостоверителни услуги.

При прехвърляне на дейността на друг доставчик, СЕП България предава цялата документация, свързана с дейността му на доставчика, на когото е прехвърлил дейността. Доставчикът на удостоверителни услуги, който е поел управлението на удостоверенията на СЕП България, е длъжен да ги поддържа до изтичане на срока на тяхната валидност при условията на тяхното издаване, без допълнително заплащане от страна на Клиента.

СЕП България прехвърля дейността си само на акредитиран доставчик на удостоверителни услуги и му предава цялата документация, свързана с дейността.

СЕП България уведомява незабавно Комисията за регулиране на съобщенията в случай на започване на производство за обявяване в несъстоятелност, производство по ликвидация или производство за прекратяване на ДУУ.

При невъзможност СЕП България да прехвърли дейността си на друг регистриран доставчик, той прекратява действието на удостоверенията и предава документацията на Комисията за регулиране на съобщенията, незабавно след прекратяването на дейността си. Комисията за регулиране на съобщенията поддържа Регистър на прекратените удостоверения на доставчик на удостоверителни услуги, след прекратяване на неговата дейност.

XVI. Прекратяване или прехвърляне на дейността на РО

Регистриращ орган на СЕП България може да прекрати своята дейност:

- При изтичане на срока по договора, уреждащ отношенията между СЕП България и лицето, опериращо като РО;
- При нарушаване на договора и/или неспазване на разпоредбите на настоящия Наръчник за потребителя;
- В случаите, уговорени в договора, уреждащ отношенията между СЕП България и лицето, опериращо като РО.

XVII. Техническа и технологична сигурност

В този раздел се описват процедурите за генериране и управление на криптографските ключови двойки на УО, РО и Титуляра/Автора, и съпътстващите генерирането технически контроли.

1. Генериране и инсталиране на ключови двойки

Управлението на ключовете се осъществява в защитена среда чрез използването на специализиран криптографски хардуер и се реализира от собственика на ключовете.

СЕП България притежава всички ключове и удостоверения на УО, функциониращи в информационна система:

- Базовия Удостоверяващ орган на СЕП България – SEP Root CA;
- Оперативния Удостоверяващ орган – eSign QES CA.

Частният ключ на SEP Root CA се използва изключително и само за подписване на публичните ключове на: eSign QES CA; SEP TSA и подписване на издавания от него CRL.

Ключовата двойка на оперативния удостоверяващ орган се използва изключително за подписване на издаваните удостоверения на крайни клиенти, eSign OCSP и CRL.

От оперативния удостоверяващ орган се подписват и инфраструктурните удостоверения, необходими за функциониране на системата за доставка на удостоверителни услуги, като:

- Подписване на съобщенията, изпращани на Титуляра/Автора и РО;
- Размяна на ключове за криптирана комуникация между УО и РО.

1.1. Генериране на ключови двойки

Всички ключове на УО се генерират в защитените помещения на СЕП България, следвайки одобрена от Ръководството на Доставчика вътрешна процедура и в присъствието на доверени лица от персонала, нотариус/юрисконсулт и представител от висшето ръководство на СЕП България.

Ключовите двойки се генерират, като се използва отделена работна станция, свързана с криптографския модул, съответстващ на FIPS 140-2 Level 3 или на аналогични изисквания за сигурност.

Ключовете на УО се генерират в съответствие с предварително тествана и одобрена процедура. Водят се записи за всички действия, изпълнявани по време на генерацията. Всеки запис съдържа описание на действието, дата и подпис на лицето, реализирало действието и лицето, контролиращо изпълнението на действието. Протокол от процедурата се подписва от всички присъстващи.

Ключовете на РО се генерират от системния оператор под наблюдението на Мениджър ИТ Сигурност, като се използва криптографския модул, съответстващ на FIPS 140-2 Level 2 или на аналогични изисквания за сигурност. Използват се за автентикиране на исканията на Титуляра/Автора, изпращани от РО към УО.

Титулярът/Авторът инициира генерирането на своята ключова двойка самостоятелно или чрез РО. Двойката ключове на Автор/Титуляр към Удостоверение за КЕП се генерира само в одобрен от Доставчика SSCD, проверен за нивото на сигурност и за успешна работа през интерфейсите на инфраструктурата на ДУУ.

1.1.1. Генериране на ключовете на SEP Root CA

Процедурата се изпълнява при инициализация на системата за доставка на удостоверителни услуги на СЕП България.

Процедурата включва:

- Генериране на базова ключова двойка;
- Инсталиране на частния ключ в криптографския модул;
- Издаване на базово, самоподписано удостоверение на ДУУ, съдържащо публичния ключ и подписано с частния ключ.

Ключовата двойка се използва за подписване на удостоверението на оперативния удостоверяващ орган, „Списъка на прекратените удостоверения“ на базовия удостоверяващ орган и удостоверението за проверка на удостоверено време.

1.1.2. Смяна на ключовете на SEP Root CA

Процедура за подмяна на ключовата двойка се реализира при изтичане на периода на валидност на базовото удостоверение. Процедурата стартира най-малко една година преди да изтече периода на валидност на старата ключова двойка на СЕП България. СЕП България издава ново удостоверение на SEP Root CA и за период от една година СЕП България поддържа новото и старото удостоверение, след което старото изтича и остава валидно новото удостоверение на SEP Root CA.

Потребителите на удостоверителни услуги могат през тази година да използват старото удостоверение, за да получат по сигурен и надежден начин новото базово удостоверение на СЕП България.

От момента на генериране на новата ключова двойка, СЕП България деактивира стария частен ключ и за подписване се използва само новия частен ключ.

1.1.3. Смяна на ключовете на оперативния УО на ДУУ

При смяна на ключовете на оперативния УО се следва процедурата, описана в т. 1.1.2 като новото оперативно удостоверение се издава от SEP Root CA и се подписва с новия частен ключ.

1.2. Предоставяне на частния ключ на автора

При издаване на Удостоверение за КЕП Титулярът/Авторът генерира ключовата двойка чрез SSCD.

В случай, че Титулярът/Авторът изрично заяви генерирането на двойката ключове на ДУУ, това става по сигурен и надежден начин, след което което ДУУ предоставя на Титуляра/Автора данните за достъп до SSCD, при спазване на реда, предвиден в "Политиката при предоставяне на удостоверителни услуги".

1.3. Предоставяне на публичния ключ на УО

Публичния ключ от двойката се предоставя за удостоверяване от УО. Това става като се спазва изискванията посочени в PKCS#10 Certification Request Syntax.

1.4. Предоставяне на публичния ключ на УО до доверяващите се страни

Публичният ключ на УО на СЕП България се разпространява като част от удостоверенията за електронен подпис, издавани от СЕП България. Базовото удостоверение на СЕП България е самоподписано удостоверение.

СЕП България разпространява своите базово и оперативно удостоверения по следния начин:

- Чрез публикуване в публичния електронен регистър на ДУУ, намиращ се на електронната страница на СЕП България;
- Заедно с потребителски пакет от определени приложения;
- Новото базово удостоверение се предоставя за изтегляне на електронната страница на СЕП България при осигуряване на защита от подправяне.

При смяна на ключовете на УО в публичния електронен регистър се публикуват новите удостоверения и се пази архив на всички стари удостоверения.

2. Дължина на ключовете

Дължината на използваните ключове е в съответствие с НИАСПКЕП и е както следва:

собственик на ключа	параметри на ключа	
	RSA	валидност
SEP Root CA	4096 bit	20 години
eSign QES CA	2048 bit	10 години

Параметрите на генерираните ключове от СЕП България са в съответствие с НИАСПКЕП.

3. Защита на частния ключ

Частните ключове на ДУУ и клиентите на удостоверителните му услуги се генерират, съхраняват и използват посредством устройства за сигурно създаване на ЕП. Хардуерните криптографски модули, които използва СЕП България са в съответствие на чл. 26 от НДДУУРНПИПУУ, като създаването, съхраняването и използването на частния ключ на ДУУ се извършват в система със защитен профил, определен в съответствие с общите изисквания (CC), ниво на сигурност EAL 4 или по-високо съгласно стандарта ISO 15408 или друга спецификация, определяща еквивалентни нива на сигурността.

СЕП България издава Удостоверения и удостоверява предоставени от Титуляра/Автора публични ключове, ако ключовата двойка е генерирана чрез SSCD с ниво на сигурност EAL 3 или по-високо.

3.1. Достъп до частния ключ на доставчика

Достъпът до частните ключове на ДУУ, използвани за подписване на Удостоверения за КЕП, се осъществява съвместно от най-малко двама служители на доверени позиции във физически защитена среда.

3.2. Резервни копия на частния ключ

СЕП България прави копия на частния си ключ с цел възстановяване след авария или повреда в използваните системи.

Частните ключове на ДУУ, използвани за подписване на Удостоверения за КЕП, се архивират, съхраняват и възстановяват съвместно най-малко от двама служители на доверени позиции във физически защитена среда.

3.3. Архивиране на частния ключ

СЕП България не поддържа архив на частните ключове след изтичане на жизнения им цикъл. Всички частни ключове в края на своя жизнен цикъл се унищожават по такъв начин, че да се предотврати тяхното използване.

3.4. Трансфер на частния ключ от и към криптомодула

Трансфер на частния ключ на СЕП България от криптомодул, може да се наложи при правене на архивно копие на ключа.

Трансфер на частния ключ на СЕП България към криптомодул, може да се наложи при възстановяване след авария или при миграция към друг криптомодул.

При трансфер частният ключсе разделя на части и всяка част се криптира с ключ. Достъпът до този ключ е чрез парола, известна само на държателя на секретната част.

3.5. Съхраняване на частния ключ в криптомодула

СЕП България съхранява своите частни ключове в криптомодули, достъпът до които се осъществява най-малко от двама надлежно овластени служители на доверени позиции.

3.6. Активиране на частния ключ

Частният ключ на СЕП България се активира след трансфер на всички поделени секретни части в криптомодула и въвеждане на ПИН или код за активиране от всеки държател на поделена част. Активирането се извършва най-малко от двама надлежно овластени служители на доверени позиции.

3.7. Деактивиране на частния ключ

Частният ключ на СЕП България се деактивира като се стартира процедура по инициализация на криптомодула. Деактивирането се извършва най-малко от двама надлежно овластени служители на доверени позиции.

3.8. Унищожаване на частния ключ

Частният ключ на СЕП България в криптомодула се унищожава, като се стартира процедура по инициализация на криптомодула. Унищожаването се извършва най-малко от двама надлежно овластени служители на доверени позиции.

Следва се процедура за унищожаване на всички поделени части на частния ключ на ДУУ.

3.9. Сертификация на криптомодула

Използваните криптомодули от СЕП България при предоставяне на удостоверителни услуги отговарят на изискванията на ЗЕДЕП и подзаконовите актове по неговото прилагане. СЕП България предоставя сертификати за криптографска сигурност на използваните криптомодули.

XVIII. Други аспекти от управлението на ключовете

1. Архивиране на публичния ключ

Публичните ключове на СЕП България се съхраняват като част от Удостоверение за КЕП и се архивират 10 (десет) години след като е изтекъл периода на тяхната валидност. До момента на архивиране удостоверенията на УО на СЕП България са достъпни чрез публичния електронен регистър.

