

СЕП България АД
София1113
бул. Шипченски проход № 18,
тел.: 0 700 18 283
www.e-sign.sep.bg



Наръчник за потребителя

Версия: 1.0
от 01.12.2011 г.

Съдържание

I.	Въведение.....	13
1.	Съдържание и характер на документа	13
2.	Детайлност и съдържание	13
3.	Срок на действие и прекратяване на действието.....	14
3.1	Срок на действие	14
3.2	Прекратяване действието на Наръчника	14
3.3	Последствия от прекратяване действието на Наръчника.....	14
4.	Уведомяване и комуникация.....	14
5.	Изменения и допълнения.....	14
6.	Разрешаване на спорове	15
7.	Приложимо законодателство	15
8.	Допълнителни разпоредби.....	15
8.1	Правоприемство	15
8.2	Отделяне на условията	15
8.3	Тълкуване	15
8.4	Форсмажор.....	15
8.5	Юрисдикция	15
9.	Ползвани източници	15
9.1	Нормативна уредба	16
9.2	Стандарти	16
10.	Определения и съкращения	16
10.1	Определения	16
10.2	Съкращения	17
II.	Практика при предоставяне на удостоверителни услуги на ДУУ.....	19
1.	Общ преглед	19
2.	Страни в удостоверителния процес	19
2.1	Удостоверяващи органи.....	19
2.1.1.	Базов удостоверяващ орган.....	19
2.1.2.	Оперативен удостоверяващ орган	20
2.1.3.	Удостоверяване на време (TimeStamp)	20
2.1.4.	On-line проверка статуса на КЕП (OCSP).....	20
2.2	Регистриращи органи	21
2.3	Крайни потребители	21

2.3.1.	Автор	21
2.3.2.	Титуляр	21
2.3.3.	Разграничаване на титуляр/автор	22
2.3.4.	Доверяващи се страни	22
2.4	Публичен регистър	22
2.5	Приложна сфера на КЕП.....	22
3.	Подходяща употреба.....	22
4.	Удостоверения за квалифициран електронен подпис.....	22
4.1	SEP Qualified Private удостоверение	23
4.2	SEP Qualified Organization удостоверение	23
4.3	SEP Qualified Profession удостоверение.....	23
4.4	SEP TSA удостоверение	23
5.	Използвани приложения	23
6.	Забрана за употреба	24
7.	Администриране на документа	24
8.	Публичен регистър	24
8.1	Публикувана информация.....	24
8.2	Периодичност на публикуване.....	24
8.3	Достъп до публичния регистър	24
8.4	Пазене на публичния регистър	25
9.	Идентификация и автентификация	25
9.1	Използвани имена	25
9.1.1.	Тип на имената	25
9.1.2.	Смисъл на имена.....	25
9.2	Правила за интерпретиране на различните именни форми	26
9.3	Уникалност на имената	26
9.4	Запазена марка.....	26
10.	Идентификация и автентификация при първоначална регистрация.....	27
11.	Методи за доказване контрола над частния ключ	27
12.	Проверка на идентичността на юридически лица.....	27
13.	Проверка самоличността на физически лица	28
14.	Непроверена информация.....	29
15.	Потвърждаване на представителството	29
16.	Подновяване	29
17.	Модификация на удостоверение – (Update)	30

18.	Идентификация и автентификация при прекратяване	30
19.	Идентификация и автентификация при спиране и възобновяване	30
19.1	Спиране на удостоверение	30
19.2	Възобновяване на удостоверение.....	31
20.	Жизнен цикъл на удостоверенията за КЕП.....	31
20.1	Подаване на искане.....	31
20.1.1.	Искане за първоначална регистрация.....	32
20.1.2.	Искане за издаване на удостоверение за КЕП	32
20.1.3.	Искане за подновяване или модификация на КЕП.....	33
20.1.4.	Искане на прекратяване или спиране	33
20.1.5.	Искане за възобновяване	34
20.2	Обработка на подадените искания.....	34
20.2.1.	On-line искания	34
20.2.2.	Off-Line искания	35
20.2.3.	Обработка на исканията от Регистриращ орган	35
20.2.4.	Обработка на исканията от Удостоверяващ орган	35
20.3	Издаване на удостоверение за електронен подпис	36
20.4	Отказ за издаване на КЕП.....	36
20.5	Приемане на удостоверение за електронен подпис.....	37
20.6	Използване на удостоверението и ключовата двойка.....	37
20.7	Подновяване.....	37
20.8	Модификация на удостоверение	38
20.9	Прекратяване на удостоверение	39
20.9.1	Обстоятелства, при които се допуска прекратяване	39
20.9.2	Кой може да иска прекратяване на удостоверение	40
20.9.3	Процедура за прекратяване на удостоверение	40
21.	Необходимост от проверка статуса на удостоверението.....	41
22.	Периодичност на публикуване на CRL.....	41
22.1	Спиране и възобновяване на удостоверение	41
22.1.1.	Обстоятелства при спиране на удостоверение	41
22.1.2.	Обстоятелства при възобновяване на удостоверение	42
22.1.3.	Кой може да иска спиране и възобновяване на удостоверение	42
22.2	Процедура по спиране и възобновяване на удостоверение.....	42
22.2.1.	Процедура по спиране на действието на удостоверение	42
22.2.2.	Процедура за възобновяване на действието на удостоверение.....	42
22.3	Ограничения на периода на спиране	43
22.4	On-line проверка на валидността на удостоверения	43
23.	Услуги по валидация	43
23.1	Експлоатационни характеристики	44

23.2	Достъпност на услугата.....	44
24.	Издаване на удостоверение за време.....	44
24.1	Процедура по предоставяне на услугата издаване на удостоверение за време ..	44
25.	Прекратяване ползване на удостоверителни услуги.....	44
26.	Съоръжения, ръководство и оперативни контроли	45
26.1	Съоръжения на доставчика	45
26.1.1.	Физическа сигурност УО и базов РО	45
26.1.2.	Физически достъп	45
26.1.3.	Електрозахранване и климатизация.....	45
26.1.4.	Наводнение.....	46
26.1.5.	Противопожарни мерки	46
26.1.6.	Съхраняване на носители.....	46
26.1.7.	Депозиране на отпадъци.....	46
26.1.8.	Съхранение на резервните копия.....	46
26.2	Съоръжения на РО	46
26.3	Сигурност на титуляра/автора	46
26.4	Контрол на процедурите	46
26.5	Доверени длъжности.....	47
26.6	Управление на персонала.....	47
26.6.1.	Квалификация и опит	47
26.6.2.	Обучение на персонала	47
26.6.3.	Процедури за действие при извънредни ситуации, повреди, аварии и природни бедствия.....	48
26.6.4.	Дисциплинарни мерки	48
26.7	Договори с външни лица	48
26.8	Документи предоставяни на персонала	48
27.	Водене на записи и преглеждане на журналите.....	48
27.1	Тип на записваните събития	49
27.2	Преглед на журналите.....	49
27.3	Период на съхранение	49
27.4	Защита на журналните файлове	50
27.5	Архивиране на журналните файлове	50
28.	Известяване за събития.....	50
29.	Оценка на уязвимостите	50
30.	Архивиране на записите.....	50
30.1	Типове архивни данни.....	51
30.2	Честота на архивиране	51
30.3	Период на съхраняване в архив	51

30.4	Защита на архива	51
30.5	Резервни копия на архива – процедура	52
30.6	Изискване за удостоверяване време за записите	52
30.7	Процедура за проверка на архивираната информация	52
31.	Смяна на ключовете	52
32.	Компрометиране и възстановяване след бедствия и аварии	53
32.1	Реакция при нарушения на сигурността	53
32.2	Щети по компютърни ресурси, софтуер и/или данни	53
32.2.1.	План за възстановяване след авария или природно бедствие	53
32.2.2.	Управление на промените	54
32.2.3.	Резервни системи	54
32.2.4.	Създаване на резервни копия	54
32.3	Допълнителни дейности	54
32.4	Компрометиране на частния ключ на УО	54
33.	Прекратяване или прехвърляне на дейността на УО	55
34.	Прекратяване или прехвърляне на дейността на РО	55
35.	Техническа и технологична сигурност	55
36.	Генериране и инсталиране на ключови двойки	55
36.1	Генериране на ключови двойки	56
36.1.1.	Генериране на ключовете на SEP Root CA	56
36.1.2.	Смяна на ключовете на SEP Root CA	56
36.1.3.	Смяна на ключовете на оперативния УО на ДУУ	56
36.2	Предоставяне на частния ключ на автора	57
36.3	Предоставяне на публичния ключ до УО	57
36.4	Предоставяне на публичния ключ на УО до доверяващите се страни	57
37.	Дължина на ключовете	57
38.	Защита на частния ключ	57
39.	Достъп до частния ключ на доставчика	58
40.	Архивиране на частния ключ	58
41.	Трансфер на частния ключ от и към криптомодула	58
42.	Съхраняване на частния ключ в криптомодула	58
43.	Унищожаване на частния ключ	58
44.	Сертификация на криптомодула	58
45.	Други аспекти от управлението на ключовете	59
45.1	Архивиране на публичния ключ	59

45.2	Период на валидност на удостоверенията и използване на ключовете	59
45.3	Данни за активиране	59
46.	Управление на компютърната сигурност	59
46.1	Технически изисквания.....	59
46.2	Оценка на сигурността	60
46.3	Технически контроли	60
46.3.1.	Управление контролите за информационна сигурност	60
46.3.2.	Мрежова сигурност	60
47.	Профили на удостоверения, списък с прекратени удостоверения и OCSP	60
47.1	Профили на удостоверенията	60
47.2	Съдържание на удостоверението.....	60
48.	Проверка и контрол на дейността	64
48.1	Честота и обстоятелства на проверките	64
48.2	Избягване конфликт на интереси	64
48.3	Обхват и детайлност на проверките.....	64
48.4	Съобщаване на резултатите.....	65
49.	Търговски и правни условия	65
49.1	Цени на удостоверителните услуги	65
49.2	Цени на услуги	65
49.3	Възстановяване на суми	65
49.4	Финансова отговорност	66
49.4.1.	Застраховка на дейността.....	66
49.4.2.	Застрахователно покритие за крайните потребители	66
50.	Конфиденциалност на информацията	66
50.1	Обхват на конфиденциалната информация	66
50.2	Информация извън обхвата на конфиденциалната информация	67
50.3	Задължение за пазене на конфиденциалната информация.....	67
51.	Защита на личните данни	67
52.	Права върху интелектуалната собственост	67
53.	Задължения и отговорности.....	67
53.1	Задължения и отговорности на „СЕП България“ АД.....	67
53.2	Задължения и отговорности на регистриращите органи.....	68
53.3	Задължения и отговорности на титуляра/автора.....	68
53.4	Задължения и отговорности на доверяващата се страна.....	69
53.5	Ограничаване на отговорността	69

54.	Лимит на отговорността	70
55.	Обезщетения и компенсации	70
III.	Политика при предоставяне на удостоверителни услуги.....	71
1.	Обхват	71
2.	Общ преглед	71
3.	Модел на удостоверителни услуги	71
3.1	Регистриране	71
3.2	Създаване на удостоверения	71
3.3	Прекратяване на удостоверения	72
3.4	Статус на издадените удостоверения	72
3.5	Предоставяне на устройства	72
3.6	Удостоверяване на време	72
4.	Предназначение	72
5.	Ниво на детайлност	72
6.	Подход.....	72
7.	Документи по отношение на трети страни	72
8.	Изисквания към дейността на ДУУ	73
9.	Инфраструктура за доставка на удостоверителни услуги – Управление на ключовете	73
9.1	Генериране на ключовете на ДУУ	73
9.1.1.	Защитена среда.....	73
9.1.2.	Упълномощен персонал.....	73
9.1.3.	Поделяне на секретни части.....	74
9.1.4.	Надеждни системи.....	74
9.2	Генериране на ключовете на „СЕП България” АД	74
9.2.1.	Стартова процедура.....	74
9.2.2.	Криптографски хардуер.....	74
9.2.3.	Използвани алгоритми	74
9.2.4.	Дължина на ключа	74
9.2.5.	Гарантиране непрекъснатост на операциите	74
9.3	Съхраняване, архивиране и възстановяване ключове на ДУУ.....	74
9.3.1.	Държане и ползване на частния ключ.....	74
9.3.2.	Защита на частния ключ	75
9.3.3.	Архивиране на частния ключ	75
9.3.4.	Копия на частния ключ	75
9.3.5.	Разпространяване на публичните ключове на ДУУ.....	75
9.3.6.	Източник и интегритет на публичния ключ.....	75
9.3.7.	Защита частния ключ на доставчика.....	75