2. Период на валидност на удостоверенията и използване на ключовете

Максималния период на валидност на удостоверенията, използвани от СЕП България при предоставяне на удостоверителни услуги и максималният период на използване на съответните частни ключове е като следва:

Удостоверение	**Период на**	
	валидност на удостоверението	**ползване на частния ключ**
SEP Root CA	20 години	19 години
eSign QES CA	10 години	9 години
SEP TSA	10 години	10 години

Удостоверение	Период на	
	валидност на удостоверението	ползване на частния ключ
eSign OCSP	10 години	10 години
eSign Qualified Private	3 години	3 години
eSign Qualified Organization	3 години	3 години
eSign Qualified Profession	3 години	3 години

3. Данни за активиране

Данните за активиране на ключовите двойки, ПИН и/или пароли и кодове на СЕП България са разделени на защитени части и се държат от различни служители на доверени позиции. СЕП България следва специална процедура по събирането и използването на данните за активиране, която гарантира защита от неправомерно и неоторизирано ползване на ключовите двойки. Всяка поделена част е защитена с отделен ПИН и/или парола или код. Данните за активиране се генерират по защитен и сигурен начин по време на процеса на генериране на поделените части.

Данните за активиране на достъпа до частния ключ на клиентите на ДУУ се генерират по време на процедурата по издаване на Удостоверение за КЕП, когато услугата по издаване е свързана с предоставяне на SSCD на Клиента.

Данните за достъп до клиентския криптомодул (PIN/PUK кодове) се предоставят на Клиента в запечатан плик или по друг сигурен и надежден начин, осигуряващ невъзможността за тяхното компрометиране.

Допуска се данните за достъп до клиентския криптомодул да се предоставят до Автора чрез Титуляра или негов пълномощник, когато това е заявено в Искането.

Титулярът/Авторът са длъжни да сменят данните за достъп до предоставения им клиетски криптомодул (SSCD) веднага след като го получат.

XIX. Управление на компютърната сигурност

1. Технически изисквания

Описаните техническите изисквания се отнасят до компютърните системи и инсталирания системен софтуер, използвани за системни операции. Защитата на компютърната система се осъществява на ниво операционна система, приложен софтуер и физически достъп.

Компютърните системи, разположени в УО, реализират следните контроли:

- Задължителна автентикация на ниво операционна система и системно приложение;
- Водене на журнал за действията на операторите;
- Достъпа до системите се осъществява само от надлежно овластени служители на СЕП България;
- Криптографски се защитава обмена и базите данни.

1.1. Оценка на сигурността

Периодично СЕП България оценява сигурността на използваните компютърни системи и технологии за предоставяне на удостоверителни услуги.

1.2. Технически контроли

2. Управление контролите за информационна сигурност

Целта на управлението на контролите за информационна сигурност е да гарантира, че системите на СЕП България функционират правилно, в съответствие с направените настройки и по начина, по който са конфигурирани.

Всички промени в системните настройки и конфигурации се тестват, наблюдават и документират.

2.1. Мрежова сигурност

Сървърите и доверените работни станции на СЕП България са свързани в отделена вътрешна локална мрежа. Достъпът от интернет се контролира от защитна стена и сензор за откриване на проникване.

СЕП България предприема мерки, за да гарантира безотказна работа на системите по предоставяне на удостоверителни услуги и гарантиране на надеждността и сигурността на обмена на данни между РО и УО. взети са допълнителни мерки по проследяване и отразяване на опити за проникване и блокиране на операциите по предоставяне на удостоверителни услуги.

XX. Профили на удостоверения, "Списък на прекратените удостоверения" и OCSP

Профилите на удостоверенията за електронен подпис и „Списъка на прекратените удостоверения" са дефинирани в съответствие с RFC 3280 и ITU-T X.509 v.3. Профилът за OCSP е в съответствие с RFC 2560, а за удостоверяване на време е в съответствие с RFC 3161.

1. Профили на удостоверенията

Полетата, включени в съдържанието на Удостоверенията и тяхната интерпретация формират профилите на издаваните удостоверения в цялата йерархия на СЕП България.

2. Съдържание на Удостоверението

СЕП България поддържа определен набор от полета и атрибути в издаваните Удостоверения за КЕП. Наличието или отсъствието на определени атрибути в полетата зависи от типа издадено Удостоверение за КЕП.

СЕП България определя и набор от разширения на Удостоверенията. Част от разширенията се отбелязват като критични, за да се гарантира правилното използване на Удостоверенията. Приложенията, които ползват Удостоверенията, трябва да отхвърлят всяко Удостоверение, което съдържа критично разширение, което е неразпознато. По-долу е дадено общо описание на поддържаните полета и разширения от СЕП България.

- Version: трета версия (X.509 v.3);
- SerialNumber: уникален сериен номер на Удостоверението в рамките на издаващия удостоверяващия орган;

- Signature: идентификатор на алгоритъма използван от издаващия удостоверяващия орган за подписване на Удостоверението;
- Issuer: Distinguished Name на издаващия удостоверяващ орган;
- Validity: периода на валидност на Удостоверението. Описва се с начална дата (notBefore) и крайна дата (notAfter) за периода на валидност;
- Subject: Distinguished Name на Титуляра/Автора;
- SubjectPublicKeyInfo: стойността на публичния ключ заедно с идентификатора на асоциирания с него алгоритъм;
- SignatureAlgorithm: идентификатор на алгоритъма, използван от издаващия удостоверяващия орган за подписване на Удостоверението;
- SignatureValue: електронния подпис на Удостоверението. (изчислява се по всички полета на основното поле: version, serialNumber, signature, issuer, validity, subject, subjectPublicKeyInfo; като се ползва signatureAlgorithm).

В следващата таблица са посочени възможните стойности на отделните полета:

име на поле	стойност или ограничение на стойността	
version	Version 3	
serialNumber	уникален сериен номер на удостоверението в рамките на издаващия удостоверяващия орган	
signature	sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5) id-ecdsa-with-sha1 (OID: 1.2.840.10045.4.1)	
issuer (Distinguished Name)	countryName	BG
	localityName	Sofia
	organizationName	System for Electronic Payments/SEP Bulgaria JSC
	organizationalUnitName	SEP
	commonName	eSign QES CA
	Street	1 Zlatovrah Str.
validity	notBefore	UTCTime формат
	notAfter	UTCTime формат
subject (Distinguished Name)	Distinguished Name на Титуляра/Автора в съответствие с изискванията на X.501. Стойностите на атрибутите са в зависимост от типа издавано Удостоверение за КЕП.	

име на поле	стойност или ограничение на стойността	
	*C, Country	Определя контекста, в който се разглеждат останалите атрибути.
	ST, State or Province	При използване съдържат географска информация свързана с Титуляра. Ако присъства organizationName то тази информация се отнася до организацията.
	*L, Location	
	O, Organization	При използване съдържат името на организацията, с която е асоцииран Титуляра и съответно свързана с организацията информация. Съдържат типа на издаденото Удостоверение
	OU, Organization Unit	
	UID, Unique Identifier	EGN/EIK на Титуляра
	*CN, Common Name	Име/псевдоном на Автора
	T, Title	При използване съдържа позицията или функцията на Автора в организацията на Титуляра.
	Street	Адрес – ж. к., ул., ном., бл., ап. на Автора
	PostalCode	Пощенски код на Титуляра
	Phone	Телефон на Титуляра
	*EmailAddress	e-mail на Автора за кореспонденция от името на Титуляра
Key Usage	{digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment, keyCertSign, cRLSign}	
Enhanced Key Usage	{serverAuth, clientAuth, codeSigning, emailProtection, timeStamping, OCSPSigning}	

име на поле	стойност или ограничение на стойността
Certificate Policies	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.30299.2.5 [1,1]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text=eSign QES CA [1,2]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://eSign.bg [2]Certificate Policy: Policy Identifier=1.3.6.1.4.1.30299 [2,1]Policy Qualifier Info: Policy Qualifier Id=User Notice [2,2]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.crc.bg/
CRL Distribution Points	1]CRL Distribution Point Distribution Point Name: Full Name URL=http://crl.sep.bg/SEP_root_ca.crl

име на поле	стойност или ограничение на стойността
Authority Information Access	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.sep.bg
Basic Constraints	cA: yes/no, Path Length Constraint=None
Subject Alternative Name	Адрес на Автора
Authority Key Identifier	
Subject Key Identifier	
subjectPublicKeyInfo	Публичният ключ на Автора и алгоритъмът, с който се използва
Qualified Certificate Statements	Посочва, че Удостоверението е издадено като удостоверение за квалифициран електронен подпис
signatureAlgorithm	sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5) id-ecdsa-with-sha1 (OID: 1.2.840.10045.4.1)
signatureValue	Електронен подпис на ДУУ

Стандартни разширения

СЕП България поддържа следните разширения:

- Authority Key Identifier: идентифицира публичния ключ на УО, съответстващ на частния ключ, използван за подписване на издаденото удостоверение. Това разширение не е критично;
- Subject Key Identifier: идентифицира удостоверение, което има определен публичен ключ. Това поле не е критично;
- Key Usage: дефинира целите, за които може да се използва ключа от удостоверението. Това налага ограничения относно проверките, които могат да се правят чрез публичния ключ от удостоверението. Това разширение позволява да се разграничи ползването на различните ключове. Възможни стойности са:
  - digitalSignature: за проверка на електронен подпис;
  - nonRepudiation: за гарантиране на факта на полагане на електронен подпис;
  - keyEncipherment: за сигурна размяна на ключове;
  - dataEncipherment: за криптиране на данни;

- keyCertSign: за проверка на електронен подпис на удостоверения;
- cRLSign: за проверка на електронен подпис на CRL;
- разширението Key Usage е критично.

- Enhanced Key Usage: дефинира приложенията, за които може да се използва ключа от удостоверението. Това разширение определя една или няколко области в добавка към Key Usage полето за допустимо използване на удостоверението. Тези области следва да се тълкуват като ограничение по отношение на допустимото използване. Възможни са един или комбинация от няколко от следните елементи:
  - serverAuth: за TLS WWW автентификация на сървър. Съвместимост с digitalSignature, keyEncipherment или keyAgreement;
  - clientAuth: за TLS WWW автентификация за клиент. Съвместимост с digitalSignature и/или keyAgreement;
  - codeSigning: за подписване на изпълним код най често разпространяван през интернет Съвместимост с digitalSignature;
  - emailProtection: за защита на E-mail. Съвместимост digitalSignature, nonRepudiation, и/или (keyEncipherment или keyAgreement);
  - timeStamping: привързва хеш на обект към определено време. Съвместимост с digitalSignature и/или nonRepudiation;
  - OCSPSigning: подписване на OCSP отговор Съвместимост с digitalSignature и/или nonRepudiation;

Това разширение не е критично.

При наличие на двете разширения Key Usage и Enhanced Key Usage, то двете разширения се обработват от приложението по отделно и Удостоверението се използва за цели, които са съвместими и с двете разширения. В противен случай не се използва за никакви цели.

- Certificate Policies: идентифицира една или няколко политики, чрез OID идентификатор на политиката и допълнителни квалификатори на политика:
- CPSuri: указател/препратка, под формата на URL, към мястото, където се намира „Практика при предоставяне на удостоверителни услуги";
- UserNotice: препратка към текст, който да се покаже на доверяващите се страни при проверка на КЕП. Текстът може да се изведе чрез препратка noticeRef или да бъде част от удостоверението explicitText;

Разширението не е критично.

- Policy Mappings: некритично разширение съдържащо една или няколко двойки OID, за които се дефинира еквивалентност на политиките;
- Issuer Alternative Names: алтернативно име на издателя на удостоверението. Полето не е критично;
- Subject Alternative Name: алтернативно име на титуляра/автора на удостоверението. Полето не е критично;
- Basic Constraints: идентифицира УО (показва, че публичния ключ принадлежи на УО) и броя на УО в йерархията до крайното клиентско удостоверение. Може да е критично за УО и да не е критично в останалите случаи. Ползва се заедно с keyCertSign;
- CRL Distribution Points: показва как и от къде може да се получи CRL. Може да има повече от един механизъм за извличане на CRL, например от LDAP или чрез HTTP. Полето не е критично;
- Authority Information Access: дефинира достъп до информация или услуги предоставяни от издателя на удостоверението. Най-често за On-line проверка за валидност на удостоверенията. Полето не е критично;
- Qualified Certificate Statements: показва, че удостоверението е издадено като удостоверение за квалифициран електронен подпис.

XXI. Проверка и контрол на дейността

1. Честота и обстоятелства на проверките

Контрол върху дейността на СЕП България, като ДУУ съгласно ЗЕДЕП се осъществява от Комисията за регулиране на съобщенията и Изпълнителна агенция „Българска служба за акредитация“.

СЕП България осъществява постоянен вътрешен контрол, който се извършва от вътрешни одитори.

За целите на вътрешния контрол се провеждат периодично пълни или частични проверки на обособени дейности и/или звена от инфраструктурата за предоставяне на удостоверителни услуги.

СЕП България осъществява постоянен контрол върху дейността на Регистриращите органи.

2. Идентификация и квалификация на проверяващите

Лицата, осъществяващи проверките, са изрично упълномощени/оторизирани от Комисията за регулиране на съобщенията, от Изпълнителна агенция „Българска служба за акредитация“ или от СЕП България.

За осъществяване на проверки може да се привличат и външни организации и/или лица, които са акредитирани за извършване на такива проверки.

Проверки на дейността на Регистриращите органи се извършват от служители на ДУУ, изрично оторизирани от СЕП България или външна проверяваща организация.

3. Избягване конфликт на интереси

Отношенията между външните проверяващи лица, извън случаите на проверка от страна на държавни органи и СЕП България, се уреждат с писмен договор.

4. Обхват и детайлност на проверките

Обхватът и детайлността на извършваните проверки е съобразно вида на осъществявания контрол и проверяваните звена.

В обхвата на вътрешна проверка са всички дейности, документи и обстоятелства от оперирането на ДУУ, които могат да включват, но не се ограничават до:

- Съответствието на процедурите и практиките на СЕП България с дефинираните в „Наръчника за потребителя“ процедури и политики;
- Спазване на процедурите и практиките определени в „Наръчника за потребителя“ от служителите и звената за предоставяне на удостоверителни услуги;
- Спазване на процедурите и практиките определени в „Наръчника за потребителя“ от външните Регистриращи органи;
- Управлението на инфраструктурата за предоставяне на удостоверителните услуги.

5. Предприемане на действия за отстраняване на недостатъците

Докладът от проверката се разглежда от управляващия мениджмънт на СЕП България. Анализират се несъответствията и се предприемат мерки за отстраняването им.

6. Съобщаване на резултатите

Резултатите от проверките стават достояние на проверяваните звена. Водят се записи за проверките. Резултатите от направените проверки се съхраняват по условията и реда на Наръчник за потребителя.

XXII. Търговски и правни условия

1. Тарифа за предоставяне на удостоверителните услуги

СЕП България в качеството си на ДУУ определя цени на предоставяните от него удостоверителни услуги. Информация за цените на удостоверителните услуги и на свързаните с тяхното предоставяне административни услуги се публикуват в „Тарифа на СЕП България за предоставяне на удостоверителни услуги“ (Тарифа) на електронната страница на СЕП България.

СЕП България си запазва правото по всяко време да променя Тарифата за предоставяните услуги. Промените в Тарифата влизат в сила в срок от 7 (седем) дни от нейното публикуване на електронната страница на СЕП България. Промените в цените имат сила занапред и са обвързващи за всички Клиенти на СЕП България, които към момента на влизане в сила на промените използват услугите на СЕП България и не са заявили в установения в съответния договор срок несъгласието си с тези промени.

1.1. Дължими суми по Договор

Дължимите от Клиента възнаграждения по сключените от тях Договори се формират въз основа на използваните съгласно Договора удостоверителни услуги, в съответствие с действащата към момента на настъпване на падежа на съответното задължение Тарифа.

В случай на забава от страна на Клиента за заплащане на дължимите суми, той дължи неустойка в размер на законоустановената лихва за забава.

Заплатените от Клиента суми не се възстановяват при прекратяване на правоотношенията му с ДУУ, независимо от основанието за това.

1.2. Плащане и фактуриране

ДУУ издава на клиента фактура за заплатените възнаграждения за удостоверителните услуги в законоустановените срокове. Неплащането в срок или плащането в непълен размер на дължимите суми от страна на клиента е основание за ДУУ да прекрати предоставяните на клиента услуги.

Всички дължими суми се заплащат в брой на каса на РО или по банков път. Плащанията по банков път се считат за извършени в момента на заверяване на банковата сметка на СЕП България с пълния размер на дължимите суми.

Всички банкови комисионни, такси и разноски във връзка с банковите преводи са за сметка на Клиента.

2. Финансова отговорност

2.1. Застраховка на дейността

СЕП България застрахова своята дейност като ДУУ съгласно ЗЕДЕП и подзаконовите актове по неговото прилагане.

Предмет на застраховка е отговорността на СЕП България в качеството му на доставчик на удостоверителни услуги за причинени на Автора/Титуляра и на всички трети лица имуществени и неимуществени вреди, за които СЕП България отговаря съгласно изискванията на чл. 29 от Закона за електронния документ и електронния подпис и останалото референтно законодателство.

СЕП България има сключен договор за застраховка с минимална застрахователна сума в размер на 600 000 лева за всяко увредено лице от всяко събитие.

При настъпване на застрахователно събитие, увреденото лице е длъжно в срок от 7 (седем) дни да уведоми писмено СЕП България и застрахователя на СЕП България.

2.2. Застрахователно покритие за потребителите

СЕП България обезщетява по застраховката всяко увредено лице от всяко събитие, в рамките на лимита, определен от ограничението на действието на издаденото удостоверение.

За избягване на всякакво съмнение, застраховката не покрива и ДУУ не отговаря и за случаите за вреди, следствие от:

- Неспазване на задълженията съгласно „Практика при предоставяне на удостоверителни услуги“;
- Компрометиране или загуба на частен ключ на Титуляра, съответно Автора, поради неполагане на дължимата грижа за опазването или ползването му;
- Неспазване на изискванията относно полагане на дължима грижа за проверка от Доверяващите се страни на валидността на електронния подпис и на издаденото от ДУУ удостоверение;
- Форсмажор, аварии и други събития, които са извън контрола на ДУУ.

3. Конфиденциалност на информацията

СЕП България спазва всички приложими правила за защитата на личните данни и на конфиденциалната информация, събирана с оглед на дейността му като доставчик на удостоверителни услуги, като спазва описаните в този „Наръчник за потребителя“ процедури.

3.1. Обхват на конфиденциалната информация

СЕП България приема за конфиденциалната информация, съдържаща се в или отнасяща се до:

- Титуляра/Автора, с изключение на публикуваната в удостоверението;
- Договора за удостоверителни услуги;
- Причината за спиране или прекратяване на Удостоверения за КЕП, извън публикуваната информация за статуса на Удостоверението;
- Кореспонденция, свързана с дейността на СЕП България, като доставчик на удостоверителни услуги;
- Частните ключове на СЕП България;
- Архивите за направени искания за издаване, спиране, възобновяване и прекратяване на Удостоверения;
- Архиви на транзакции;
- Записи на външни и вътрешни проверки и доклади;
- Планове за възстановяване след бедствия и непредвидени случаи.

3.2. Информация извън обхвата на конфиденциалната информация

СЕП България не разглежда като конфиденциалната информация съдържаща се в или отнасяща се до:

- Удостоверенията, публикувани в Регистъра на ДУУ;
- Данните, които се съдържат в Удостоверенията;
- Данните за статуса на удостоверенията, публикувани в „Списъка на прекратените удостоверения“;
- Всяка друга информация, която е публично достъпна и/или известна.

3.3. Задължение за пазене на конфиденциалната информация

СЕП България не разкрива и не може да се иска от него да разкрива или да предоставя на трети лица каквато и да било конфиденциална информация, освен когато е задължен по силата на специален закон да разкрие такава информация, пред компетентен орган на властта.

Регистриращите органи, Титулярът/Авторът или упълномощените от тях лица, ако Титулярът е юридическо лице, нямат право да разпространяват или да допускат разпространяване на информация, станала им известна при или по повод изпълнение на задълженията им по договорите със СЕП България, без предварително изрично писмено разрешение от страна на СЕП България.

4. Защита на личните данни

ДУУ събира данни и информация за Титуляра/Автора, само за целите на издаване и поддържане на удостоверения за електронен подпис.

ДУУ събира, обработва, съхранява и предоставя достъп до тези лични данни на трети лица при спазване изискванията на Закона за защита на личните данни.

ДУУ е регистриран като администратор на лични данни от Комисията за защита на личните данни по реда на Закона за защита на личните данни.

ДУУ предварително информира лицата за видовете информация, която събира за тях.

5. Права върху интелектуалната собственост

СЕП България притежава и си запазва всички права на интелектуална собственост върху бази данни, електронни страници, търговски марки и знаци, използвани от СЕП България (например eSign) удостоверения за електронен подпис, издадени от СЕП България, както и всякакви други документи, които разработва и поддържа.

СЕП България разрешава издадените удостоверения, без ограничен достъп от автора, да бъдат размножавани и разпространявани, при условие че те са възпроизвеждат при разпространението изцяло.

Всички права върху търговски имена, марки и запазени знаци се запазват от собствениците на тези права. СЕП България използва обекти на такива права само за целите на предоставяне на удостоверителни услуги.

Двойките ключове, както и секретните части на частните ключове на СЕП България са собственост на СЕП България.

6. Задължения и отговорности

6.1. Задължения и отговорности на СЕП България

СЕП България е акердитиран доставчик на удостоверителни услуги съгласно §41 от Закона за изменение и допълнение на Закона за електронния документ и електронния подпис, обнародван в ДВ бр.100 от 2010г. и

осъществява дейността си съгласно изискванията на референтното законодателство. В това свое качество СЕП България гарантира, че:

- Спазва всички разпоредби на ЗЕДЕП и подзаконовите актове по неговото прилагане;
- Изпълнява стриктно определените процедури и спазва политиките по издаване управление на удостоверения за квалифициран електронен подпис, както са обявени пред Комисията за регулиране на съобщенията;
- Информацията, включена в издаденото удостоверение е точна и пълна и съответства на състоянието към момента на извършване на проверката.

СЕП България отговаря пред Автора, съответно пред Титуляра на КЕП и пред всички трети лица за вредите:

- От неизпълнение на изискванията по чл. 21 от ЗЕДЕП и на задълженията му по чл. 22 и 25 от ЗЕДЕП;
- От неверни или липсващи данни в Удостоверението към момента на издаването му;
- Които са им причинени, в случай че по време на издаването на Удостоверението лицето, посочено като Автор, не е разполагало с частния ключ, съответстващ на публичния ключ;
- От алгоритмичното несъответствие между частния ключ и публичния ключ, вписан в Удостоверението.

6.2. Задължения и отговорности на регистриращите органи

РО действат от името и за сметка на СЕП България. Лицата започват дейност като РО на СЕП България след обучение и оторизация. По време на осъществяване на дейността като РО, СЕП България контролира и проверява регулярно РО. Отношенията между лицето, осъществяващо дейност като РО на СЕП България и СЕП България се уреждат с договор.

СЕП България гарантира, че:

- РО спазват всички разпоредби на ЗЕДЕП и подзаконовите актове по неговото прилагане;
- РО изпълняват стриктно определените процедури и спазва политиките по издаване управление на удостоверения за квалифициран електронен подпис, както са обявени пред Комисията за регулиране на съобщенията;
- РО извършват идентификация и автентикация на лицата, на които се издава Удостоверение за КЕП;
- РО сключват Договори с клиентите и приемат искания за удостоверителни услуги, в съответствие с разпоредбите на този Наръчник;
- Потвърдената от оператор на РО информация и включена в издаденото Удостоверение е точна и пълна и съответства на състоянието към момента на извършване на проверката.