9.4	Използване на ключовете на ДУУ	75
9.5	Физическа защита.....	75
9.6	Прекратяване на жизнения цикъл на ключове на ДУУ	75
9.7	Жизнен цикъл на криптографския хардуер ползван за подписване на КЕП	75
9.7.1.	Доставка на криптографски хардуер	76
9.7.2.	Съхранение на криптографски хардуер	76
9.7.3.	Съвместен контрол.....	76
9.7.4.	Функциониране на криптографския хардуер.....	76
9.7.5.	Унищожаване на частните ключове в криптографския хардуер	76
10.	Осигуряване на титуляра/автора услуги по управление на ключовете.....	76
10.1	Използвани алгоритми	76
10.2	Дължина на ключовете.....	76
10.3	Съхраняване на генерираните ключове.....	76
10.4	Предоставяне на ключовете	76
10.5	Данни за активиране	77
11.	Инфраструктура за доставка на удостоверителни услуги – Управление жизнения цикъл на КЕП.....	77
11.1	Регистрация на титуляра/автора	77
11.1.1.	Предоставяне на информация за удостоверителните услуги	77
11.1.2.	Канали за информиране	77
11.1.3.	Проверка регистрация.....	77
11.2	Идентификация на физически лица	77
11.3	Идентификация на юридически лица	77
11.4	Съхранявана информация.....	78
11.4.1.	Данни за представителство	78
11.4.2.	Данни за обратна връзка.....	78
11.5	Договорни отношения.....	78
11.6	Време за съхранение	78
11.7	Притежание на частния ключ.....	78
11.8	Притежание на SSCD	78
11.9	Подновяване, смяна на ключове и актуализиране	78
11.9.1.	Актуален КЕП.....	79
11.9.2.	Променени условията на „СЕП България” АД	79
11.9.3.	Променено съдържание на КЕП	79
11.9.4.	Запазване на ключовата двойка	79
11.10	Създаване на удостоверение	79
12.	Идентификация.....	79
12.1	Идентификатор на политиката	79

12.2	Потребителска общност и приложение на КЕП.....	79
12.3	Спазване на политиката.....	80
12.3.1.	Общи сведения.....	80
12.3.2.	Съответствие с политиката.....	80
12.4	Профил на КЕП.....	80
13.	Мерки срещу фалшифициране на КЕП.....	80
14.	Сигурна генерация.....	80
15.	Конфиденциалност и интегритет на данните за регистрация.....	80
16.	Проверка на източника на регистрационните данни.....	81
17.	Разпространяване на реда и условията.....	81
18.	Публикувана информация.....	81
19.	Достъпност и разпространение на информацията.....	81
19.1	Достъп при генерация.....	81
19.2	Ограничаване на достъпа.....	81
19.3	Информация за доверяваща се страна.....	81
19.4	Предоставяне на информация за КЕП.....	81
19.5	Публичност и достъпност на информацията за КЕП.....	82
20.	Прекратяване, спиране и възобновяване на КЕП.....	82
20.1	Документиране на процедурата.....	82
20.2	Приемане на искания за прекратяване/спиране.....	82
20.3	Проверка на заявките.....	82
20.4	Спиране на КЕП преди прекратяване.....	82
20.5	Информирание за промяна на статуса.....	82
20.6	Необратимост на прекратяването.....	82
21.	Списък с прекратени удостоверения.....	82
21.1	Достъпност на списъка с прекратени удостоверения.....	83
21.2	Статус на удостоверенията за електронен подпис.....	83
22.	Интегритет и автентичност на информацията за статуса на КЕП.....	83
22.1	Публикуване на информация за статуса на КЕП.....	83
22.2	Период на съхранение на прекратените КЕП в CRL.....	83
23.	Базово удостоверение на УО.....	83
24.	Удостоверение на оперативния УО.....	85
25.	Потребителски удостоверения.....	87
25.1	Профил на SEP Qualified Private.....	87

25.2	Профил на SEP Qualified Organization.....	88
25.3	Профил на SEP Qualified Profession	90
26.	Идентификатор на подписващия алгоритъм	92
27.	Поле с електронен подпис	92
28.	Профил на списъка с прекратени удостоверения	92
29.	SEP TSA профил	94
30.	OCSP профил	95

Авторското право върху настоящия документ принадлежи на "СЕП България" АД.
Всяко използване на цялата или на част от него, извършено без съгласието на "СЕП България" АД,
представлява нарушение на Закона за авторското право и сродните му права.

I. Въведение

„СЕП България“ АД е регистрирано, като доставчик на удостоверителни услуги (ДДУ) от Комисията за регулиране на съобщенията по реда определен от ЗЕДЕП с документ за регистрация № 1170 от 17.07.2008 г.

Този „Наръчник за Потребителя“ (НАРЪЧНИК) обединява Практиката при предоставяне на удостоверителни услуги на ДУУ „СЕП България“ АД (тук и по-долу споменавана като „ПРАКТИКА“), детайлизира правилата по отношение на удостоверителната практика на „СЕП България“ АД, описани в „Политиката по предоставяне на удостоверителни услуги“ (тук и по-долу споменавана като „ПОЛИТИКА“) и описва процесите по предоставяне на удостоверителни услуги и областта на приложение на удостоверенията за електронен подпис, резултат от тези услуги.

1. Съдържание и характер на документа

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

- „Политика за предоставяне на удостоверителни услуги“;
- „Практика при предоставяне на удостоверителни услуги“.

„Наръчник за потребителя“ е публичен документ за ДУУ, има характер на общи условия и е обвързващ за издателя си. Той се представя на Комисията за регулиране на съобщенията и на всички заинтересовани страни.

2. Детайлност и съдържание

Документът „Политика за предоставяне на удостоверителни услуги“ описва политиката на издаване на удостоверения от доставчика и видовете услуги, предоставяни от „СЕП България“ АД.

Документът „Практика при предоставяне на удостоверителни услуги“ е документ, разработен в съответствие с изискванията на политиката по предоставяне на удостоверителни услуги и описва процедурите по издаване на удостоверения от „СЕП България“ АД и видовете предоставяни услуги.

Практиката съдържа важна информация за титулярите/авторите на КЕП и трети доверяващи се страни.

Политиката на „СЕП България“ АД описва общите правила на удостоверителната практика на „СЕП България“ АД, като определя детайлността и характера на практиката, участниците в удостоверителния процес, техните задължения и отговорности, типовете КЕП, процедурите по проверка на идентичността съответно на самоличността на титуляра/автора, областта на приложение на КЕП.

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

Практиката на „СЕП България“ АД отразява политиките по издаване на КЕП на физически, юридически лица и лица упражняващи свободни професии. Приложимостта на тези КЕП и отговорностите на получателите на КЕП, ДУУ и доверяващите се страни.

Настоящият НАРЪЧНИК 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.

Всички документи, които имат публичен характер са достъпни на адрес: <http://e-sign.sep.bg>.

Наръчникът на „СЕП България“ АД е достъпен в електронна форма в директорията на „СЕП България“ АД на електронен адрес <http://e-sign.sep.bg>

3. Срок на действие и прекратяване на действието

3.1 Срок на действие

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

Срокът на Договора за удостоверителни услуги е равен на срока на валидност на издадените по него удостоверения или докато изтече срокът на валидност на всички издадени въз основа на него удостоверения.

3.2 Прекратяване действието на Наръчника

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

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

Договорът за удостоверителни услуги се прекратява с прекратяване на действието на всички издадени въз основа на него удостоверения или при наличието на други основания за прекратяване, посочени в Наръчника за потребителя.

3.3 Последствия от прекратяване действието на Наръчника

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

4. Уведомяване и комуникация

Всяка заинтересована страна може да отправи съобщение до „СЕП България“ АД във връзка с дейностите по предоставяне на удостоверителни услуги писмено или по електронен път.

За уведомяване и изпращане на индивидуални съобщения до титуляра/автора, или определени лица, участващи в удостоверителния процес, „СЕП България“ АД изпраща на предоставен от тях електронен адрес писма по електронна поща подписани с квалифициран електронен подпис или sms.

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

5. Изменения и допълнения

„СЕП България“ АД, при необходимост променя и допълва този Наръчник. Всяка промяна в него се съобщава пред Комисията за регулиране на съобщенията.

Всяко лице може да отправя предложения за промени и допълнения или да посочи грешки и непълноти като ги изпрати на „СЕП България“ АД.

„СЕП България“ АД уведомява участниците в удостоверителния процес за настъпилите промени в документите, регламентиращи дейността му.

Удостоверенията, издадени от „СЕП България“ АД, се подновяват при условията на текущите актуални Политика за предоставяне на удостоверителни услуги и Практика при предоставяне на удостоверителни услуги.

6. Разрешаване на спорове

При възникване на спорове във връзка с предоставянето на удостоверителни услуги от „СЕП България“ АД, заинтересованите лица могат да подават жалби.

Жалбите се подават в писмена форма до изпълнителния директор на „СЕП България“ АД чрез началника на отдел “Удостоверителни услуги” на следния адрес:

Адрес: „СЕП България“ АД, гр. София, 1113,
бул. „Шипченски проход“ № 18.

В седемдневен срок от подаването на жалбата, Мениджър „Обслужване на клиенти“ изпраща жалбата и писменото си становище по нея на изпълнителния директор на „СЕП България“ АД.

Изпълнителният директор на „СЕП България“ АД се произнася по жалбата в четиринадесетдневен срок от получаването, за което писмено уведомява жалбоподателя.

7. Приложимо законодателство

За неуредените в настоящия Наръчник при предоставяне на удостоверителни услуги въпроси се прилага българското законодателство.

8. Допълнителни разпоредби

8.1 Правоприемство

Правата и задълженията, посочени в този Наръчник, могат да бъдат прехвърляни от страните по взаимно съгласие, 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.

8.2 Отделяне на условията

Ако някоя от клаузите в този Наръчник или нейното прилагане се окаже недействителна или изпълнима изцяло или частично, то клаузата ще бъде тълкувана по такъв начин, че да отговаря на първоначалните намерения на страните.

8.3 Тълкуване

Този Наръчник при предоставяне на удостоверителни услуги следва да се тълкува в съответствие с общоприетите бизнес практики при дадените обстоятелства и ползването на продукта или услугата по предназначение.

8.4 Форсмажор

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

8.5 Юрисдикция

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

9. Ползвани източници

При разработката на Наръчника са използвани два вида източници:

Нормативни – закони и подзаконови актове.

Международно признати стандарти – Европейска стандартизационна рамка базирана на документите на ETSI и CEN Workshop Agreement.

Използват се последните актуални версии на източниците към момента на публикуване на настоящия документ.

9.1 Нормативна уредба

При разработката на настоящия Наръчник са взети предвид следните нормативни документи:

- [1] ЗЕДЕП: „Закон за електронния документ и електронния подпис“;
- [2] НРРДУУ: „Наредба за реда за регистрация на доставчиците на удостоверителни услуги“;
- [3] НДДУУ: „Наредба за дейността на доставчиците на удостоверителни услуги“;
- [4] НИАСПКЕП: „Наредба за изискванията към алгоритмите за създаване и проверка на квалифициран електронен подпис“;
- [5] НРУВСДРДУУ: „Наредба 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“.

9.2 Стандарти

При разработката на настоящия Наръчник са взети предвид следните международно признати стандарти:

- [1] RFC 3280: „Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile“;
- [2] RFC 3628: “Requirements for Time-Stamping Authorities“;
- [3] RFC 3647: „Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework“;
- [4] RFC 3739: „Internet X.509 Public Key Infrastructure: Qualified Certificates Profile“;
- [5] ETSI TS 101 456 V1.4.3: “Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates” technical specification (2007-05);
- [6] ETSI TS 101 862 V1.3.3: “Qualified Certificate profile” technical specification (2006-01);
- [7] ETSI TS 102 023 v.1.2.1: “Policy Requirements for time-stamping authorities”(2003-01);
- [8] ANSI X9.79: "Public Key Infrastructure (PKI) - Practices and Policy Framework";
- [9] CWA 14167-1: "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1 System Security Requirements".

10. Определения и съкращения

В този раздел се представят използваните съкращения и се дават определенията на използваните термини.