6.3. Задължения и отговорности на Титуляра/Автора

Титулярът сключва Договор за удостоверителни услуги със СЕП България лично или чрез надлежно упълномощено лице.

Титулярът гарантира:

- За действията на Авторите, за които е поискал издаване на Удостоверение за КЕП;
- Че Авторът е овластен да извършва електронни изявления от негово име и държи частния ключ, съответстващ на посочения в Удостоверението публичен ключ;
- Че е подал точна, пълна и вярна информация на ДУУ в съответствие с изискванията на този Наръчник;

- Че ще използва ключовата двойка само за съответния КЕП и в съответствие с всяко друго ограничение, предвидено в законодателството и настоящия Наръчник;
- Че упражнява дължимата грижа за избягване на всякакво неоторизирано използване на частния ключ на Автора;
- Че ако Титулярът/Авторът генерират сами двойката ключове:
  - Използват алгоритми, одобрени като подходящи за целите на КЕП;
  - Използват дължина на ключовете, одобрена като подходяща за целите на КЕП;
- Частният ключ на Автора се използва единствено под контрола на Автора;
- Че ще уведоми ДУУ незабавно, ако настъпи някое от следните събития преди края на периода на валидност, посочен в Удостоверението:
  - Загуба на частния ключ на Автора, кражба, съмнение за компрометиране;
  - Загубен контрол върху частния ключ на Автора поради компрометиране на данните за активиране (т.е. ПИН) или по друга причина;
  - Невярно, непълно или променено съдържание на Удостоверението.
- В случай, че бъде информиран, че ДУУ, издал Удостоверението на Автора, е бил компрометиран, да осигури, че преустановяване използването на Удостоверението от Автора.

Авторът отговаря спрямо третите добросъвестни лица, когато при създаването на двойката ключове е използвал алгоритъм, който не отговаря на изискванията на НИАСПКЕП.

Авторът отговаря спрямо третите добросъвестни лица, ако:

- Не изпълнява точно изискванията за сигурност, определени от ДУУ;
- Не поиска от ДУУ прекратяване действието на Удостоверението, когато е узнал, че частният ключ е бил използван неправомерно или съществува опасност от неправомерното му използване.

Авторът отговаря спрямо третите добросъвестни лица за неверни изявления, направени пред ДУУ и имащи отношение към съдържанието или към издаването на Удостоверението.

Когато Удостоверението е издадено с вписан Титуляр, той отговаря за неизпълнението от страна на Автора на задълженията по предходните точки.

6.4. Отговорност на Титуляра и на Автора към ДУУ:

Авторът/Титулярът отговаря спрямо ДУУ, ако Авторът е предоставил неверни данни, съответно е премълчал данни, имащи отношение към съдържанието или към издаването на Удостоверението, и когато не е държал частния ключ, съответстващ на посочения в Удостоверението публичен ключ.

6.5. Задължения и отговорности на доверяващата се страна

Доверяващата се страна е отговорна за проверка на валидноста на Удостоверението за КЕП в съответствие с раздел VII, т.7.2 от Наръчника и за използването на Удостоверенията за КЕП в съответствие с разпоредбите на т.25, като съобразяват действията си с ограниченията, включени в Удостоверението за КЕП.

7. Ограничаване на отговорността

СЕП България носи отговорност само и единствено за вредите, посочени в т.6.1. на настоящия раздел. За избягване на всякакво съмнение, СЕП България не носи отговорност за:

- Пропуснати ползи или други косвени вреди, произтичащи от или във връзка с използването, или невъзможността за използване на Удостоверения за КЕП и електронните подписи;
- Всякакви други вреди, освен тези, които са свързани с доверяване на информацията, посочена в даденото Удостоверение за КЕП, базирана на потвърдената информация;
- Използването на Удостоверение за КЕП, което не е валидно или са надвишени определените ограничения, посочени в него или в тази Практика;
- Сигурността, използването, целостта на продуктите, включително хардуера и софтуера, които Титулярът/Авторът използват;
- Компрометиране на частния ключ на Автора;
- Нарушаване на права на трети лица по отношение на техни търговски марки, търговски наименования или други имуществени или неимуществени права, когато информация, съдържаща се в издадени удостоверения, е довела до такива нарушения.
- Вреди, настъпили в резултат на небрежност, неполагане на грижа или липса на познания във връзка с работата с удостоверения за електронни подписи;
- Вреди, настъпили поради несвоевременно прекратяване и/или спиране на Удостоверения и проверка на статуса на Удостоверения.

8. Лимит на отговорността

СЕП България ограничава действието на електронните подписи, за които издава Удостоверения за електронен подпис до определен лимитиран имуществен интерес. СЕП България ограничава своята отговорност до рамките на посочените по-долу лимити:

Тип Удостоверение за КЕП	Максимален лимит на отговорност
eSign Qualified Private	60 000 лева
eSign Qualified Organization	60 000 лева
eSign Qualified Profession	60 000 лева

Посочените лимити на отговорност се считат за ограничения на отговорността на ДУУ по смисъла на чл.29, ал.3 ЗЕДЕП.

Посочените лимити са максималните лимити, в рамките на които СЕП България отговаря за претърпени вреди при ползването на издадени от него удостоверения за квалифициран електронен подпис.

9. Обезщетения и компенсации

Във всички случаи на неизпълнение на задълженията от страна на Титуляра, произтичащи от „Наръчника за потребителя“ или от Договора за удостоверителни услуги, СЕП България ще претендира получаване на обезщетение за претърпени щети.

Глава Трета

„Политика при предоставяне на удостоверителни услуги“

I. Обхват и предназначение

Тази Глава съдържа общ преглед на политиката по предоставяне на удостоверителни услуги на СЕП България в качеството му на регистриран доставчик на удостоверителни услуги (ДУУ). Представена е общата концепция на СЕП България относно предоставяне на удостоверителни услуги. Документът дефинира страните участници в процеса по предоставяне на удостоверителни услуги, техните задължения, типовете Удостоверения за КЕП, процеса по проверка на самоличността, съответно идентичността и областта на приложение на издадените удостоверения за квалифициран електронен подпис.

Подробно описание на процесите и правилата, по които действа СЕП България, като доставчик на удостоверителни услуги, са представени в „Практика при предоставяне на удостоверителни услуги” на СЕП България.

II. Общ преглед

СЕП България в качеството си на регистриран Доставчик на удостоверителни услуги, осъществява следната дейност:

- Издава удостоверения за квалифициран електронен подпис, съгласно чл. 24 от ЗЕДЕП и води Регистър за тях;
- Предоставя на всяко лице достъп до публикуваните удостоверения за квалифициран електронен подпис;
- Предоставя услуги по създаване на частен и публичен ключ за усъвършенстван електронен подпис;
- Предоставя и/или одобрява устройства за сигурно създаване на електронен подпис;
- Предоставя услуги по удостоверяване на време съгласно чл. 40 от ЗЕДЕП, като удостоверява датата и часа на представяне на подписан с квалифициран електронен подпис, електронен документ.

СЕП България предоставя удостоверителни услуги посредством удостоверяващ орган и регистриращи органи.

Удостоверяващият орган и регистриращите органи извършват дейностите си по предоставяне на удостоверителните услуги от името и за сметка на СЕП България.

III. Модел на удостоверителни услуги

СЕП България дефинира следния технологичен модел за предоставяне на удостоверителни услуги:

1. Регистриране

Регистрирането представлява обработка и запис на данни в процеса на заявяване и приемане на Искане, в това число проверка чрез допустимите средства на самоличността, съответно идентичността на Автора и на Титуляра, и ако е необходимо - други данни за тези лица. Част от технологичната услуга „Регистриране“ е обработването на подадените Искания за управление, за спиране, възобновяване и прекратяване на издадени Удостоверения за КЕП.

2. Създаване на Удостоверения.

Технологичната услуга „Създаване на Удостоверения“ включва създаването, подписването и публикуването на Удостоверението в “Списък на издадените удостоверения“, въз основа на данните, проверени при технологичната услуга „Регистриране“ .

3. Прекратяване на Удостоверения

Технологичната услуга „Прекратяване на Удостоверения“ включва обработка и изпълнение на Исканията за спиране и/или прекратяване на Удостоверения за КЕП.

4. Проверка на статус на издадените Удостоверения.

Технологичната услуга „Проверка на статус на Удостоверения“ представлява предоставяне на информация за статуса на Удостоверение за КЕП на доверяващите се страни. Това се реализира чрез разпространение на „Списъка на прекратените удостоверения“ или услуги, предоставящи информация за статуса на Удостоверението на КЕП в реално време. Информацията за статуса на Удостоверенията за КЕП се обновява регулярно.

5. Предоставяне на устройства

Технологичната услуга „Предоставяне на устройства“ представлява предоставяне на клиентски криптомодул или други устройства за сигурно създаване на електронен подпис (SSCD). Устройствата се подготвят и предоставят на Авторите пряко или по сигурен начин чрез Титуляра. Услугата, когато е приложимо, включва подготовка, генериране и предоставяне на Авторите/Титулярите на устройства и необходимите данни за активиране и достъп до тях.

6. Удостоверяване на време

Услугата представлява издаване на удостоверение за времето на представяне на електронен подпис, създаден за определен електронен документ.

IV. Ниво на детайлност

Тази Политика представя общите положения на изискванията към организацията на работа във връзка с предоставянето на удостоверителни услуги, които се реализират от ДУУ.

СЕП България при нужда разработва, внедрява и документира вътрешни оперативни указания, инструкции или правила, свързани с посочените практики и политики, в които се детайлизира изпълнението на специфични задачи или конкретизират отговорности свързани с ежедневните дейности по предоставяне на удостоверителни услуги. Тези правила нямат публичен характер.

Политиката е дефинирана независимо от специфичните детайли, свързани с операционната среда на ДУУ.

V. Изисквания към дейността на ДУУ

СЕП България, в качеството си на регистриран ДУУ, реализира контроли, които удовлетворяват изискванията, дефинирани в тази политика.

При осъществяване на дейността по предоставяне на удостоверителни услуги, СЕП България спазва условията на настоящата политика и нормативната уредба на Р България в сферата на удостоверителните услуги.

СЕП България разполага с необходимите технологии, хардуер, софтуер, помещения и персонал, за да предоставя удостоверителни услуги съгласно ЗЕДЕП и тази Политика.

В съответствие с тази Политика, СЕП България в своята Практика при предоставяне на удостоверителни услуги декларира, че:

- Спазва ЗЕДЕП и подзаконовата нормативна уредба, както и всички практики и процедури, разработени въз основа на изискванията посочени в тази политика;
- Посочва задължения на трети лица, имащи отношение към предоставяне на удостоверителните услуги, включително приложимите политики и практики;
- Публикува и осигурява достъп както до своята „Практика при предоставяне на удостоверителни услуги“ на всички потребители на удостоверителни услуги, така и до други документи, необходими за определяне на съответствието с удостоверителната политика;
- Определя висш ръководен орган, който управлява и одобрява практики при предоставяне на удостоверителни услуги, съгласно тази политика и ги представя пред Комисията за регулиране на съобщенията за одобрение;
- Ангажира висшето ръководство и неговата отговорност по отношение на установяване и спазване на практиките при предоставяне на удостоверителни услуги;
- Дефинира процес по преглед на практиките при предоставяне на удостоверителни услуги, включително отговорности по поддръжката им;
- Информира незабавно за настъпили промени в своята „Практика при предоставяне на удостоверителни услуги”, Документира използваните алгоритми и техните параметри.