10.1 Определения

В настоящия документ са използвани следните определения:

Автор: автор на електронното изявление е физическото лице, което в изявлението се сочи като негов извършител. Авторът се идентифицира в КЕП като притежател на частния ключ, съответстващ на публичния ключ в КЕП.

Данни за проверка на подписа: данни, като кодове и публични криптографски ключове, използвани за проверка на електронния подпис.

Доверяваща се страна: получатели на КЕП, например като част от електронни изявления, които предприемат действия, доверявайки се на удостоверението и/или на електронните подписи, проверени чрез публичния ключ от това удостоверение.

Квалифициран електронен подпис: 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 и удостоверяващо връзката между автора и публичния ключ за проверка на подписа, и
- е създаден посредством устройство за сигурно създаване на подписа.

Устройство за сигурно създаване на електронен подпис (SSCD): механизъм за създаване на електронен подпис, който отговаря на изискванията на чл. 17, ал. 1 ЗЕДЕП.

Механизъм за проверка на подписа: е конфигуриран софтуер или хардуер, използван за прилагане на данните за проверка на подписа.

Персонален идентифициращ номер (ПИН): поредица от символи, която служи като идентификатор на притежателя на средството за идентификация.

Пълномощник: лице упълномощено от титуляра или автора да подаде искане за издаване на КЕП или да предприема други дейности свързани с промяна статуса на издадените КЕП.

Титуляр: титуляр на електронното изявление е лицето, от името, на което е извършено електронното изявление. Титулярът подава искане за издаване на КЕП, от свое име или от името на други лица, които упълномощава да извършват електронни изявления от негово име и сключва договор с ДУУ.

Удостоверение за квалифициран електронен подпис (КЕП): Удостоверението е електронен документ, издаден и подписан от доставчика на удостоверителни услуги, който може да съдържа:

- указание, че удостоверението е издадено за квалифициран 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;
- усъвършенствания 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, когато той е акредитиран.

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.

Идентификаторът на обект (OID): е уникална поредица от цели числа, която се присвоява на регистриран обект.

Online Certificate Status Protocol (OCSP): е Интернет протокол за on-line проверка на статуса на издадено удостоверение за електронен подпис.

10.2 Съкращения

В настоящия документ са използвани следните съкращения:

SSCD Устройство за сигурно създаване на електронен подпис

ДУУ Доставчик на удостоверителни услуги

ЕП	Електронен подпис
УО	Удостоверяващ орган
Политика	Политика за предоставяне на удостоверителни услуги; ППУИ
Практика	Практика при предоставяне на удостоверителни услуги; ППУ
РО	Регистриращ орган
УД	Удостоверителна дейност
УЕП	Удостоверение за електронен подпис
КЕП	Квалифициран електронен подпис
УсЕП	Усъвършенстван електронен подпис
УУ	Удостоверителни услуги
OID	Object Identifier
OCSP	Online Certificate Status Protocol
SEP ROOT	Базов удостоверяващ орган на „СЕП България“ АД
SEP CA	Удостоверяващ орган на „СЕП България“ АД
TSA	Time Stamp Authority
e-sign	Бранд на удостоверителните услуги по предоставяне и управление на удостоверения за електронен подпис, удостоверения за време, криптографски и PKI услуги

II. Практика при предоставяне на удостоверителни услуги на ДУУ

1. Общ преглед

Практиката при предоставяне на удостоверителни услуги е описание и основна част от документите за дейностите на Удостоверяващия орган и регистриращите органи, титуляр/автор и доверяващите се страни.

Удостоверителните услуги на „СЕП България“ АД се предоставят чрез йерархия от удостоверяващи органи, подписващи типовете издавани удостоверения за електронен подпис, обектите за удостоверяване на време и резултата от on-line проверката за статуса на удостоверенията за електронен подпис.

„СЕП България“ АД има един оперативен удостоверяващ орган, йерархично разположен под базовия удостоверяващ орган. Оперативният удостоверяващ орган подписва различните типове КЕП издавани от ДУУ – „СЕП България“ АД и удостоверението за on-line валидация. Базовият удостоверяващ орган подписва оперативния удостоверяващ орган и удостоверението за валидация на удостоверено време.

КЕП, издадени от „СЕП България“ АД, включват в съдържанието си идентификатор на политиката, според която са издадени и по този начин подпомагат доверяващите се страни при проверката за приложимост на КЕП.

„СЕП България“ АД се ръководи в своята дейност от законите на Република България и правилата, произтичащи от „Политиката по предоставяне на удостоверителни услуги“ на „СЕП България“ АД.

„СЕП България“ АД разработва редица съпровождащи документи, които имат различен характер и в зависимост от това се определя достъпа до тях.

2. 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“ АД. Описва процеса по предоставяне на удостоверителни услуги, взаимодействието между РО, УО, автори/титуляри и доверяващи се страни. Практиката е водещ документ и при осъществяване на проверки на дейността на ДУУ. Отнася се до дейността на:

- Удостоверяващите органи – SEP Root CA, SEP QES CA;
- Регистриращите органи;
- Авторите/Титулярите на удостоверения за КЕП;
- Доверяващите се страни.

„СЕП България“ АД предоставя удостоверителни услуги на всички юридически и физически лица, приемащи правилата и практиките, описани в този документ. Целта е потребителите на удостоверителните услуги на „СЕП България“ АД да се уверят, че декларираната сигурност и довереност е отразена в практиката на доставчика при предоставяне на удостоверителни услуги.

2.1 Удостоверяващи органи

„СЕП България“ АД предоставя удостоверителни услуги чрез йерархия от удостоверяващи органи и мрежа от регистриращи органи (РО), като издава и управлява КЕП на автори (физически лица), респективно титуляри (юридически или физически лица). „СЕП България“ АД в качеството си на ДУУ публикува и предоставя информация за статута на КЕП на доверяващите се страни за целите на проверка на електронни подписи.

2.1.1. 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“ АД. SEP Root CA функционира на база на УЕП издаден от самия него. **В това УЕП не се включва OID за политиката, спрямо която се издават и управляват УЕП.** 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“ АД. Това означава, че удостоверителния път за всеки издаден КЕП в йерархията на ДУУ започва от УЕП на УО – SEP Root CA.

Базовият УО на „СЕП България“ АД – SEP Root CA издава УЕП за:

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

2.1.2. Оперативен удостоверяващ орган

Оперативен УО на „СЕП България“ АД е SEP QES CA. Оперативният УО издава КЕП в съответствие с „Политика за предоставяне на удостоверителни услуги“ на „СЕП България“ АД на физически или юридически лица. Включва в издадените 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	SEP QES CA	Обект/Типове удостоверения	
1.3.6.1.4.1.30299	2	1	1	SEP Qualified Private
			2	SEP Qualified Organization
			3	SEP Qualified Profession
			4	SEP Server
			5	SEP TSA
			6	SEP OCSP

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

Оперативният УО издава удостоверения за КЕП на потребители.

Оперативният УО издава удостоверението за проверка на On-line отговора за статуса на издадено удостоверение за електронен подпис (OCSP)s.

2.1.3. Удостоверяване на време (TimeStamp)

SEP TimeStamp удостоверения за време се издават на физически и на юридически лица, които са автори, съответно титуляри или са доверяващи се страни. Удостоверението за време има официална удостоверителна сила след вписването му във воденият от SEP 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

2.1.4. On-line проверка статуса на КЕП (OCSP)

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

обект	идентификатор на политика
SEP OCSP	1.3.6.1.4.1.30299.2.1.6

2.2 Регистриращи органи

Регистриращите органи са част от инфраструктурата на „СЕП България“ АД за предоставяне на удостоверителни услуги. РО представляват „СЕП България“ АД при контакта с титулярите/авторите 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 КЕП.

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

- Приемат, проверяват, одобряват или отхвърлят исканията за издаване на КЕП;
- Приемат, проверяват, одобряват или отхвърлят исканията за управление на КЕП;
- Участват във всички етапи при идентифицирането на заявителите на удостоверителни услуги и проверка на самоличността, съответно на тяхната идентичност;
- Други дейности свързани с предоставяне на удостоверителни услуги описани в политиките, практиките и процедурите на ДУУ.

Регистриращите органи действат от името на „СЕП България“ АД след одобрение от страна на „СЕП България“ АД, в съответствие с неговите политики, практики и процедури. „СЕП България“ АД следи за спазване на всички изисквания посочени в настоящия документ от Регистриращите органи.

РО приема, проверява и одобрява или отхвърля искания за регистриране и издаване на КЕП, подновяване, спиране/възобновяване и прекратяване на КЕП. Проверката на искането има за цел да удостовери автентичността на искането, като се основава на приложените към искането документи, както и данните включени в искането. Начинът на проверка и необходимите документи придружаващи искането се определя от заявените КЕП.

При проверка на идентичността съответно самоличността на титуляра/автора операторите на РО пряко или непряко идентифицират лицата, на които ще се издават КЕП, като използват методи за идентификация, даващи същата степен на увереност като физическата идентификация.

„СЕП България“ АД сключва договор с РО, в който се детайлизират обхвата и операциите, за които е оторизирани РО, като Наръчника за потребителя на ДУУ е част от този договор.

РО регистрират исканията на крайните клиенти за всички видове удостоверителни услуги в зависимост от оторизацията, която имат от ДУУ.

Всяко юридическо може да функционира като РО на ДУУ – „СЕП България“ АД, стига да заяви това и да изпълни условията, произтичащи от регламентиращите документи на ДУУ.

Списък на РО, които са оторизирани от ДУУ, е публичен и е достъпен чрез публичния регистър на интернет адреса на доставчика.

2.3 Крайни потребители

Крайни потребители на удостоверителните услуги на „СЕП България“ АД са автори/титуляри и доверяващи се страни.

Информация за автора/титуляря се вписва в съответни полета на КЕП и се идентифицират от нея.

Доверяващите се страни използват удостоверенията за КЕП, издадени на автори/титуляри, за да проверят валидността на електронни подписи, идентичността на подписалия или за да осигурят конфиденциалност и непроменяемост на информацията, която изпращат.

Крайният потребител може да подава искания до ДУУ, чрез свой упълномощен представител.

2.3.1. Автор

Автор на електронното изявление - физическото лице, което в изявлението се сочи като негов извършител. Никой освен автора няма право на достъп до данните за създаване на КЕП.

2.3.2. Титуляр

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

2.3.3. Разграничаване на титуляр/автор

Когато КЕП е издадено на физическо лице за лично ползване, физическото лице се явява титуляр и автор. В този случай титуляра и автора съвпадат.

Когато КЕП е издадено по искане на юридическо лице за негови служители, то юридическото лице е титуляр, а служителите на юридическото лице автори. В този случай титуляра и автора се различават.

2.3.4. Доверяващи се страни

Доверяващата се страна е отговорна за проверката на текущия статус на КЕП, след което решава дали да се довери или да не се довери. Такова решение се взема всеки път, когато доверяващата се страна желае да използва КЕП, за да провери електронен подпис, да идентифицира източника или автора на съобщение, или да изгради защитен комуникационен канал с притежателя на КЕП. Доверяващата се страна трябва да използва информацията от КЕП (идентификатор на политиката) за да определи дали определено удостоверение за КЕП се използва правилно и в съответствие с определена Политика за предоставяне на удостоверителни услуги.

2.4 Публичен регистър

Публичният регистър е набор от публично достъпни каталози и директории, съдържащи:

- Издадените удостоверенията на всички УО от инфраструктурата на ДУУ;
- Всички издадени удостоверения от ДУУ;
- Списъците с прекратени удостоверения;
- Предишни и актуални версии на документите, регламентиращи дейността на ДУУ;
- Друга информация, която може да се променя и модифицира в реално време.

„СЕП България“ АД в качеството си на ДУУ поддържа електронен публичен регистър.

Съдържанието на регистъра е достъпно на интернет адреса на доставчика.

2.5 Приложна сфера на КЕП

Приложната сфера на издадените от ДУУ – „СЕП България“ АД удостоверения за КЕП се определя от обхвата на допустимото им използване. Този обхват се дефинира като дейности, за които може да се използва КЕП.

КЕП, издавани от „СЕП България“ АД, могат да се използват за обработка и защита на информация. Това са дейности, които включват идентификация, подписване, автентификация и криптиране.

Доверяващите се страни преценяват дали типът на КЕП и гаранциите, свързани с него са достатъчни за целите, за които се използва. Титулярите трябва да са запознати с изискванията на доверяващата се страна и да подадат заявка за подходящ тип КЕП.

3. Подходяща употреба

„СЕП България“ АД издава удостоверения за квалифициран електронен подпис и специализирани удостоверения за електронен подпис.

4. Удостоверения за квалифициран електронен подпис

Удостоверенията за квалифициран електронен подпис могат да се използват за дейности, които приравняват електронният подпис, положен на електронния документ с аналогичен саморъчен подпис, положен на документ в хартиена форма.

Електронният подпис, за който е издадено удостоверение от „СЕП България“ АД от следния тип: SEP Qualified Private, SEP Qualified Organization и SEP QES Profession, в съответствие с тази практика, има значението на саморъчен подпис по отношение на всички, включително и държавен орган или орган на местното самоуправление.

4.1 SEP Qualified Private удостоверение

За потвърждаване съгласието/самоличността на 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.

4.2 SEP Qualified Organization удостоверение

За потвърждаване на съгласието/самоличността, съответно на идентичността, на автора/титуляра 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.

4.3 SEP Qualified Profession удостоверение

За потвърждаване на съгласието/самоличността и професионална принадлежност на 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. Лицето е титуляр и автор на изявленията.

Изявленията са от името и за сметка на лицето.

4.4 SEP TSA удостоверение

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.

5. Използвани приложения

КЕП, издадени в съответствие с Наръчника се използват с приложения, които отговарят най-малко на следващите изисквания:

- Приложенията по подходящ начин управляват частните и публичните ключове, както и тяхното използване;
- КЕП и асоциираните публични ключове, се използват в съответствие с определеното предназначение, одобрено от „СЕП България“ АД;
- Имат вграден механизъм за проверка статуса на 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 КЕП и самото приложение на автора.

Списък с препоръчани и проверени приложения се публикува в публичния регистър на ДУУ на адрес: <http://e-sign.sep.bg>.

Приложенията се включват в списъка с препоръчаните приложения на база писмена декларация на производителя и/или тестове проведени от „СЕП България“ АД.

6. Забрана за употреба

КЕП, издадени от УО на „СЕП България“ АД да не се използват за цели или с приложения, неотговарящи на изискванията, посочените по-горе.

7. Администриране на документа

„СЕП България“ АД разработва чернова, предоставя за одобрение съгласно вътрешните правила, поддържа и адаптира настоящата „Практика при предоставяне на удостоверителни услуги“.

8. Публичен регистър

„СЕП България“ АД в качеството си на Доставчик на удостоверителни услуги води електронен регистър, в който публикува удостоверенията на УО от своята йерархия, издадените удостоверения и информацията необходима на страните, ползващи удостоверителните услуги.

8.1 Публикувана информация

„СЕП България“ АД публикува в регистъра информация за:

- Своите удостоверения за електронен подпис;
- Издадените удостоверения за електронен подпис;
- Издадените удостоверения за време;
- Отделен Списък с прекратените удостоверения;
- Наръчник за потребителя;
- Начина на използване на електронен подпис;
- Цената за получаване и използване на удостоверение, както и цените на останалите услуги, предоставяни от доставчика на удостоверителни услуги.

8.2 Периодичност на публикуване

„СЕП България“ АД поддържа актуална информация в своя публичен регистър като го актуализира със следната периодичност:

Наръчник за потребителя – съобразно изискванията на ЗЕДЕП и подзаконовите му нормативни актове;

Списъците на спрените и прекратените удостоверения извършва автоматично или поне през 3 часа;

При всяко настъпило събитие;

Актуална и допълнителна информация относно предоставянето на удостоверителни услуги – при необходимост.

8.3 Достъп до публичния регистър

„СЕП България“ АД води електронен регистър на издадените от него удостоверения с X.500 и LDAP базиран достъп.

„СЕП България“ АД не ограничава достъпа до регистъра и съдържащата се в него информация.

Авторът може да ограничи достъпа до удостоверението за своя подпис, като посочи това по време на регистрацията. Ограничаването се осъществява чрез възпрепятстване възможността за изтегляне на удостоверението. Когато достъпа е ограничен, „СЕП България“ АД предоставя само следната информация от съдържанието на удостоверението. Данните включват, но не са ограничени само до:

- Име/псевдоним на автора;
- Наименование на титуляра юридическо лице;
- Сериен номер на удостоверението;
- Период на валидност на удостоверението;
- Статус на удостоверението.

Независимо от това дали достъпът до удостоверението е ограничен или не, „СЕП България“ АД винаги предоставя информация за неговия статус.

Достъпът до „Списъка с прекратени удостоверения“ не се ограничава по никакъв начин.

8.4 Пазене на публичния регистър

„СЕП България“ АД пази своя публичен регистър така, че:

- 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.

9. Идентификация и автентификация

Този раздел представя общите правила за проверка на самоличността, съответно на идентичността, на автора и на титуляра прилагани от „СЕП България“ АД при издаване на КЕП и преди да се издаде удостоверение за електронен подпис. Правилата се основават на конкретния тип информация която се включва в удостоверенията. ДУУ е задължен да осигури точността и верността на тази информацията в момента на издаване на КЕП или постъпване на искане за управление на КЕП.

Проверката задължително се извършва по време на регистрацията и подаване на искане от автора или титуляра.

9.1 Използвани имена

9.1.1. Тип на имената

КЕП, издавани от „СЕП България“ АД отговарят на стандарт X.509 v3. На практика това означава, че 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“ АД включва в съдържанието на КЕП електронен адрес в съответствие с RFC822.

Имената на директориите, където се съхраняват удостоверенията за електронен подпис, списъците с прекратени 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 удостоверения за КЕП съдържат информация както е определено в чл.24 от ЗЕДЕП. Минималната информация, която се включва е както следва:

- Данни за ДУУ издал КЕП;
- Политиката, според която се издава КЕП;
- Данни за автора/титуляра;
- Уникален идентификатор на удостоверението;
- Ползвани алгоритми;
- Ограничения в ползването на удостоверението.

Списъка с данните, които се включват в КЕП и тяхната интерпретация е в съответствие с X.509 v3 и е представена в глава Профили на удостоверения, списък с прекратени удостоверения и OCSP.

9.1.2. Смисъл на имена

Имената, включени в потребителския Distinguished Name имат конкретен смисъл и съдържат идентифициращата информация за автора/титуляра и издателя на КЕП.

Структурата на Distinguished Name се одобрява/присвоява и проверява от РО в зависимост от автора/титуляра и типа удостоверение.

Distinguished Name може да съдържа набор от следните полета, чието описание и абривиатури на имената е в съответствие с препоръките RFC 3280 и X.520:

C, Country	– страната, на чиято територия ДУУ осъществява своята на дейност;
ST, State or Province	– областен град, където е седалището по регистрация на титуляра или постоянен адрес на автора;
L, Location	– населено място, където е седалището по регистрация на титуляра или постоянен адрес на автора;
O, Organization	– името на титуляра, който се представлява от автора идентифициран в CommonName;
OU, Organization Unit	– името на организационната единица на титуляра, която представлява автора, идентифициран в CommonName;
CN, Common Name	– името на титуляра/автора или името на автора, който представлява титуляра;
T, Title	– позиция или функция на автора в организацията на титуляра;
UID, Unique Identifier	– за гарантиране посредством това поле, уникалността на удостоверението;
Street	– адрес на титуляра;
E, emailAddress	адрес за електронна кореспонденция на титуляра/автора.

Distinguished Name на титуляра/автора се потвърждава от оператора на РО и одобрява от УО.

9.2 Правила за интерпретиране на различните именни форми

Интерпретацията на имената на полетата в КЕП, издадени от „СЕП България“ АД, е в съответствие с профилите на удостоверенията. При създаването и интерпретирането на различните Distinguished Name се прилагат общите правила.

9.3 Уникалност на имената

За да осигури уникалност на издадените КЕП, „СЕП България“ АД присвоява уникален сериен номер за всяко издадено удостоверение. Сериеният номер в комбинация с Distinguished Name на автора/титуляра, прецизно и по уникален начин го идентифицира.

„СЕП България“ АД гарантира уникалност на имената също така и за публичния регистър и директориите. По този начин се гарантира безпроблемна работа и се предпазват от подмяна на услугата, приложенията, ползващи структурата на имената на УО.

9.4 Запазена марка

„СЕП България“ АД съобразява своята дейност със Закона за авторското право и сродните му права. Лицата, желаещи включване в съдържанието на удостоверението запазено име или име на марка следва да докажат пред „СЕП България“ АД правата си върху тях. Например, това могат да бъдат имена на домейни в интернет.

10. Идентификация и автентификация при първоначална регистрация

Първоначална проверка на идентичността съответно на самоличността на титуляра и на автора се осъществява при регистрацията за ползване на удостоверителни услуги на „СЕП България“ АД.

Регистрацията на титуляра/автора се осъществява, когато авторът/титулярят подава искане за издаване на КЕП и не притежава валидно КЕП, издадено от „СЕП България“ АД.

Регистрацията включва процедури, които позволяват на ДУУ преди да издаде КЕП на автора да събере достоверни данни, идентифициращи получателя на КЕП.

Всеки титуляр/автор е обект на регистрационния процес само веднъж. След проверка на данните предоставени от титуляра, титуляра/автора се включват в регистъра на одобрените потребители на удостоверителни услуги на „СЕП България“ АД.

Всеки автор/титуляр желаещ ползването на удостоверителна услуга и искащ издаването на КЕП трябва да:

- Попълни регистрационна форма на интернет сайта на ДУУ или да изпрати/предостави данните необходими за издаване на КЕП;
- Предостави на РО изискваните за регистрация документи;
- Подпише договор;
- Заплати дължимата цена на услугата.

„СЕП България“ АД допуска, когато е приложимо, изпращането на данните за регистрация по сигурен канал(по куриер, чрез електронна поща или интернет сайт и др.).

Идентификацията и автентификацията на титуляра/автора при първоначална регистрация преди издаване на удостоверение за електронен подпис, изисква титулярът да бъде физически идентифициран от оператор РО. Идентификацията може да се осъществи пряко или непряко. При пряката идентификация авторът/титулярът посещава офис на РО или оператор РО посещава автора/титуляра. При непряката идентификация оператор РО използва документи и други средства, които дават същата степен на сигурност както при пряката идентификация.

11. Методи за доказване контрола над частния ключ

Ако лице контролира частния ключ, когато заявява издаване на КЕП, УО и/или РО трябва да се убедят, че предоставения 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 публичния ключ на автора съответства на частния ключ и се намира под неговия изключителен контрол.

Основната проверка се извършва като се подпише с електронен подпис от автора, искане за издаване на КЕП, подновяване на ключове/удостоверение или за прекратяване на удостоверение.

Частният ключ трябва да се генерира от клиентския криптомодул SSCD. Авторът може да контролира потребителския криптомодул по всяко време на генерация на ключовата двойка или модула(смайт/им картата) да се предаде на автора след генерацията на ключовата двойка. В този случай „СЕП България“ АД гарантира, че криптомодула и ключовете са предоставени по сигурен начин на автора, за който са предназначени. Клиентският криптомодул може да се предостави на автора и чрез титуляра. Титулярът е собственик на криптомодула.

12. Проверка на идентичността на юридически лица

РО изисква представянето на подходящи документи, които по категоричен начин и без никакво съмнение потвърждават идентичността на юридическото лице, което може да се впише, като титуляр в удостоверението и на физическото лице, което ще представлява юридическото и ще се впише като автор в удостоверението.

Юридическото лице – титуляр, може да подаде искането пряко чрез представляващия го или чрез упълномощено лице, като изрично посочи на кои лица - автори, иска да се издаде КЕП.

РО може да събере необходимите данни за идентификация сам, като използва публични регистри.

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

- Упълномощен представител на юридическото лице лично посети РО;
- Представител на РО посети седалището на юридическото лице посочено в искането;
- Оператор РО използва непряк метод даващ същата степен на сигурност на идентификацията както при пряка физическа идентификация.

Ако проверката е успешна, оператор на РО:

- Изпраща данните към УО;
- Регистрира всички документи и доказателства или данните получени от публични регистри използвани от оператора при проверката на идентичността на юридическото лице и представителя действащ от негово име.

Водят се записи за процеса по проверка на идентичността, които включват:

- РО извършил проверката;
- Представените документи и доказателства, фактите от тях и периода им на валидност;
- Дата и час на проверката;
- Самоличността на представителя на юридическото лице.

В случай, че лицето притежава КЕП издаден от „СЕП България“ АД то проверката може да се осъществи като се използват преди това подадени документи, ако данните съдържащи се в тях са актуални. В този случай, лицето декларира, че данните не са променени от момента на тяхната регистрация в системата.