VI. Инфраструктура за доставка на удостоверителни услуги – Управление на ключовете

1. Генериране на ключовете на ДУУ

СЕП България използва надежден процес за генериране, за да генерира частните си ключове. Генерирането се осъществява в защитена среда. СЕП България поделя частните си ключове на секретни части. СЕП България е собственик на частните ключове, за които използва процедурата за разпределяне на секретни части. СЕП България има правото да прехвърля такива секретни части на лица, които са изрично упълномощени.

1.1. Защитена среда

Физическият достъп до защитената част на системите на СЕП България е ограничен и до нея имат достъп само надлежно упълномощени служители, в зависимост от техните функционални задължения.

1.2. Упълномощен персонал

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

1.3. Поделяне на секретни части

СЕП България използва поделяне на секретни части за частните си ключове и ги разпределя между упълномощени лица, които се грижат за съхраняването на секретните части.

1.4. Надеждни системи

СЕП България използва надеждни системи при предоставяне на своите удостоверителни услуги и генериране на ключовите си двойки. 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. Генериране на ключовете на СЕП България

СЕП България генерира по сигурен начин и защитава собствените си частни ключове, като използва надеждна система и взема необходимите мерки, за да предотврати компрометирането или не оторизираното им използване.

2.1. Стартова процедура

СЕП България внедрява и документира стартовата процедура по генериране на ключовете, в съответствие с тази Политика. СЕП България внедрява европейските и общопризнати в международната практика стандарти за надеждни системи и прави всичко възможно, за да ги съблюдава.

2.2. Криптографски хардуер

Генерирането на ключовете на СЕП България се осъществява от хардуерно криптографско устройство за създаването, съхраняването и използването на частния ключ с ниво на сигурност EAL 3 или по-високо съгласно стандарта ISO 15408 или друга спецификация, определяща еквивалентни нива на сигурността.

2.3. Използвани алгоритми

Ключовете на СЕП България се генерират, като се използват алгоритми, признати за подходящи за целите на издаване на удостоверения за квалифициран електронен подпис и отговарят на изискванията на „Наредба за изискванията към алгоритмите за създаване и проверка на квалифициран електронен подпис".

2.4. Дължина на ключа

Избраната дължина и алгоритми за ключовете, подписващи издаваните Удостоверения за КЕП, са признати за подходящи за целите на издаването на удостоверения за квалифициран електронен подпис.

2.5. Гарантиране непрекъснатост на операциите

Преди края на периода на валидност на ключовете, подписващи издаваните Удостоверения за КЕП, СЕП България генерира нова ключова двойка за подписване на Удостоверения и прилага всички необходими мерки, за да избегне прекъсване на операциите на всяка страна, която може да разчита на ключовете на УО. Новите ключове се генерират и разпространяват в съответствие с тази Политика.

3. Съхраняване, архивиране и възстановяване ключове на ДУУ

СЕП България осигурява конфиденциалност и интегритет на своите частни ключове.

3.1. Държане и ползване на частния ключ

Частните ключове на ДУУ, използвани за подписване на Удостоверения за КЕП, се държат и използват, без да напускат сигурно криптографско устройство, което е с ниво на сигурност EAL 3 или по-високо съгласно стандарта ISO 15408 или друга спецификация, определяща еквивалентни нива на сигурността.

3.2. Защита на частния ключ

Когато частните ключове са извън сигурното криптографско устройство, те са защитени по такъв начин, че се осигурява същото ниво на защита, каквато се осигурява и от сигурното криптографско устройство.

3.3. Архивиране на частния ключ

Частните ключове на ДУУ, използвани за подписване на Удостоверения за КЕП, се архивират, съхраняват и възстановяват съвместно най-малко от двама служители на доверени позиции във физически защитена среда.

3.4. Копия на частния ключ

При контрола по създаване на архивни копия на частните ключове на ДУУ, използвани за подписване на Удостоверения за КЕП, се прилагат равни или по-високи мерки за сигурност от използваните при експлоатация.

3.5. Съхраняване на частните ключове на ДУУ

При съхраняване на ключовете в специализиран хардуерен модул, се реализира механизъм за контрол на достъпа гарантиращ, че ключовете са недостъпни извън хардуерния модул.

3.6. Разпространяване на публичните ключове на ДУУ

СЕП България предприема мерки, за да гарантира, че се поддържа интегритета и автентичността на публичните ключове на ДУУ, използвани за проверка на електронен подпис и всички асоциирани с тях параметри.

3.7. Източник и интегритет на публичния ключ

Публичните ключове на ДУУ, използвани за проверка на ЕП са достъпни за всички участници в удостоверителния процес по такъв начин, че се осигурява интегритета на публичните ключове и може да се провери техния произход.

3.8. Защита частния ключ на доставчика

Единствено ДУУ има достъп до частния ключ. Частния ключ не се предоставя под никаква форма и по никакъв начин на други лица за ползване или съхранение.

4. Използване на ключовете на ДУУ

СЕП България, като ДУУ, осигурява подходящо използване на своите частни ключове.

Частните ключове на ДУУ, използвани при генериране на Удостоверения за КЕП, може да се използват за подписване и на други типове удостоверения, както и на информацията за статуса на издадените Удостоверения КЕП дотолкова, доколкото не са нарушени изискванията дефинирани в този документ.

5. Физическа защита

Частните ключове на ДУУ, използвани за подписване на Удостоверения за КЕП могат да се използват само във физически защитена среда.

6. Прекратяване на жизнения цикъл на ключове на ДУУ

СЕП България предприема мерки, с които осигурява, че частните ключове на ДУУ, използвани за подписване на Удостоверения за КЕП не могат да се използват след края на техния жизнен цикъл.

Всички копия на частните ключове на ДУУ, използвани за подписване на Удостоверения за КЕП, както и данните за тяхното генериране, се унищожават или се привеждат в неработоспособно състояние.

7. Жизнен цикъл на криптографския хардуер ползван за подписване на Удостоверения за КЕП

СЕП България предприема мерки, с които осигурява, защитата и сигурността на криптографския хардуер по време на неговия жизнен цикъл.

7.1. Доставка на криптографски хардуер

Криптографският хардуер използван за подписване на Удостоверения за КЕП и информацията за издадените Удостоверения за КЕП не е бил компрометиран по време на доставката.

7.2. Съхранение на криптографски хардуер

Криптографският хардуер използван за подписване на Удостоверения за КЕП и информацията за статуса на издадените Удостоверения за КЕП, не е бил компрометиран по време на съхранението.

7.3. Съвместен контрол

Инсталирането, активирането, архивирането и възстановяването на частните ключове на ДУУ, използвани за подписване на Удостоверения за КЕП в криптографския хардуер се осъществява съвместно най-малко от двама служители на доверени позиции.

7.4. Функциониране на криптографския хардуер

Криптографският хардуер използван за подписване на Удостоверения за КЕП и информацията за статуса на издадените Удостоверения за КЕП функционира коректно.

7.5. Унищожаване на частните ключове в криптографския хардуер

Частните ключове на ДУУ, използвани за подписване на Удостоверения за КЕП, съхранявани в криптографския хардуер се унищожават, когато хардуера вече не се използва от ДУУ за тази цел.

VII. Осигуряване на услуги по управление на ключовете на Титуляра/Автора

В случай, че СЕП България предоставя услуги на Титуляра/Автора по управление на ключовете, то СЕП България предприема мерки, с които да осигури генерирането на ключове за Автора по сигурен начин и при секретност на частния ключ на Автора.

1. Използвани алгоритми

В случаите, в които ДУУ генерира ключове за Автора, използва алгоритми, признати за подходящи за използване, за целите на КЕП, за времето на валидност на издаденото към него Удостоверение.

2. Дължина на ключовете

В случаите, в които ДУУ генерира ключове за Автора, използва дължина на ключове, призната за подходяща за използване за целите на КЕП, за времето на валидност на издаденото към него Удостоверение.

3. Съхраняване на генерираните ключове

В случаите, в които ДУУ генерира ключове за Автора, ДУУ осигурява необходимите средства за сигурно създаване и съхранение на ключове за Автора (като SSCD), до предаването им на Автора по сигурен начин.

4. Предоставяне на ключовете

В случаите, в които ДУУ генерира ключове за Автора, частните ключове се предоставят на Автора, така че да не се компрометира сигурността и интегритета им. След като се доставят, частните ключове се намират под изключителния контрол на Автора.

4.1. Подготовка на SSCD

ДУУ осигурява сигурно и надеждно издаване и съхранение на Удостоверения за КЕП чрез SSCD.

4.2. Контрол при подготовката на SSCD

Подготовката на SSCD се осъществява по сигурен и контролиран от ДУУ начин. Използваните SSCD са с ниво на сигурност EAL 3 и по-високо съгласно стандарта ISO 15408.

4.3. Съхраняване и предоставяне на SSCD

Съхраняването и разпространяването на SSCD се осъществява по сигурен и контролиран от ДУУ начин. SSCD се предоставя на Автора, ако е необходимо чрез Титуляра, така че да не се компрометират.

4.4. Деактивация и реактивация на SSCD

Деактивирането и активирането на SSCD се осъществява по сигурен и контролиран от ДУУ начин.

5. Данни за активиране

Когато към SSCD има асоциирани потребителски данни за активиране (ПИН код), данните за активиране се подготвят по сигурен начин и се разпространяват отделно от SSCD. Разделянето може да е по време, по място или и двете.

В случай, че данните за активиране не са разделени от SSCD, то се вземат допълнителни мерки, които да възпрепятстват компрометирането им със съответна степен на сигурност.

VIII. Инфраструктура за доставка на удостоверителни услуги – Управление на жизнения цикъл на Удостоверение за КЕП

1. Регистриране на Титуляра/Автора

СЕП България предприема мерки за осигуряване на правилна идентификация и автентикация на заявителите на Удостоверения за КЕП, проверка на тяхното овластяване, и приемането на пълни и точни Искания за издаване на Удостоверения за КЕП.

1.1. Предоставяне на информация за удостоверителните услуги

Преди подписване на договор за удостоверителни услуги с Титуляра, ДУУ информира Клиента, респективно неговия пълномощник, за реда и условията относно използването на Удостоверения. Подробна информация е представена на електронната страница на СЕП България.

1.2. Проверка при регистриране

ДУУ по време на регистрането по смисъла на раздел III, т. 1 проверява чрез допустими средства, в съответствие с националното законодателство, самоличността съответно идентичността и, ако е приложимо, други данни за лицето, на което се издава удостоверението за квалифициран електронен подпис. Проверката на доказателствата за идентичността на физическото лице, може да се извърши както пряко, така и непряко, като се използват средства, осигуряващи сигурност, еквивалентна на физическо присъствие.

2. Идентификация на физически лица

Физическите лица, трябва да представят доказателства за:

- Пълното име на физическото лице – Автор и Титуляр;
- Национален идентификационен номер или други данни, които могат да се използват, за да се различи лицето от други със същите имена.

3. Идентификация на юридически лица

Когато за целите на издаване на Удостоверение за КЕП, се идентифицира физическо лице, свързано с юридическо лице или организация, трябва да се представят доказателства за:

- Пълното име на физическото лице – Автор;
- Национален идентификационен номер или други данни, които могат да се използват, за да се различи лицето от други със същите имена;
- Пълното име и юридическия статус на свързваното юридическо лице или организация – Титуляр;
- Всякаква приложима регистрационна информация или информация от регистър;
- Доказателство, че физическото лице – Автор представлява юридическото/физическото лице или организация – Титуляр.

4. Съхранявана информация

ДУУ записва цялата информация, използвана за проверка на идентичността и, ако е приложимо, други специфични атрибути, включително имена и референтни номера на документите, използвани при проверката и ограниченията на тяхната валидност.