13. Проверка самоличността на физически лица

От проверката на самоличността на физическото лице, трябва да стават ясни:

- Самоличността на физическото лице – автор, съответно титуляр;
- Съществуването на физическото лице – автор, съответно титуляр.

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

- Физическото лице лично посети РО;
- Представител на РО посети физическото лице посочено в искането;
- Оператор РО използва непряк метод даващ същата степен на сигурност на идентификацията както при пряка физическа идентификация.

Искането се подава от лицето, посочено като автор.

Ако проверката е успешна, упълномощен оператор на РО:

- Изпраща потвърдените данни към УО;
- Регистрира всички документи и доказателства или данните получени от публични регистри използвани от оператора при проверката на самоличността на физическото лице.

Водят се записи за процеса по проверка на самоличността, които включват:

- РО извършил проверката;
- Представените документи и доказателства, фактите от тях и периода им на валидност;
- Дата и час на проверката;
- Самоличността на представителя на юридическото лице.

В случай, че лицето притежава КЕП, издаден от „СЕП България“ АД, то проверката може да се осъществи като се използват преди това подадени документи, ако данните, съдържащи се в тях са актуални. В този случай, лицето декларира, че данните не са променени от момента на тяхната регистрация в системата.

14. Непроверена информация

За да може да реализира своята дейност като ДУУ, „СЕП България“ АД включва в съдържанието на издаваните удостоверения данни, които не са задължителни съгласно чл. 24 от ЗЕДЕП.

Информацията, която е извън обхвата на ЗЕДЕП е не потвърдена информация и не може да се провери от ДУУ чрез ползване на официални документи и/или публични регистри или по друг допустим от закона начин. Информация която се включва в удостоверението, но не се п

верява от ДУУ, може да бъде но не се ограничава само до:

- Електронен адрес за кореспонденция;
- Специфични за автора/титуляра идентификатори.

Непотвърдената информация се включва в съдържанието на удостоверението на база декларация от страна на подалия искане за регистрацията титуляр.

„СЕП България“ АД не носи никаква отговорност за включената непотвърдена информация в съдържанието на удостоверението, включително и при невъзможност от страна на титуляра/автора да ползват определени услуги.

15. Потвърждаване на представителството

„СЕП България“ АД при регистрацията и подаване на искане, проверява представителната власт на лицата упълномощени от титуляра, съответно автора, преди да предприеме действия по издаване и управление на удостоверения за електронен подпис. Представителството се проверява на база предоставени от титуляра/автора официални документи, от които е виден факта и обема на представителната власт.

„СЕП България“ АД може да събере необходимите данни от публично достъпни регистри.

„СЕП България“ АД вписва по подходящ начин в съдържанието на удостоверението основанието на овластяване на физическото лице – автор.

Детайлно описание на процедурата по проверка представителството на лице е представена в Идентификация и автентификация при подновяване или модификация на КЕП

Подновяване на ключова двойка или удостоверение, като и модификация на удостоверение може да се извърши само в случаите, в които титуляра/автора има валидно удостоверение за електронен подпис от „СЕП България“ АД.

Автентификацията на автора се осъществява чрез:

- Електронен подпис и съответен публичен ключ от валидно удостоверение;
- Име и парола и/или предварително договорен, между автора/титуляра и доставчика, код за управление;
- Пряко или непряко от оператор РО.

Приложими са и други начини за автентификация, които могат да се договорят между ДУУ и титуляра, при условие че се гарантира нивото на сигурност.

Може да се подновяват или модифицират само валидни удостоверения, които не са прекратени и информацията, съдържаща се в удостоверението не е променена.

16. Подновяване

Подновяване имаме тогава, когато се издава ново удостоверение за КЕП на база издадено преди това валидно удостоверение.

Подновяване на ключова двойка може да се осъществи от автор/титуляр. Новото удостоверение съдържа данните от предишното и нови ключова двойка, сериен номер и период на валидност.

Титулярът може да поднови удостоверение, което вече притежава, ако няма промяна в съдържанието на удостоверението. Проверката на титуляра/автора се осъществява чрез електронен подпис и съответен публичен ключ от валидното удостоверение. Издава се ново удостоверение, съдържащо данните от

представеното при идентификацията и автентификацията удостоверение и нова ключова двойка, сериен номер и период на валидност.

Може да се подновяват ключовете само на валидни удостоверения, които не са прекратени и информацията съдържаща се в удостоверението не е променена.

17. Модификация на удостоверение – (Update)

Модификацията на удостоверение може да се осъществи от титуляр/автор, който има издадено преди това валидно удостоверение за електронен подпис.

При модификация на удостоверение се издава ново на базата на съществуващо.

Проверката на титуляра/автора се осъществява чрез: електронен подпис и съответен публичен ключ от валидно удостоверение за електронен подпис, различно от модифицираното, пряко или непряко от оператор РО.

Издава се ново удостоверение, съдържащо данните за автора/титуляра от представеното при идентификацията и автентификацията. Има нов публичен ключ и сериен номер и се различава поне по едно поле от модифицираното.

Може да се модифицират само валидни удостоверения, които не са прекратени и информацията за титуляра, съдържаща се в удостоверението не е променена.

Допуска се модификация на полетата, свързани с името на автора и непотвърдена информация за титуляра. Изходното модифицирано удостоверение се прекратява.

18. Идентификация и автентификация при прекратяване

Искането за прекратяване може да се подаде по електронен път или в хартиена форма.

При електронно подаване на искане за прекратяване титуляра или от надлежно овластен автор се автентифицира чрез своя електронен подпис или предварително договорен, между него и доставчика, код за управление.

Ако авторът е загубил контрол върху частния си ключ подаденото искане се проверява от оператор на РО, като проверката не може да бъде в електронна форма.

Може да се подава искане на прекратяване на повече от едно удостоверение.

Идентификацията и автентификацията се осъществява при условията на точка "Идентификация и автентификация при първоначална регистрация".

19. Идентификация и автентификация при спиране и възобновяване

19.1 Спиране на удостоверение

Искането за спиране може да се подаде от:

- Титуляра или упълномощен автор на удостоверението за КЕП;
- Комисията за регулиране на съобщенията;
- Други държавни органи, определени със закон;
- ДУУ.

Искането за спиране може да се подаде по електронен път или в хартиена форма.

При електронно подаване на искане за спиране, подалия искането може да се автентифицира чрез своя електронен подпис или предварително договорен, между него и доставчика, код за управление.

Оператор РО проверява всички искания за спиране постъпили в хартиена форма.

ДУУ не извършва идентификацията и автентификацията на подалия искането за спиране на удостоверение.

ДУУ незабавно уведомява по подходящ начин титуляра/автора за спирането на удостоверение.

Максималният срок, през който удостоверение може да бъде спряно, е до 48 часа от спирането му.

19.2 Възобновяване на удостоверение

Искането за възобновяване може да се подаде от:

- Титуляра/автора на удостоверението за електронен подпис, като декларира, че е узнал причината за спирането и искането за възобновяване е направено вследствие на узнаването;
- Комисията за регулиране на съобщенията за удостоверенията, за които е наредила спиране;
- Други държавни органи за удостоверенията, за които са наредили спиране.

Искането за възобновяване може да се подаде по електронен път или в хартиена форма.

При електронно подаване на искане за възобновяване, подалият искането се автентифицира чрез своя електронен подпис или предварително договорен, между него и доставчика, код за управление.

Идентификацията и автентификацията на подалия искането, се осъществява при условията на „Идентификация и автентификация при първоначална регистрация”.

ДУУ възобновява удостоверението след изтичане на максималният срок, през който удостоверение може да бъде спряно.

20. Жизнен цикъл на удостоверенията за КЕП

Разглеждат се основните процедури свързани с издаване и управление на удостоверения за електронен подпис.

„СЕП България” АД предоставя следните удостоверителни услуги: първоначална регистрация, издаване на КЕП, подновяване на КЕП, модификация на КЕП, спиране и възобновяване на КЕП и прекратяване на КЕП.

Всяка процедура стартира с подаване на искане от титуляра или овластен автор. Според подаденото искане ДУУ взема съответното решение относно предоставяне или отхвърляне на исканата услуга. Подаденото искане трябва да съдържа данни за исканата услуга и необходимите данни за идентификация на титуляра/автора.

Ако подаденото искане съдържа публичен ключ, ключа следва да е генериран по такъв начин, че да е криптографски свързан с другите данни от искането.

Искането може да съдържа и заявка за генериране на ключова двойка от ДУУ от името на титуляра/автора. След генерирането ключовата двойка се предоставя по сигурен начин на титуляра/автора.

20.1 Подаване на искане

За да се получи удостоверителна услуга от „СЕП България” АД то потребителите на удостоверителни услуги трябва да я заявят пред ДУУ или регистриращ орган на ДУУ.

Исканията за удостоверителни услуги се подават до „СЕП България” АД чрез:

- Използване на On-line форма на интернет страницата на ДУУ;
- Оператор РО.

Исканията се подават в електронна или хартиена форма. Хартиената форма изисква да се попълнят необходимите формуляри и се предоставят на оператор РО. Електронната форма изисква да се попълнят формулярите в електронен вид и да се подпишат с електронен подпис, след което се предоставят на ДУУ. За подаване на искания по електронен път чрез интернет се използват мрежови протоколи като HTTPS, S/MIME или TCP/IP. Могат да се подават искания за:

- Първоначална регистрация на юридическо или физическо лице като потребител на удостоверителните услуги на „СЕП България” АД. Едновременно с регистрацията може да се поиска и ползване на удостоверителна услуга;
- За издаване на КЕП;
- Подновяване на КЕП;
- Модификация на КЕП;

- Спиране на КЕП;
- Възобновяване на КЕП;
- Прекратяване на КЕП.

Подателите на исканията се идентифицират и автентифицират чрез:

- Електронен подпис и публичен ключ от валидно удостоверение за електронен подпис;
- Име, парола и/или код за управление получен при първоначалната регистрация или при получаване на удостоверителна услуга;
- Физическо представяне и предоставяне на идентифициращи документи и саморъчен подпис при подаване на искането в писмена форма чрез оператор РО;
- Изпращане на нотариално заверени подписи на съответните документи.

Начина на идентификация и автентификация на заявителя зависи от подаденото искане, обстоятелствата свързани с искането и наличието на предварителна регистрация.

Операторът на РО може да:

- Представява ДУУ пред титуляра/автора;
- Подаде от името на титуляра/автора всяко искане за удостоверителна услуга;
- Проверява предоставените данни и документи съпровождащи искането и потвърждава подаденото искане.

„СЕП България” АД издава КЕП след първоначална регистрация и постъпване на искане за издаване на КЕП, подновяване на КЕП или модификация на КЕП.

При постъпване на on-line искане за издаване на КЕП, е възможно издаването на допълнителни КЕП на предварително идентифициран титуляр.

20.1.1. Искане за първоначална регистрация

Искането за регистрация се подава от титуляра или негов пълномощник. On-line или чрез оператор РО и трябва да съдържа следната информация:

- Пълното име на титуляра потребител на удостоверителна услуга;
- Идентификатори: ЕГН, ЛНЧ, ЕИК или БУЛСТАТ;
- Адрес на титуляра;
- Име за регистрация и парола;
- Електронен адрес за кореспонденция;
- Допълнителни данни и/или документи необходими за получаване на удостоверителна услуга.

В зависимост от титуляра, някоя от посочената информация може да не бъде включена в искането на първоначална регистрация.

Предоставената информация се съхранява в регистъра с потребители на удостоверителни услуги и се ползва при подаване искания за удостоверителни услуги към ДУУ.

20.1.2. Искане за издаване на удостоверение за КЕП

Искането за издаване на удостоверение за електронен подпис се подава от титуляра или автора. Когато титулярът е юридическо лице, искането изхожда от представляващия юридическото лице или от негов изрично упълномощен представител. Възможни са два начина на подаване на искането: on-line или чрез оператор РО. Информацията, която се съдържа в искането, зависи от типа искано удостоверение за КЕП, броят автори и включва:

- Пълното име на титуляра;
- Име или имената на авторите – представители на титуляра;
- Представителство на авторите по отношение на титуляра;
- Идентификатори: ЕГН, ЛНЧ, ЕИК ;
- Адрес на седалище на титуляра;

- Адреси на авторите;
- Тип искано удостоверение за КЕП;
- Публичен ключ;
- Име и парола зададени при първоначална регистрация;
- Електронен адрес за кореспонденция;
- Допълнителни данни и/или документи необходими за получаване на удостоверителна услуга.

В зависимост от искания тип КЕП, някои от посочената информация може да не бъде включена в искането за издаване на КЕП.

Необходимите данни и документи са посочени на интернет адрес <http://e-sign.sep.bg>.

При налична регистрация и валидно КЕП на титуляра, част или всички данни могат да се автентифицират чрез електронен подпис за останалите данни, титуляра представя оригинални документи или заверени копия пред оператор РО.

Оператор РО проверява:

- Представените данни и придружаващи документи;
- Идентичността съответно самоличността на титуляра/автора;

Потвърждава данните от искането за издаване на КЕП, след което предава искането на УО на ДУУ за обработка.

20.1.3. Искане за подновяване или модификация на КЕП

Искането за подновяване или модифициране на удостоверение за КЕП се подава от автора/титуляра или негов пълномощник.

Възможни са два начина на подаване на искането: on-line или чрез оператор РО.

Информацията, която се съдържа в искането е следната:

- Distinguished Name на автора/титуляра подал искането;
- Distinguished Name на КЕП, за което е подадени искането;
- Тип на КЕП, за което е подадено искането;
- Нов публичен ключ или искане за генерация на такъв от ДУУ;
- Допълнителни данни и/или документи необходими за получаване на удостоверителна услуга.

В зависимост от исканата услуга, някои от посочената информация може да не бъде включена в искането за подновяване или модифициране на удостоверение за електронен подпис.

Необходимите данни и документи са посочени на интернет адрес <http://e-sign.sep.bg>.

При налична регистрация и валидно КЕП на автора/титуляра, част или всички данните могат да се автентифицират чрез електронен подпис за останалите данни, авторът/титулярът представя оригинални документи или заверени копия пред оператор РО.

Оператор РО проверява:

- Представените данни и придружаващи документи;
- Идентичността съответно самоличността на титуляра/автора.

Потвърждава данните от искането за подновяване или модифициране на КЕП, след което предава искането на УО на ДУУ за последваща обработка.

20.1.4. Искане на прекратяване или спиране

Искането за прекратяване или спиране на удостоверение за КЕП се подава от автора/титуляра или пълномощник.

Възможни са два начина на подаване на искането: on-line или чрез оператор РО.

Информацията, която се съдържа в искането е следната:

- Distinguished Name на автора/титуляра подал искането;

- Списък с удостоверенията, които да се прекратят или спрат, съдържащ сериен номер и причина за прекратяване;
- Допълнителни данни и/или документи необходими за получаване на удостоверителна услуга.

В зависимост от исканата услуга, някои от посочената информация може да не бъде включена в искането за прекратяване или спиране на удостоверение за електронен подпис.

Необходимите данни и документи са посочени на интернет адрес <http://e-sign.sep.bg>.

При налична регистрация и валидно КЕП на автора/титуляра, част или всички данни могат да се автентифицират чрез електронен подпис за останалите данни, автора/титуляра представя оригинални документи или заверени копия пред оператор РО.

Оператор РО проверява:

- Представените данни и придружаващи документи;
- Идентичността съответно самоличността на автора/титуляра при прекратяване на удостоверение за КЕП.

Потвърждава данните от искането за прекратяване или спиране на КЕП, след което предава искането на УО на ДУУ за последваща обработка.

20.1.5. Искане за възобновяване

Искането за възобновяване на удостоверение за електронен подпис се подава от автора/титуляра или негов пълномощник.

Авторът/Титулярът на удостоверението за КЕП, декларира, че е узнал причината за спирането и искането за възобновяване е направено вследствие на узнаването.

Възможни са два начина на подаване на искането: on-line или чрез оператор РО.

Информацията, която се съдържа в искането следната:

- Distinguished Name на автора/титуляра подал искането;
- Декларация, че авторът/титулярът е узнал причината за спирането и искането за възобновяване е направено вследствие на узнаването;
- Сериен номер на удостоверението, което да се възобнови;
- Допълнителни данни и/или документи необходими за получаване на удостоверителна услуга.

В зависимост от исканата услуга, някои от посочената информация може да не бъде включена в искането за възобновяване на удостоверение за електронен подпис.

Необходимите данни и документи са посочени на интернет адрес <http://e-sign.sep.bg>.

При наличие на валидно КЕП подалия искането може да се автентифицира чрез електронен подпис в противен случай, искането се подава писмено пред оператор РО. При необходимост се предоставят допълнителни документи пред оператор РО.

Оператор РО проверява:

- Представените данни и придружаващи документи;
- Идентичността съответно самоличността на титуляра/автора при възобновяване на удостоверение за електронен подпис.

Потвърждава данните от искането за възобновяване на КЕП, след което предава искането на УО на ДУУ за последваща обработка.

20.2 Обработка на подадените искания

„СЕП България“ АД приема индивидуални искания и искания за повече от едно лице. Исканията могат да се подадат On-line или Off-Line.

20.2.1. On-line искания

On-line исканията се приемат през портала на ДУУ на адрес <https://e-sign.sep.bg>. Авторът/Титулярят или негов пълномощник, посещава портала на ДУУ. Попълва съответната форма или форми като следва и

спазва указанията дадени на всяка стъпка от процеса по подаване на искане за удостоверяваща услуга. Ако е необходимо в зависимост от следващата процедура се посочва РО пред който ще се представят допълнителните данни и документи за получаване на удостоверяващата услуга.

Искането се обработва в автоматичен режим ако е достатъчна проверка само в базата данни на ДУУ.

Искането се обработва от оператор РО, когато е необходимо да се провери и сравнят данните от подаденото искане с данни от други източници и допълнително представените данни и документи за получаване на удостоверяващата услуга.

20.2.2. Off-Line искания

Off-Line искания имаме тогава, когато се изисква титуляра или негов пълномощник, ако титулярът е юридическо лице, да се представи лично пред оператор РО. Off-Line искане имаме и когато допълнителните данни и документи за получаване на удостоверяващата услуга се изпратят по сигурен начин до РО на ДУУ. Проверката на документите и лицата се осъществява според правилата в този Наръчник.

Когато титуляр, юридическо лице пряко или чрез представител, подава искане за удостоверяваща услуга за повече от един автор, то данните за всичките автори се проверяват и обработват заедно.

20.2.3. Обработка на исканията от Регистриращ орган

Всяко подадено искане към РО, независимо от това дали е on-line или off-Line, се обработва по следния начин:

- Операторът получава искането в електронна форма или на хартия;
- Операторът проверява данните посочени в искането и проверява за доказателства относно държането на частен ключ;
- Данните се сверяват с данни от публични регистри и/или допълнително предоставени документи;
- При успешна проверка, операторът одобрява искането като го подписва. При грешни и неверни данни искането се отхвърля;
- Одобреното искане се подава към УО;
- РО може да провери и други данни ако е необходимо;
- Води записи за процедурата в базата данни и системните журнали.

Комплектова и изпраща за съхранение хартиените документи до УО, след приключване на процедурата.

20.2.4. Обработка на исканията от Удостоверяващ орган

УО преглежда одобрените от РО искания и ги предвижда за следваща обработка. Исканията трябва да са потвърдени/подписани от оператор на РО. Ако исканията не са потвърдени или е необходима проверка осъществявана от УО, то УО:

- Свързва данните от искането с наличните данни за регистриран преди това титуляра от своята база данни;
- Проверява автентичността на искането (електронен подпис или име, парола и/или код за управление);
- Извършва формална проверка на искането (синтаксис и съдържание);
- Проверява дали титуляра/автора има право да подава искания за конкретния тип удостоверение;
- Води записи за процедурата в базата данни и системните журнали.

Ако искането е одобрено, УО проверява дали одобрението е от упълномощен РО. Ако е така то следващите стъпки са аналогични на гореописаните.

20.3 Издаване на удостоверение за електронен подпис

При получаване на одобрено искане за издаване, УО издава удостоверение за КЕП. Удостоверението се смята за валидно от момента на публикуване в публичния електронен регистър на ДУУ. Периодът на валидност на издаденото удостоверение зависи от неговия тип и е както е посочено в таблицата:

тип удостоверение	период на валидност
SEP Qualified Private	3 години
SEP Qualified Organization	3 години
SEP Qualified Profession	3 години

Всички удостоверения са издават on-line. Процедурата по издаване е следната:

- Обработеното искане се подава към сървъра на УО за издаване на удостоверения;
- Ако искането е и за генериране на ключова двойка, сървъра на УО използва хардуерен крипто-модул;
- Алгоритмите за проверка на КЕП съставляват логическо цяло с алгоритмите за създаването им. Алгоритмите и параметрите за квалифициран електронен подпис отговарят на съответни изисквания по отношение на хеш-функциите и асиметричните алгоритми съгласно изискванията на НИАСПКЕП;
- Ако процедурата е успешна, сървъра генерира удостоверението и го подписва като използва хардуерен криптомодул. Генерираното удостоверение се съхранява в базата данни на УО;
- УО подготвя отговор, съдържащ генерираното удостоверение за КЕП и го представя on-line или чрез РО.

„СЕП България“ АД използва някои от следните методи, за да информира автора/титуляра за генерирането на удостоверението:

- Информацията се предоставя като част от следваната on-line процедура по издаване на КЕП;
- Изпращане на поща, електронна поща или sms до автора/титуляра, на предоставен от него адрес, информация, позволяваща на автора/титуляра да получи КЕП.

„СЕП България“ АД публикува удостоверението в публичната си директория.

Публикуването на КЕП 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.

УО полага всички усилия, за да гарантира, че от момента на получаване на искането за регистрация и издаване, подновяване на удостоверение или ключ, искането ще се разгледа и ще се издаде ново удостоверение в рамките на период до 7 дни.

Периодът зависи от пълнотата на предоставените данни в искането и от изпълнението на възможните допълнителни изисквания на ОУ/РО. Това са искания зависещи от характера на крайния получател и типа получавани от него КЕП и са свързани с необходимостта от уточняване на данните вписани в КЕП. В този случай е възможно да се увеличи периода на изчакване над посочената по-горе стойност.

20.4 Отказ за издаване на КЕП

Отказ за издаване може да се получи, когато:

- Авторът/титулярът не може да докаже своите права по отношение на поисканото Distinguished Name;
- При съмнения или несъмнени доказателства, че титулярът/авторът е използвал неверни данни и/или неистински или подправен документ;
- Ако се създават умишлени трудности в работата на „СЕП България“ АД;
- Достигнат е предварително договорен лимит за брой на издадени КЕП;
- По други причини.

Информацията за отказа за издаване на КЕП и причините свързани с този отказ се изпраща на заявителя. Лицето, на което е отказано да му бъде издадено КЕП може да подаде жалба в 3 дневен срок, както е посочено в раздел „Разрешаване на спорове“.

20.5 Приемане на удостоверение за електронен подпис

При некоректно попълнена или невярна информация в съдържанието на удостоверението, то не може да се приеме. Операторът РО или авторът/титулярът коригират данните и ги подават за нова генерация.

След издаване, удостоверението се получава от автора/титуляра. Авторът трябва да провери за съответствието на публичния ключ от удостоверението с частния ключ, който държи. Ако публичния ключ от удостоверението не съответства на частния ключ, държан от автора, то издаденото удостоверение се прекратява. Прекратяването на удостоверението, в този случай, има смисъла на отказ на автора/титуляра да приеме издаденото удостоверение.

Удостоверението се смята за прието ако в рамките на 3 (три) дни след получаването на удостоверението не е постъпило искане за прекратяване.

При приемане на удостоверението, авторът/титулярът се съгласяват, че преди да използват КЕП за криптографски операции са се запознали с процедурите по издаване на КЕП, описани в този документ.

С приемането на удостоверението авторът/титулярът приемат изискванията и правилата на „Политиката по предоставяне на удостоверителни услуги“ и „Практиката при предоставяне на удостоверителни услуги“ и са съгласни с изявленията направени в „Договора за предоставяне на удостоверителни услуги“ сключен между тях и „СЕП България“ АД.

20.6 Използване на удостоверението и ключовата двойка

Титулярът/авторът, могат да използват частния ключ и удостоверението за електронен подпис:

- Съобразно тяхното предназначение, както е посочено в този документ и в съответствие със съдържанието на КЕП (полета keyUsage, EnhancedKeyUsage);
- Съобразно договора за предоставяне на удостоверителни услуги сключен между тях и „СЕП България“ АД;
- Само през време на периода на валидност, освен случаите на приложение на КЕП за проверка на електронен подпис или за декриптиране на получени съобщения;
- До момента на прекратяване на удостоверението;
- Когато удостоверението е спряно и титуляра/авторът е използвал частния ключ за електронен подпис, то подписите ще се смятат за валидни само ако удостоверението бъде възобновено.