4.1. Данни за представителство

Ако Искането за издаване на Удостоверение за КЕП се подава от лице, различно от Автора/Титуляра, следва да се представят доказателства, че подалият Искането е упълномощен да действа от името на идентифицирания в Удостоверението за КЕП Автор/Титуляр.

4.2. Данни за обратна връзка

Авторът/Титулярът предоставя контактни данниза установяване на връзка с него.

5. Договорни отношения

ДУУ съхранява в своя архив подписан Договор с Клиента, който урежда правата, задълженията и отговорностите на страните по него.

6. Време за съхранение

Записите, идентифицирани по-горе, се пазят за период от време, за който е информиран субекта и, при необходимост, за целите на предоставяне на доказателства при съдебен процес в съответствие с приложимото законодателство.

7. Притежание на частния ключ

Ако ДУУ не е генерирал частния ключ на Автора, процесът по заявяване издаване на Удостоверение гарантира, че Авторът държи частния ключ, съответстващ на публичния ключ, предоставен за удостоверяване.

8. Притежание на SSCD

Ако ДУУ не е генерирал ключовата двойка и удостоверителната политика изисква използването на SSCD, процесът по заявяване издаване на Удостоверение гарантира, че публичният ключ, предоставен за удостоверяване, е генериран чрез SSCD.

9. Подновяване, смяна на ключове и актуализиране

ДУУ се уверява, че Исканията за подновяване, модификация и управление на Удостоверение за КЕП са пълни и точни и изхождат от Титуляра или надлежно упълномощено от него лице. Това включва смяна на ключове след прекратяване или преди изтичане периода на валидност на Удостоверението за КЕП или актуализиране на регистрираните записи поради промяна в данните на Автора/Титуляра.

9.1. Актуално Удостоверение за КЕП

В случай на подновяване на Удостоверение за КЕП, ДУУ проверява наличието и валидността на Удостоверението за КЕП, както и валидността на информацията, използвана при проверка на идентичността на Автора/Титуляра.

9.2. Променени условията на СЕП България

При промяна на условията за предоставяне на удостоверителни услуги, ДУУ информира Автора/Титуляра за настъпилите промени по реда, предвиден в този Наръчник. Ако някои от условията и реда на ДУУ са променени, то те се съобщават на Титуляра и той трябва да ги приеме в съответствие с този Наръчник.

9.3. Променено съдържание на Удостоверение за КЕП

При настъпила промяна на данните, вписани в Удостоверение за КЕП, Авторът/Титулярът представя информацията, необходима за промяна на регистрираните данни по реда, предвиден в този Наръчник. Ако някое от имената в Удостоверението или данни са променени или предишното Удостоверение е било

прекратено, то информацията за регистриране се проверява, записва и Титулярът ги приема в съответствие с този Наръчник.

10. Създаване на удостоверение

СЕП България предприема мерки, за да осигури сигурно и надеждно генериране на удостоверенията за квалифициран електронен подпис.

IX. Идентификация

СЕП България включва идентификатори на удостоверителните политики, за да осигури на доверяващите се страни лесен достъп до информация за реда и условията, съответстващи на удостоверителната политика в съответствие, с която са издадени Удостоверенията за КЕП.

Съответствието с идентифицираната удостоверителна политика се описва чрез включване на съответните идентификатори в издаваните Удостоверения за КЕП.

1. Идентификатор на политиката

Идентификаторът на удостоверителна политика е:

itu-t(0)identified-organization(4)etsi(0)qualified-certificate-policies(1456)policy-identifiers(1)qcp-public-with-sscd(1)

Идентификаторите на политиката, според която се издават различните типове Удостоверения за КЕП, се включват в съдържанието на всяко издадено Удостоверение в съответствие с тази политика за всеки конкретен тип Удостоверение за КЕП.

2. Потребителска общност и приложение на Удостоверения за КЕП

Удостоверения за КЕП, издадени в съответствие с тази Политика имат смисъла на удостоверения за квалифициран електронен подпис съгласно ЗЕДЕП.

Електронният подпис, за който е издадено Удостоверение за КЕП, отговарящо на изискванията на тази Политика, има значението на саморъчен подпис по отношение на всички, включително държавни органи или органи на местното самоуправление.

3. Спазване на политиката

1.1. Общи сведения

ДУУ използва идентификатора, дефиниран в по-горе, за доказване на съответствие с тази удостоверителна политика.

1.2. Съответствие с Политиката

Спазването на тази Политика от ДУУ означава, че:

- ДУУ спазва всички задължения, които са дефинирани в този Наръчник;
- ДУУ е реализирал контроли, които удовлетворяват всички изисквания, дефинирани в раздел V „Изисквания към дейността на ДУУ".

X. Профил на Удостоверения за КЕП

Удостоверенията, издавани в съответствие с тази удостоверителна Политика съдържат:

- Указание, че удостоверението е издадено като удостоверение за квалифициран електронен подпис;
- Идентификация на ДУУ и държавата, в която оперира;
- Имената на подписващия или, ако е приложимо, псевдоним, който да се идентифицира като такъв;
- Осигуряване на специфични атрибути на подписващия, които да се включат в Удостоверението, ако е приложимо, в зависимост от това за какви цели е предназначено удостоверението;
- Данните за проверка на подписа, които съответстват на данните за създаване на подписа, намиращи се под контрола на подписващия;
- Индикация за началото и края на периода на валидност на удостоверението;
- Идентификационен код на удостоверението;
- Усъвършенствания електронен подпис на ДУУ, издал удостоверението;
- Ако е приложимо ограничение на обхвата на приложение на удостоверението;
- Ако е приложимо ограничение на размера на транзакциите, за които удостоверението може да се използва.

XI. Мерки срещу фалшифициране на Удостоверения за КЕП

ДУУ предприема мерки срещу фалшифициране на Удостоверенията и в случаите, когато ДУУ генерира данните за създаване на подписа, гарантира конфиденциалността по време на процеса на генериране на тези данни.

XII. Сигурно генериране

Ако ДУУ генерира ключовете на Автора то:

- Процедурата по издаване на Удостоверение се изпълнява едновременно с процедурата по генериране на ключова двойка от ДУУ;
- Частния ключ (или SSCD) по сигурен начин се предава на Автора.

XIII. Конфиденциалност и интегритет на данните за регистрация

Конфиденциалността и интегритета на данните за регистрация са гарантирани и в случаите, когато се обменят с Титуляра, Автора или между различни компоненти от инфраструктурата на ДУУ.

XIV. Проверка на източника на регистрационните данни

Когато се използват външни доставчици на регистрационни услуги, ДУУ проверява дали данните за регистрация се обменят с познат доставчик на регистрационни услуги, чиято идентичност е автентикирана.

XV. Разпространяване на реда и условията

ДУУ предоставя условията и реда на своята дейност на всички участници в удостоверителния процес.

XVI. Публикувана информация

ДУУ предоставя за ползване от потребителите реда и условията на своята дейност и реда за ползване на Удостоверенията, в това число:

- Приложението на удостоверителна политика за издаване на удостоверения за квалифициран електронен подпис с използване на SSCD;
- Ограничения в използването;
- Задълженията на Клиента, включително по отношение на изискванията на Политиката за използване на SSCD;
- Информация за начините на проверка на статуса на Удостоверението за КЕП, включително проверка в "Списъка на прекратените удостоверения", така че доверяващите се страни да имат предвид „разумно доверяване" на Удостоверенията;
- Ограниченията в отговорността, включително целите/употребата, за които ДУУ приема (или изключва) юридическа отговорност;
- Периода от време, през който информацията за регистрацията се съхранява;
- Периода от време, през който ДУУ пази журналите със записите от събитията;
- Процедурите за подаване на жалби, оплаквания и решаване на спорове;
- Приложимото законодателство;
- Информация за регистрация на ДУУ от Комисията за регулиране на съобщенията или други сертификации за съответствие с тази Политика, като се посочи и според коя схема.

XVII. Достъпност и разпространение на информацията

Информацията, посочена по-горе, е достъпна без ограничения и може да бъде предавана електронно.

1. Достъп при генериране

След генерирането Удостоверението за КЕП е достъпно за преглед и използване от Автора/Титуляра.

2. Ограничаване на достъпа

Удостоверението за КЕП е публично достъпно за преглед само в случаите, когато е получено изричното указание на Автора/Титуляра.

3. Информация за доверяваща се страна

ДУУ предоставя на доверяващата се страна реда и условията за използване на Удостоверенията.

4. Предоставяне на информация за КЕП

Информацията, определена по-горе, е достъпна 24 часа на ден 7 дни в седмицата. След авария на системата, услуги или поради други фактори, които не са под контрола на ДУУ, ДУУ ще положи максимални усилия, за да осигури преустановяване на тези информационни услуги за период, не по-дълъг от максималният период от време, посочен в „Практиката при предоставяне на удостоверителни услуги".

5. Публичност и достъпност на информацията за Удостоверенията за КЕП

Информацията, посочена в Раздел XVII е публична и достъпна за всички.

XVIII. Прекратяване, спиране и възобновяване на Удостоверение за КЕП

ДУУ прекратява Удостоверенията за КЕП своевременно след получаване на оторизирани и валидирани Искания за прекратяване на Удостоверения.

1. Документиране на процедурата

ДУУ документира като част от своята Практика, процедурите по прекратяване/спиране на Удостоверения за КЕП, включително:

- Кой може да подава сведения и Искане за прекратяване/спиране;
- Как се подават сведения и Искания за прекратяване/спиране;
- Изисквания за допълнително потвърждаване на сведенията и Исканията за прекратяване;
- Дали и поради каква причина Удостоверението може да бъде спряно;
- Механизмите използване за разпространяване на информация за прекратените Удостоверения;

2. Приемане на Искания за прекратяване/спиране

Исканията за прекратяване се обработват незабавно в момента на тяхното постъпване.

3. Проверка на заявките

Исканията за прекратяване се автентикират и се проверява дали са постъпили от оторизиран източник.

4. Спиране на Удостоверение за КЕП преди прекратяване

При получаване на Искане за спиране, Удостоверението за КЕП се спира от ДУУ до получаване на Искане за неговото прекратяване или до изтичане на максималния срок за спиране на Удостоверение за КЕП..

5. Информиране за промяна на статуса

Авторът/Титулярът се информират за всяка настъпила промяна в статуса на Удостоверението за КЕП.

6. Необратимост на прекратяването

След прекратяване на Удостоверение за КЕП, неговият статус преминава в „невалиден“ и не може да бъде променян отново..

XIX. Списък на прекратените удостоверения

Актуализирането на списъците на издадените и прекратените удостоверения за квалифициран електронен подпис се извършва най-малко през 3 (три) часа и:

- Всеки CRL посочва максималното време за публикуване на следващия CRL;
- Нов CRL може да се публикува преди посоченото време за следващото публикуване на CRL;
- CRL се подписва от ДУУ.

1. Достъпност на списъка на прекратените удостоверения

Услугите по управление на статуса на прекратените Удостоверения са достъпни 24 часа на ден, 7 дни в седмицата. След авария на системата или поради други фактори, които не са под контрола на ДУУ, ДУУ ще положи максимални усилия, за да осигури преустановяване на тези информационни услуги за период не по-дълъг от максималния период от време, посочен в Практиката.

2. Статус на Удостоверенията

Информацията за статуса на Удостоверения е достъпна 24 часа на ден, 7 дни в седмицата. След авария на системата или поради други фактори, които не са под контрола на ДУУ, ДУУ ще положи максимални усилия, за да осигури преустановяване на тези информационни услуги за период не по-дълъг от максималния период от време, посочен в Практиката.

XX. Интегритет и автентичност на информацията за статуса на Удостоверение за КЕП

ДУУ е предприел мерки по защита на интегритета и автентичността на информацията за статуса на Удостоверенията.

1. Публикуване на информация за статуса на Удостоверение за КЕП

Информацията за статуса на Удостоверенията е публична и достъпна за всички.

2. Период на съхранение на прекратените Удостоверения за КЕП в CRL

Информацията за статуса на Удостоверенията се съхранява най-малко до изтичане на срока на валидност на издаденото Удостоверение.

XXI. Базово удостоверение на УО

Базовото удостоверение на СЕП България е първо в йерархията от удостоверения на ДУУ. Удостоверението се издава от SEP Root CA удостоверяващ орган и е самоподписано. При генерирането на това удостоверение се следва специална процедура по сигурно и надеждно генериране на ключовата двойка. Частният ключ се използва за подписване на удостоверението на оперативния УО и удостоверението за времето на представяне на електронен подпис, създаден за определен електронен документ.

Периодът на валидност на базовото удостоверение е 20 (двадесет) години. Дължината на ключа е 4096 бита за RSA алгоритъм.

Базовото удостоверение на СЕП България има смисъл на удостоверение за квалифициран подпис, съгласно разпоредбите нана ЗЕДЕП.

Профил на удостоверението на SEP Root CA:

име на поле	стойност или ограничение на стойността	
version	Version 3	
serialNumber	уникален сериен номер на удостоверението в рамките на издаващия удостоверяващ орган	
signature	sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5)	
issuer	C	BG

име на поле	стойност или ограничение на стойността	
(Distinguished Name)	L	Sofia
	O	System for Electronic Payments/SEP Bulgaria JSC
	OU	SEP
	CN	SEP Root CA
validity	notBefore	UTC формат
	notAfter	UTC формат
subject (Distinguished Name)	C	BG
	L	Sofia
	O	System for Electronic Payments /SEP Bulgaria JSC
	OU	SEP
	CN	SEP Root CA
Key Usage	Certificate Signing, Off-line CRL Signing, CRL Signing (06)	

име на поле	стойност или ограничение на стойността
Certificate Policies	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.30299 [1,1]Policy Qualifier Info: Policy Qualifier Id=User Notice Notice Text=SEP Bulgaria JSC – accredited certification service provider [1,2]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.crc.bg/ [2]Certificate Policy: Policy Identifier=1.3.6.1.4.1.30299.2 [2,1]Policy Qualifier Info: Policy Qualifier Id=User Notice Notice Text=SEP Root CA [2,2]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://eSign.bg
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.sep.bg/SEP_root_ca.crl

име на поле	стойност или ограничение на стойността
Authority Information Access	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.sep.bg
Basic Constraints	Subject Type=CA Path Length Constraint=None
Issuer Alternative Names	
Subject Alternative Name	
Authority Key Identifier	
Subject Key Identifier	
subjectPublicKeyInfo	Публичният ключ на Автора и алгоритъма, с който се използва
signatureAlgorithm	sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5)
signatureValue	Електронен подпис на ДУУ

XXII. Удостоверение на оперативния УО

Оперативният УО на СЕП България подписва издаваните удостоверения за квалифициран електронен подпис и включва в тях идентификатор на политиката, според която се издават и идентификатор на типа издавано Удостоверение. Удостоверението на оперативния УО се издава от базовия удостоверяващ орган.

Периодът на валидност на оперативното удостоверение е 10 (десет) години..Дължината на ключа е 2048 бита за RSA алгоритъм.

Оперативното удостоверение на СЕП България има смисъл на удостоверение за квалифициран подпис, съгласно разпоредбите на ЗЕДЕП.

Оперативният УО eSign QES CA, издава удостоверения за квалифициран електронен подпис в съответствие с политика с OID: 1.3.6.1.4.1.30299.2.1.

Профил на удостоверението на eSign QES CA:

име на поле	стойност или ограничение на стойността
version	Version 3

име на поле	стойност или ограничение на стойността	
serialNumber	Уникален сериен номер на удостоверението в рамките на издаващия удостоверяващ орган	
signature	sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5)	
issuer (Distinguished Name)	C	BG
	L	Sofia
	O	System for Electronic Payments/SEP Bulgaria JSC
	OU	SEP
	CN	SEP Root CA
validity	notBefore	UTC формат
	notAfter	UTC формат
subject (Distinguished Name)	C	BG
	L	Sofia
	O	System for Electronic Payments /SEP Bulgaria JSC
	OU	eSign QES
	CN	eSign QES CA
	Street	1 Zlatovrah Str.
Key Usage	Certificate Signing, Off-line CRL Signing, CRL Signing (06)	
Enhanced Key Usage		

име на поле	стойност или ограничение на стойността
Certificate Policies	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.30299.2.5 [1,1]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text=eSign QES CA [1,2]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.esign.bg [2]Certificate Policy: Policy Identifier=1.3.6.1.4.1.30299 [2,1]Policy Qualifier Info: Policy Qualifier Id=User Notice [2,2]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.crc.bg/
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.sep.bg/SEP_root_ca.crl

име на поле	стойност или ограничение на стойността
Authority Information Access	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.sep.bg
Basic Constraints	Subject Type=CA Path Length Constraint=None
Issuer Alternative Names	
Subject Alternative Name	
Authority Key Identifier	
Subject Key Identifier	
subjectPublicKeyInfo	Публичният ключ на Автора и алгоритъма, с който се използва
signatureAlgorithm	sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5)
signatureValue	Електронен подпис на ДУУ

XXIII. Потребителски удостоверения

Потребителските Удостоверения за КЕП се издават от оперативния УО.

Периодът на валидност на издадените Удостоверения е 3 (три) години. Дължината на ключа е 2048 бита за RSA алгоритъм или 163 бита за ECDSA алгоритъм.

1. Профил на eSign Qualified Private

Удостоверение от типа SEP Qualified Private се използва за потвърждаване съгласието/самоличността на физическо лице при участие в електронен обмен, като Web-базирани приложения, подписване на електронни документи и/или договори, банкови транзакции и извършване на изявления по смисъла на ЗЕДЕП.

Изявленията са от името и за сметка на лицето.

Профил на eSign Qualified Private Удостоверение:

име на поле	стойност или ограничение на стойността
version	Version 3

име на поле	стойност или ограничение на стойността	
serialNumber	Уникален сериен номер на удостоверението в рамките на издаващ удостоверяващия орган	
signature	sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5) id-ecdsa-with-sha1 (OID: 1.2.840.10045.4.1)	
issuer (Distinguished Name)	C	BG
	Street	1 Zlatovrah Str.
	L	Sofia
	O	System for Electronic Payments/SEP Bulgaria JSC
	OU	eSign QES
	CN	eSign QES CA
validity	notBefore	UTC формат
	notAfter	UTC формат
subject (Distinguished Name)	*C	BG
	S	Област на Автора
	*L	Населено място на Автора
	*OU	SEP Qualified Private
	*CN	Име/псевдоним на Автора
	UID (0.9.2342.19200300.100.1.1)	EGNxxxxxxxxxx[ЕГН/ЛНЧ/ггммдд на Титуляра]
	*E	e-mail адрес на Автора
	Street	Адрес на Автора
	Phone	Телефон на Автора
Key Usage	Digital Signature, Non-Repudiation, Key Encipherment, Data Encipherment (f0)	

име на поле	стойност или ограничение на стойността
Enhanced Key Usage	Client Authentication (1.3.6.1.5.5.7.3.2) Secure Email (1.3.6.1.5.5.7.3.4)
Certificate Policies	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.30299.2.5.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text=This certificate is issued as qualified certificate for qualified electronic signature using secure signature creation device [1,2]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.esign.bg
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.sep.bg/eSign_QES_ CA.crl
Authority Information Access	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.sep.bg
Basic Constraints	Subject Type=End Entity Path Length Constraint=None
Authority Key Identifier	
Subject Key Identifier	

име на поле	стойност или ограничение на стойността
Qualified Certificate Statements	Посочва, че удостоверението е издадено като удостоверение за квалифициран електронен подпис
subjectPublicKeyInfo	Публичният ключ на Титуляра/Автора и алгоритъмът, с който се използва
signatureAlgorithm	sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5) id-ecdsa-with-sha1 (OID: 1.2.840.10045.4.1)
signatureValue	Електронен подпис на ДУУ

2. Профил на eSignQualified Organization

Удостоверение от типа SEP Qualified Organisation се използва за потвърждаване на съгласието, съответно на идентичността, на юридическо лице при участие в електронен обмен, като Web-базирани приложения, подписване на електронни документи и/или договори, банкови транзакции и извършване на изявления по смисъла на ЗЕДЕП.

Титулярът и Авторът се различават, като Авторът е физическо лице, а Титулярът - юридическо.

Авторът върши изявленията от името и за сметка на Титуляра.

Профил на eSignQualified Organization Удостоверение:

име на поле	стойност или ограничение на стойността	
version	Version 3	
serialNumber	уникален сериен номер на удостоверението в рамките на издаващ удостоверяващия орган	
signature	sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5) id-ecdsa-with-sha1 (OID: 1.2.840.10045.4.1)	
issuer (Distinguished Name)	C	BG
	Street	1 Zlatovrah Str.
	L	Sofia
	O	System for Electronic Payments /SEP Bulgaria JSC
	OU	eSign QES

име на поле	стойност или ограничение на стойността	
	CN	eSign QES CA
validity	notBefore	UTC формат
	notAfter	UTC формат
subject (Distinguished Name)	*C	BG
	S	Област на населеното място, където Автора работи за Титуляра
	*L	Населено място, където Автора работи за Титуляра
	O	Пълно име на юридическото лице – Титуляр
	*OU	SEP Qualified Organization
	OU	Организационна единица на Титуляра
	*CN	Име/псевдоним на Автора
	T	Позиция на Автора/овластяване
	OU	EIKxxxxxxxxxx[ЕИК на титуляра] / друг идентификатор
	*E	Служебен e-mail адрес на Автора за водене на кореспонденция от името на Титуляра
	Street	Служебен адрес на Автора
	Phone	Телефон на Автора
Key Usage	Digital Signature, Non-Repudiation, Key Encipherment, Data Encipherment (f0)	
Enhanced Key Usage	Client Authentication (1.3.6.1.5.5.7.3.2) Secure Email (1.3.6.1.5.5.7.3.4)	

име на поле	стойност или ограничение на стойността
Certificate Policies	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.30299.2.5.2 [1,1]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text=This certificate is issued as qualified certificate for qualified electronic signature using secure signature creation device [1,2]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.esign.bg
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.sep.bg/eSign_QES_ CA.crl
Authority Information Access	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.sep.bg
Basic Constraints	Subject Type=End Entity Path Length Constraint=None
Authority Key Identifier	
Subject Key Identifier	
Qualified Certificate Statements	Посочва, че удостоверението е издадено като удостоверение за квалифициран електронен подпис

име на поле	стойност или ограничение на стойността
subjectPublicKeyInfo	Публичният ключ на Титуляра/Автора и алгоритъмът, с който се използва
signatureAlgorithm	sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5) id-ecdsa-with-sha1 (OID: 1.2.840.10045.4.1)
signatureValue	Електронен подпис на ДУУ

Предвижда се издаване удостоверения с пояснителен текст "TEST" в subject (Distinguished Name) полетата (без EGN/EIK) за случаи, изискващи допълнителни настройки на системи за верифициране на КЕП SEP Organization. Предназначението на такива Удостоверения за КЕП е само и единствено за провеждане на тестове.

3. Профил на eSign Qualified Profession

Удостоверение от типа SEP Qualified Profession се използва за потвърждаване на съгласието/самоличността и професионална принадлежност на лице, извършващо услуги с личен труд или упражняващо свободна професия, при участие в електронен обмен, като Web-базирани приложения, подписване на електронни документи и/или договори, банкови транзакции и извършване на изявления по смисъла на ЗЕДЕП. Лицето е Титуляр и Автор на изявленията.