Доверяващите се страни могат да ползват публичния ключ и удостоверението за електронен подпис:

- Съобразно тяхното предназначение, както е посочено в този документ и в съответствие със съдържанието на КЕП. (полета keyUsage, EnhancedKeyUsage);
- Само за проверка статуса на издадено удостоверение за електронен подпис 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 може да ползва публичния ключ от това удостоверение.

20.7 Подновяване

Подновяване на ключова двойка или удостоверение, може да се извърши само в случаите, в които титуляра/автора има издадено преди това валидно удостоверение за електронен подпис от „СЕП България“ АД.

При подновяване „СЕП България“ АД препоръчва винаги да се генерира нова ключова двойка за удостоверението за електронен подпис.

Подновяване може да се осъществи от автор/титulary, който има издадено преди това валидно удостоверение за електронен подпис. Новото удостоверение съдържа: данните от подновяването удостоверение и евентуално нова ключова двойка, сериен номер и период на валидност.

Всички удостоверения могат да се подновяват on-line. Процедурата по подновяване е следната:

- Обработеното искане се подава към сървъра на УО за подновяване на удостоверения;
- Искането може да съдържа новата ключова двойка или искане за генериране на ключова двойка;
- УО използва клиентския хардуерен криптомодул за генерация на ключова двойка като съответствието между ключовата двойка се проверява;
- Ако процедурата е успешна сървъра генерира удостоверението и го подписва като използва хардуерен криптомодул;
- Генерираното удостоверение се съхранява в базата данни на удостоверяващия орган;
- УО подготвя отговор, съдържащ генерираното удостоверение за КЕП и го представя on-line или чрез РО.

„СЕП България“ АД използва следните методи, за да информира титуляра/автора за генерирането на подновеното удостоверение:

Информацията се предоставя като част от следваната on-line процедура по подновяване на КЕП;

Изпращане на поща, електронна поща или sms до автора/титulary.

„СЕП България“ АД публикува удостоверението в публичната си директория. Публикуването на КЕП е равносилно на уведомяване на доверяващите се страни за това, че е издадено ново удостоверение на лицето вписано в него и това лице може да се идентифицира чрез този КЕП.

„СЕП България“ АД винаги информира автора/титulary, минимум 30 дни предварително, относно предстоящото изтичане на периода на валидност на удостоверение за КЕП.

20.8 Модификация на удостоверение

Модификация на удостоверение имаме, когато подменяме валидно удостоверение, което се използва, с ново удостоверение, което се различава по съдържанието на поне едно поле от подменяното.

Може да се модифицират само валидни удостоверения, които не са прекратени и информацията за автора/титulary съдържаща се в удостоверението не е променена.

Допуска се модификация на полетата свързани с името на автора и непотвърдена информация за титуляра. Изходното модифицирано удостоверение се прекратява.

Издава се ново удостоверение, съдържащо данните за автора/титulary от представеното при идентификацията и автентификацията. Има нов публичен ключ и сериен номер и се различава поне по едно поле от модифицираното. Това може да е ново съдържание или ново поле.

Процедурата по модифициране е следната:

- Обработеното искане се подава към сървъра на УО за издаване на ново, удостоверение заедно с променени данни;
- Искането може да съдържа новата ключова двойка или искане за генериране на ключова двойка;
- УО използва клиентския хардуерен криптомодул за генерация на ключова двойка като съответствието между ключовата двойка се проверява;
- Ако процедурата е успешна, сървъра генерира удостоверението и го подписва като използва хардуерен криптомодул;
- Генерираното удостоверение се съхранява в базата данни на удостоверяващия орган;
- УО подготвя отговор съдържащ генерираното КЕП и го представя On-line или чрез РО, на титуляра/автора за одобрение.

„СЕП България“ АД използва следните методи, за да информира автора/титulary за генерирането на модифицираното удостоверение:

Информацията се предоставя като част от следваната On-line процедура по модифициране на КЕП; Изпращане на поща, електронна поща или sms до автора/титуляра, на предоставен от него адрес.

„СЕП България“ АД публикува удостоверението в публичната си директория. Публикуването на КЕП е равносилно на уведомяване на доверяващите се страни за това, че е издадено ново удостоверение на лицето, вписано в него и това лице може да се идентифицира чрез този КЕП.

Ако процедурата по модификация е успешна, модифицираното удостоверение 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 частния ключ, съответстващ на публичния от замененото удостоверение не е бил компрометиран.

20.9 Прекратяване на удостоверение

Прекратяване е действие, при което удостоверението за електронен подпис се включва в Списъка с прекратени удостоверения(CRL). От момента на включване вече не може да се потвърждават електронни подписи с това удостоверение.

„СЕП България“ АД уведомява титуляра/автора при прекратяване на удостоверението.

20.9.1 Обстоятелства, при които се допуска прекратяване

Основната причина за прекратяване на КЕП е загубата на контрол или съмнение за загуба на контрол, върху частния ключ от лицето, вписано като автор в удостоверението.

Удостоверение за електронен подпис може да се прекрати:

- Ако информацията, съдържаща се в удостоверението, се промени;
- Ако частния ключ, съответстващ на публичния от удостоверението или носителя използван за съхранението му, са компрометирани или има съмнение за компрометиране;
- По искане на титуляра или автора за прекратяване на удостоверението и/или за прекратяване на договорните отношения със „СЕП България“ АД;
- По искане на посочени в нормативен акт органи;
- Прекратяване на представителната власт на физическото лице спрямо юридическото лице, вписано в съдържанието на КЕП;
- Прекратяване на юридическото лице на титуляра;
- Смърт или поставяне под запрещение на физическото лице – автор;
- Установяване, че КЕП е издаден въз основа на неверни данни;
- От „СЕП България“ АД при несъгласие или неизпълнение на задълженията на титуляра/автора по тази практика;
- При забавяне или не плащане на определените такси за ползване на удостоверителни услуги;
- При компрометиране на частния ключ на ДУУ;
- При прекратяване на дейността на ДУУ. В този случай се прекратяват всички издадени удостоверения и удостоверенията на ДУУ;
- Когато авторът не е върнал предоставената му за ползване от титуляра криптографска карта при отпадане на основанието за овластяване. В този случай КЕП се прекратява по искане на титуляра;
- Други обстоятелства, възпрепятстващи титуляра/автора от изпълнение на задълженията му според тази практика;
- Промени в регулаторната рамка или юридическия статут на титуляра/автора.

Искането за прекратяване може да се подаде от титуляра/автора като се обърнат към РО. Подаваният искането установява пряк физически контакт с оператора на РО. Искането се потвърждава от оператор РО. Възможно е да се подаде в електронна или хартиена форма.

Искането за прекратяване може да се подаде директно до УО. В този случай искането се автентифицира чрез електронен подпис на титуляра.

Искането за прекратяване съдържа информация, която позволява по категоричен начин да се идентифицира титуляра/автора „Идентификация и автентификация при прекратяване”, от РО или от УО.

20.9.2 Кой може да иска прекратяване на удостоверение

Следните участници в удостоверителния процес, могат да подадат искане за прекратяване на КЕП:

- Титулярът/авторът или негов представител;
- Оператор РО, който може да иска прекратяване на КЕП от името на титуляра/автора или от свое име, ако информацията, с която разполага удовлетворява изискванията за прекратяване на КЕП;
- По искане на посочени в нормативен акт органи;
- Упълномощен представител на УО.

Когато страната, искаща прекратяване на удостоверението не е собственик на удостоверението оператор РО или УО трябва да:

- Провери дали подалия искането е оторизиран да поиска прекратяване (дали действа от името на титуляра/автора като техен представител);
- Да изпрати известие до титуляра/автора за прекратяването или за началото на процеса по прекратяване.

Всяко искане може да бъде изпратено:

- Директно до УО по електронен път с или без потвърждение от оператор РО;
- Пряко или непряко с посредничеството на оператор РО до УО, като не е в електронна форма – хартиен документ, факс, телефонно обаждане.

20.9.3 Процедура за прекратяване на удостоверение

Искането за прекратяване се обработва по следния начин:

- Първи метод – подадено искане за прекратяване, до УО, по електронен път. Искането е подписано с валиден частен ключ или е оторизирано чрез парола и/или код за управление. Искането може да се инициира изключително по инициатива на титуляра/автора. Титулярът/авторът може да поиска прекратяване на повече от едно удостоверение;
- Втори метод – подадено искане за прекратяване, до УО, по електронен път. Искането е потвърдено от оператор РО. Този метод е приложим, когато титуляра/авторът е изгубил своя частен ключ, ПИН или парола, или при кражба на частен ключ. Също така е приложим и при искане за прекратяване подадено от оператор РО, който е преценил, че има достатъчно основания за прекратяване на КЕП;
- Трети метод – основава се на подаване на искане, което не е в електронна форма, като хартиен документ, факс, телефонно обаждане.

Във всички случаи УО, след успешна проверка на искането за прекратяване, прекратява удостоверението. Информацията за прекратеното на удостоверение се публикува в Списък с прекратени удостоверения на УО, издал удостоверението.

„СЕП България” АД изпраща потвърждение за прекратяване на удостоверението или решение за отказ на искането за прекратяване заедно с причината за отказа, до подалия искането за прекратяване.

Процедурата за прекратяване на удостоверение за КЕП е както следва:

- При получаване на искане за прекратяване, УО го одобрява, ако искането е подадено по електронен път като УО проверява верността на удостоверението, чието прекратяване се иска и верността на електронните данни приложени към искането, ако е подадено от РО. При подаване на искането на хартия се изисква проверка на подалия искането. Проверката може да се извърши по телефона, чрез факс, или при посещение на РО от пълномощен представител или обратно;
- Ако проверката е успешна, УО публикува информация за прекратяването на удостоверението в CRL заедно с информация относно причината за прекратяване;

- УО изпраща потвърждение за прекратяване на удостоверението или решение за отказ на искането за прекратяване заедно с причината за отказа, до подалия искането за прекратяване;
- Допълнително, ако искането не е подадено от титуляра/автора на удостоверението, УО трябва да уведоми титуляра/автора за прекратяването или иницирирането на процес по прекратяване.

21. Необходимост от проверка статуса на удостоверението

Доверяващите се страни, при получаване на документ подписан с електронен подпис, са длъжни да проверят дали публичния ключ от удостоверението, който съответства на частния ключ на автора използван при електронния подпис, не е публикуван в CRL. Доверяващата се страна е длъжна да направи проверката в актуалния текущ CRL или по OCSP.

Ако проверяваното удостоверение за електронен подпис се намира в CRL, доверяващата се страна е длъжна да отхвърли документа, асоцииран с удостоверението, ако причината за прекратяване е една от следващите:

unspecified	– не е посочена причина за включване на удостоверението в CRL;
keyCompromise	– нарушена е сигурността на частния ключ;
caCompromised	– нарушена е сигурността на ключа на УО;
cessationOfOperation	– причината, поради която е издадено удостоверението вече не съществува;
certificateHold	– удостоверението е спряно.
affiliationChanged	– модифицирани са данни на удостоверението;
superseded	– удостоверението включено в CRL е заменено с друго удостоверение;

Крайното решение относно валидността на удостоверението се взема от доверяващата се страна.

22. Периодичност на публикуване на CRL

Всеки УО, който е част от йерархията на „СЕП България“ АД издава свой отделен Списък с прекратените удостоверения.

Списък с прекратените удостоверения, на оперативния УО, се обновява най-малко веднъж на 3 (три) часа и при всяко настъпило събитие. Списъка с прекратените удостоверения на базовия УО, се обновява най-малко 1 (един) път годишно и при всяко настъпило събитие.

Списък с прекратените удостоверения се публикува в публичния регистър на ДУУ.

22.1 Спиране и възобновяване на удостоверение

22.1.1. Обстоятелства при спиране на удостоверение

Спиране е действие, при което удостоверението за КЕП се включва временно в Списъка с прекратени удостоверения. За времето на престой на удостоверението в CRL, с него не може да се потвърждават електронни подписи. След изваждане на удостоверението от CRL то отново може да се използва за потвърждаване на електронни подписи.

Действието на удостоверенията, издадени от „СЕП България“ АД, може да бъде спряно при наличие на съответните основания, за необходимият според обстоятелствата срок, но за не повече от 48 часа.