Изявленията са от името и за сметка на лицето.

Профил на eSignQualified Profession Удостоверение:

име на поле	стойност или ограничение на стойността	
version	Version 3	
serialNumber	Уникален сериен номер на удостоверението в рамките на издаващ удостоверяващия орган	
signature	sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5) id-ecdsa-with-sha1 (OID: 1.2.840.10045.4.1)	
issuer (Distinguished Name)	C	BG
	Street	1 Zlatovrah Str.
	L	Sofia
	O	System for Electronic Payments /SEP Bulgaria JSC

име на поле	стойност или ограничение на стойността	
	OU	eSign QES
	CN	eSign QES CA
validity	notBefore	UTC формат
	notAfter	UTC формат
subject (Distinguished Name)	*C	BG
	S	Област на Титуляра по адрес на регистрация
	*L	Населено място на Титуляра по адрес на регистрация
	O	Пълно име на юридическото лице – Титуляр
	*OU	SEP Qualified Profession
	OU	Организационна единица на Титуляра[професия, членство]
	UID (0.9.2342.19200300.100.1.1)	EGNxxxxxxxxx[ЕГН/ЛНЧ/ггммдд на Автора]/ друг идентификатор
	*CN	Име/псевдоним на Автора
	T	Позиция на Автора/овластяване
	OU	EIKxxxxxxxxx[ЕИК на титуляра] / друг идентификатор
	*E	Служебен e-mail Адрес на Автора за водене на кореспонденция от името на Титуляра
	Street	Служебен адрес на Автора
	Phone	Телефон на Автора
Key Usage	Digital Signature, Non-Repudiation, Key Encipherment, Data Encipherment (f0)	
Enhanced Key Usage	Client Authentication (1.3.6.1.5.5.7.3.2)	

име на поле	стойност или ограничение на стойността
	Secure Email (1.3.6.1.5.5.7.3.4)
Certificate Policies	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.30299.2.5.3 [1,1]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text=This certificate is issued as qualified certificate for qualified electronic signature using secure signature creation device [1,2]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.esign.bg
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.sep.bg/eSign_QES_ CA.crl
Authority Information Access	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.sep.bg
Basic Constraints	Subject Type=End Entity Path Length Constraint=None
Authority Key Identifier	
Subject Key Identifier	
Qualified Certificate	Посочва, че удостоверението е издадено като удостоверение за

име на поле	стойност или ограничение на стойността
Statements	квалифициран електронен подпис
subjectPublicKeyInfo	Публичният ключ на Титуляра/Автора и алгоритъмът, с който се използва
signatureAlgorithm	sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5) id-ecdsa-with-sha1 (OID: 1.2.840.10045.4.1)
signatureValue	Електронен подпис на ДУУ

Предвижда се издаване Удостоверения с пояснителен текст "TEST" в subject (Distinguished Name) полетата (без EGN/EIK) за случаи, изискващи допълнителни настройки на системи за верифициране на КЕП SEP Qualified Profession. Предназначението на такива Удостоверения за КЕП е само и единствено за провеждане на тестове.

XXIV. Идентификатор на подписващия алгоритъм

Полето signatureAlgorithm съдържа идентификатор на алгоритъма използван за създаване на електронен подпис от УО.

СЕП България използва следните алгоритми:

- sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5)
- id-ecdsa-with-sha1 (OID: 1.2.840.10045.4.1)

XXV. Поле с електронен подпис

Стойността на полето signatureValue е резултатът от хеш функция, изчислена по всички полета на Удостоверението и криптирана с частния ключ на издаващия УО на ДУУ.

XXVI. Профил на Списъка на прекратените удостоверения

„Списъкът на прекратените удостоверения" (CRL) съдържа следните полета:

- tbsCertList: информация за прекратените удостоверения;
- signatureAlgorithm: идентификатор на алгоритъма, използван за подписване на „Списъка на прекратени удостоверения";
- signatureValue: електронния подпис на УО, издал „Списъка на прекратените удостоверения".

Смисълът на signatureAlgorithm и signatureValue е аналогичен на удостоверенията за електронен подпис.

Полето tbsCertList съдържа поредица от задължителни и незадължителни полета. Задължителните идентифицират издателя на CRL, а незадължителните съдържат информация за прекратените удостоверения и разширенията на CRL.

Полетата са като следва:

- version: версия на формата на CRL.
- signature: идентификатор на използвания алгоритъм от издалия CRL УО;
- issuer: име на УО издал CRL. Всеки УО от йерархията на СЕП България, издава отделен CRL;
- thisUpdate: дата на публикуване на CRL кодирана в UTC формат;
- nextUpdate: известява за датата на която ще се публикува следващия CRL. Ако полето е налично, стойността му посочва най-крайната дата на публикуване. Възможно е CRL да се обнови преди тази дата.
- revokedCertificates: „Списък на прекратените удостоверения“ като полето е празно ако няма прекратени Удостоверения. Информацията се съдържа в следните подплета:
  - userCertificate: сериен номер на прекратеното Удостоверение;
  - revocationDate: дата, на която е прекратено Удостоверението;
  - crlEntryExtensions: допълнителна информация за прекратеното Удостоверение.
- crlExtensions: допълнителна информация относно CRL;
- AuthorityKeyIdentifier: позволява да се идентифицира публичния ключ, съответстващ на частния ключ, използван за подписване на CRL;
- CRLNumber: съдържа монотонно нарастваща последователност от числа. Предоставя лесен начин да се определи кога един CRL се заменя от друг.
- Причини за прекратяване:
  - unspecified: без посочване на конкретна причина за прекратяване;
  - keyCompromise: компрометиран частен ключ;
  - cACompromise: компрометиран ключ на УО;
  - affiliationChanged: обновени данни за Титуляра/Автора;
  - superseded: сертификата е подновен;
  - cessationOfOperation: Удостоверението е прекратено;
  - certificateHold: Удостоверението е спряно;
- removeFromCRL: Удостоверението е възобновено.

Профил на „Списъка на прекратените удостоверения“:

поле	стойност, подполе спойност	
version	Version 2	
issuer (Distinguished Name)	C	BG
	S	Sofia
	L	Sofia
	O	System for Electronic Payments /SEP Bulgaria JSC

	OU	SEP
	CN	{SEP Root CA, eSign QES CA}
	Street	1 Zlatovrah Str.
	E	eSign@sep.bg
thisUpdate	Дата на издаване на "Списъка на прекратените удостоверения"	
nextUpdate	Дата на издаване на следващ „Списък на прекратените удостоверения"	
signature	Електронен подпис на издателя на „Списъка на прекратените удостоверения"	
CRLNumber	Число от монотонно нарастваща редица	
AuthorityKeyIdentifier		
revokedCertificates	userCertificate	Сериен номер
	revocationDate	Дата на поставяне в „Списъка на прекратените удостоверения"
	crlEntryExtensions	{unspecified, keyCompromise, cACompromise, affiliationChanged, superseded, cessationOfOperation, certificateHold, removeFromCRL, privilegeWithdrawn}

XXVII. SEP TSA профил

Удостоверението за време е подписан от доставчика на удостоверителни услуги електронен документ, който удостоверява времето на представяне на електронен подпис, създаден за определен електронен документ.

Удостоверението на SEP TSA е в съответствие със стандарта RFC 3280, а заявките и отговорите към SEP TSA, за удостоверяване на време са съгласно RFC 3161.

Профил на удостоверението на SEP TSA:

име на поле	стойност или ограничение на стойността
version	Version 3
serialNumber	Уникален сериен номер на удостоверението в рамките на издаващия удостоверяващия орган
signature	sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5)

име на поле	стойност или ограничение на стойността	
issuer (Distinguished Name)	C	BG
	L	Sofia
	O	System for Electronic Payments /SEP Bulgaria JSC
	OU	SEP QES
	CN	SEP Root CA
validity	notBefore	UTCTime формат
	notAfter	UTCTime формат
subject (Distinguished Name)	C	BG
	L	Sofia
	O	System for Electronic Payments /SEP Bulgaria JSC
	OU	SEP QES
	CN	SEP TSA
	E	eSign@sep.bg
Key Usage	digitalSignature, nonRepudiation	
Enhanced Key Usage	timeStamping	

име на поле	стойност или ограничение на стойността
Certificate Policies	[1] Certificate Policy: Policy Identifier=1.3.6.1.4.1.30299.2.1.5 [1,1]Policy Qualifier Info: Policy Qualifier Id=User Notice explicitText: SEP TSA [1,2]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://e-sign.sep.bg
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.sep.bg/SEP_root_ca.crl
Authority Information Access	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.sep.bg
Basic Constraints	cA: no pathLenConstraint: 0
Issuer Alternative Names	
Subject Alternative Name	
Authority Key Identifier	

име на поле	стойност или ограничение на стойността
Subject Key Identifier	
subjectPublicKeyInfo	Публичният ключ на Титуляра/Автора и алгоритъма, с който се използва
signatureAlgorithm	sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5)
signatureValue	Електронен подпис на ДУУ

XXVIII. OCSP профил

Услугата по проверка статуса на издадените Удостоверения, СЕП България предоставя освен чрез достъп по CRL и чрез онлайн протокола за проверка статуса на издадените Удостоверения - OCSP. В този случай се предоставя информация за статуса на всички Удостоверения, издадени в йерархията на СЕП България.

Удостоверението, с което се проверява онлайн отговора, се издава от eSign QES CA. eSign QES CA подписва със своя частен ключ резултата от проверката преди да го изпрати на потребителя. OCSP удостоверението е съгласно RFC 3280, а заявките и отговорите към eSign QES CA, за удостоверяване на статуса на издадено от СЕП България удостоверение, са съгласно RFC 2560.

Профил на удостоверението на eSign OCSP:

име на поле	стойност или ограничение на стойността	
version	Version 3	
serialNumber	уникален сериен номер на удостоверението в рамките на издаващия удостоверяващия орган	
signature	sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5)	
issuer (Distinguished Name)	C	BG
	Street	1 Zlatovrah Str.
	L	Sofia
	O	System for Electronic Payments /SEP Bulgaria JSC
	OU	eSign QES
	CN	eSign QES CA

име на поле	стойност или ограничение на стойността	
	E	eSign@sep.bg
validity	notBefore	UTCTime формат
	notAfter	UTCTime формат
subject (Distinguished Name)	C	BG
	L	Sofia
	O	System for Electronic Payments /SEP Bulgaria JSC
	OU	eSign QES
	CN	eSign OCSP
	E	eSign@sep.bg
Key Usage	digitalSignature, nonRepudiation	
Enhanced Key Usage	OCSPSigning	
Certificate Policies	[1] Certificate Policy: Policy Identifier=1.3.6.1.4.1.30299.2.5.5 [1,1]Policy Qualifier Info: Policy Qualifier Id=User Notice explicitText: eSign OCSP [1,2]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.esign.bg	

име на поле	стойност или ограничение на стойността
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.sep.bg/eSign_QES_ CA.crl
Authority Information Access	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.sep.bg
Basic Constraints	cA: no pathLenConstraint: 0
Issuer Alternative Names	
Subject Alternative Name	
Authority Key Identifier	
Subject Key Identifier	
subjectPublicKeyInfo	Публичният ключ на Титуляра/Автора и алгоритъмът, с който се използва
signatureAlgorithm	sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5)
signatureValue	Електронен подпис на ДУУ

СЕП България включва в издаваните удостоверени в полето Authority Information Access информация за ползването на On-line проверка за статуса на издадени удостоверения.

Настоящият Наръчник е изготвен от СЕП България и одобрен с решение на Съвета на директорите от 21.06.2013г.