За периода на временно спиране на удостоверението, същото се счита за невалидно.

„СЕП България“ АД уведомява титуляра/автора при спиране на удостоверението.

22.1.2. Обстоятелства при възобновяване на удостоверение

Възобновяване е действие, при което титулярът/авторът, след като е бил уведомен, че удостоверението му е било включено в CRL, е поискал изваждането на удостоверението от този списък.

Действието на удостоверението се възобновява с изтичане на срока на спиране, при отпадане на основанието за спиране или по искане на титуляра, след като „СЕП България“ АД, се увери, че той е узнал причината за спирането и искането за възобновяване е направено вследствие на узнаването. УО възобновява действието на удостоверението, като го изважда от списъка с прекратени удостоверения.

От момента на възобновяване на действието на удостоверението, същото се счита за валидно.

Ако по време на спиране на удостоверение са били положени електронни подписи, то те се смятат за валидни само след възобновяване на съответното удостоверение.

22.1.3. Кой може да иска спиране и възобновяване на удостоверение

23.1.3.1. Основания за спиране на удостоверение

„СЕП България“ АД спира действието на удостоверение за електронен подпис при постъпване на искане от страна на:

- Комисията за регулиране на съобщенията;
- Титуляра/автора;
- 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.

23.1.3.2. Основания за възобновяване на удостоверение

„СЕП България“ АД възобновява действието на удостоверение за електронен подпис, при:

- Изтичане на срока на спиране на действието на удостоверението;
- Разпореждане на КРС – когато причината за спирането на действието е разпореждане на КРС;
- Постъпване на искане за възобновяване от страна на титуляра, след като „СЕП България“ АД, съответно КРС се увери, че титулярът/авторът е узнал причината за спирането, както и че искането за възобновяване е направено вследствие на узнаването;
- Отпадане на основанията за спиране.

22.2 Процедура по спиране и възобновяване на удостоверение

22.2.1. Процедура по спиране на действието на удостоверение

„СЕП България“ АД спира удостоверение за електронен подпис след настъпване на някое от основанията посочени по-горе по следния начин:

- При получаване на искане за спиране, УО го одобрява, ако искането е подадено по електронен път, като УО проверява верността на удостоверението, чието прекратяване се иска и верността на електронните данни приложени към искането, ако е подадено от РО. При подаване на искането на хартия може да се провери самоличността или представителната власт на подалия искането. Проверката може да се извърши по телефона, чрез факс, или при посещение на РО от пълномощен представител или обратно;
- УО на „СЕП България“ АД спира действието на удостоверението, като го включва в списъка със спрените и прекратените удостоверения с причина за прекратяване hold;
- УО на „СЕП България“ АД незабавно уведомява титуляра/автора за спирането на действието на удостоверението.

22.2.2. Процедура за възобновяване на действието на удостоверение

„СЕП България“ АД възобновява удостоверение за електронен подпис след настъпване на някое от основанията посочени по-горе, по следния начин:

- След изтичане на срока на спиране на действието на удостоверението – след изтичане на 48 часа от момента на спиране на действието на удостоверението, неговото действие се възобно-

вява автоматично от УО на „СЕП България“ АД, ако до този момент не е получено искане за прекратяване;

- По разпореждане на КРС – „СЕП България“ АД получава разпореждането на КРС за възобновяване на действието на удостоверението. УО на „СЕП България“ АД възобновява действието на удостоверението.
- По искане от страна на титуляра/автора – след като „СЕП България“ АД, съответно КРС се увери, че титулярът/авторът е узнал причината за спирането и искането за възобновяване е направено вследствие на узнаването. Процедурата в този случай е следната:
 - Искането може да се подаде по електронен път или на хартия, от титуляра/автора и негов пълномощник;
 - Подалия искането за възобновяване се автентифицира;
 - Подалия искането декларира, че е узнал причината за спирането и искането за възобновяване е направено вследствие на узнаването;
 - При получаване на искане за възобновяване, УО го одобрява, ако искането е подадено по електронен път, като УО проверява верността на удостоверението, чието прекратяване се иска и верността на електронните данни приложени към искането, ако е подадено от РО;
 - Ако проверката е успешна, УО възобновява удостоверението;
 - УО изпраща потвърждение за възобновяване на удостоверението до титуляра;
 - От момента, в който Удостоверяващият орган е възобновил действието на удостоверението, същото се счита за валидно. Ако в периода на спиране на удостоверението е постъпило искане за прекратяване, то „СЕП България“ АД прекратява удостоверението за КЕП в съответствие с тази практика.

22.3 Ограничения на периода на спиране

Максималният срок за спиране на удостоверение за електронен подпис е 48 часа, след което, ако не е постъпило искане за прекратяване, УО го възобновява.

22.4 On-line проверка на валидността на удостоверения

„СЕП България“ АД предоставя възможност за On-line проверка статуса на издадените удостоверения. Тази услуга се предоставя чрез OCSP протокол, описан в RFC 2560. Чрез използването на OCSP е възможно да се получава по-често и по-навременна информация, в сравнение с използването на CRL, за статуса на издадените удостоверения.

Модела на предоставяне на OCSP услугата се базира на запитване – отговор. Като отговорите които се получават от OCSP сървъра, осигуряващ услугата, са следните:

- good – означава положителен отговор на запитването, който трябва да се интерпретира като потвърждение на валидността на удостоверението;
- revoked – означава, че удостоверението е било прекратено;
- unknown – означава, че статуса на удостоверението не е установен или удостоверението не е издадено от съответния УО.

23. Услуги по валидация

Доверяващите се страни могат да използват следните услуги са да проверят статуса на издадено от „СЕП България“ АД удостоверение за електронен подпис:

- Проверка в списъка с прекратени удостоверения;
- On-line проверка чрез OCSP протокол.

Допълнителна информация за съдържанието на удостоверението може да се намери в публичния регистър на доставчика.

23.1 Експлоатационни характеристики

За да се осъществи проверка за статуса на издадено удостоверение е необходимо:

- При CRL – да се изтегли CRL за съответния УО и да се инсталира в приложението на крайния потребител. Мястото, от където може да се изтегли CRL се посочва във всяко издадено удостоверение;
- При OCSP – да се изпрати заявка за валидация до сървъра на „СЕП България“ АД. Протокола за обмен е дефиниран в RFC 2560.

23.2 Достъпност на услугата

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

24. Издаване на удостоверение за време

„СЕП България“ АД предоставя услуги по издаване на удостоверение за времето на представяне на електронен подпис, създаден за определен електронен документ.

Удостоверението за време има официална удостоверителна сила след вписването му във воден от ДУУ регистър за издадените удостоверения за време.

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

24.1 Процедура по предоставяне на услугата Издаване на удостоверение за време

Системата на „СЕП България“ АД, 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 подписване се удостоверява и версия на заявката.

Заявката за удостоверяване на време може да се генерира чрез интернет портала на Дставчика на адрес: <http://tsa.sep.bg> или чрез специализиран клиентския софтуер на „СЕП България“ АД.

Постъпващите заявки се обработват последователно. Точността, с която се издават удостоверенията за време от „СЕП България“ АД, 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“ АД.

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

25. Прекратяване ползване на удостоверителни услуги

„СЕП България“ АД няма ангажимент към титуляра по отношение на предоставяне на услуги по управление на удостоверения, след като Договорът за предоставяне на удостоверителни услуги, сключен между тях е прекратен или изтекъл.

Клиентът на удостоверителните услуги на „СЕП България“ АД, може по всяко време да подаде искане за прекратяване ползване на удостоверителни услуги.

Когато клиентът е поискал прекратяване ползване на удостоверителни услуги, „СЕП България“ АД, прекратява договорните отношения с титуляра/автора и прекратява издадените удостоверения, в които титулярът/авторът е вписан.

„СЕП България“ АД не обезщетява титуляра/автора, при прекратяване на ползването на удостоверителни услуги по негово искане.

26. Съоръжения, ръководство и оперативни контроли

Представят се 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“ АД.

26.1 Съоръжения на доставчика

26.1.1. Физическа сигурност УО и базов РО

Мрежовите компютърни системи, терминалите на операторите и информационните ресурси на „СЕП България“ АД 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.

Местоположение и конструкция

„СЕП България“ АД 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.

26.1.2. 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 доставчика, точно кои служители в кое помещение се намират и как се придвижват от едно помещение в друго.

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 достъпа 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“ АД, имащ право на достъп до посетеното помещение.

Всичко 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“ АД. 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.

26.1.3. 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.

26.1.4. Наводнение

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

26.1.5. Противопожарни мерки

Взети са мерки по откриване и гасене на пожар в помещенията на „СЕП България“ АД. 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.

26.1.6. 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. Достъпа 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.

26.1.7. Депозирание 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.

26.1.8. Съхранение на резервните копия

„СЕП България“ АД съхранява резервни копия от всички необходими данни, с чиято помощ може да възстанови своите операции в рамките на 48 часа. Това са копия на пароли, ПИН, криптографски карти, архиви на актуалните данни и резервни копия на информационните системи.

26.2 Съоръжения на РО

Компютърните системи в РО се разполагат в подходящо оборудвани помещения и работят в On-line 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. Може да намерите на следния адрес: <http://e-sign.sep.bg>.

26.3 Сигурност на титуляра/автора

Титуляра/авторът е отговорен за съхранението на паролите за достъп, идентификационни кодове, ПИН и деблокиращ ПИН.

26.4 Контрол на процедурите

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

26.5 Доверени длъжности

„СЕП България“ АД 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 организира работата на служителите си по начин, който гарантира, че дейностите по:

- Генериране и поддържане на инфраструктурата на публичния ключ на доставчика на удостоверителни услуги;
- 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 и
- Съхранение на данни и архивиране се изпълняват от различни лица Идентификация и автентификация за доверени длъжности.

„СЕП България“ АД няма да назначи на доверена или ръководна длъжност, лице, за което е известно, че е осъждано за умишлено престъпление от общ характер.

26.6 Управление на персонала

„СЕП България“ АД предприема мерки, за да се гарантира 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;
- 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.

26.6.1. Квалификация и опит

„СЕП България“ АД 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“ АД преди да назначи лице на съответните длъжности проверява познанията и квалификацията му.

26.6.2. Обучение на персонала

Персоналът на доставчика на удостоверителни услуги – „СЕП България“ АД, 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;
- Системния софтуер на УО и РО;
- Работа с клиенти и защита на личните данни.

26.6.3. Процедури за действие при извънредни ситуации, повреди, аварии и природни бедствия.

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.

26.6.4. Дисциплинарни мерки

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

26.7 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.

26.8 Документи предоставяни на персонала

Ръководството на „СЕП България“ АД, 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 заявки;
- 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.

27. Водене на записи и преглеждане на журналите

За да управлява ефективно своите операции и управлява своя персонал, „СЕП България“ АД води записи за всички свои 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 имат.

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.

Системният контролор на ДУУ 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.

27.1 Тип на записваните събития

Всяка критична дейност по отношение на сигурността на „СЕП България“ АД 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“ АД. 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 регистрации и 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 журналиите 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 защитните периметри;
- Смяна 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 и взето решение в електронна форма. Цялата кореспонденция в електронна форма между ДУУ и другите участници в удостоверителния процес;
- История на архивните копия на журналиите, системите и бази данни.

Достъп до журналиите имат само системния контролърор и лица, осъществяващи проверка на дейността на ДУУ.

27.2 Преглед на журналиите

Поне веднъж месечно се прави детайлен преглед на журналиите. При проверката журналът се преглежда и за цялостност и автентичност. Веднъж седмично подробно се преглеждат журналиите от произволно избрана операция.

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

27.3 Период на съхранение

Журналиите се съхраняват на дисковете на информационните системи докато се достигне определен размер. През това време те са достъпни on-line за всички упълномощени лица. След това се архивират

и достъпа до тях е off-Line. Архивите се пазят най-малко 10(десет) години от получаване на информацията и сключване на договор с клиента.

27.4 Защита на журналните файлове

Журналните файлове се криптират при архивиране, като ключа за архивиране е под изключителния контрол на системния контролор.

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

- Само упълномощени лица – проверяващи и служители на ДУУ, имат право да преглеждат файловете;
- Само системния контролор има право да архивира и изтрива файлове съдържащи регистрирани събития;
- Открива се всяко нарушение на целостта на данните и се гарантира, че всеки запис 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.

27.5 Архивиране на журналните файлове

„СЕП България“ АД 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“ АД. Архивните копия, които са в електронен вид, може да са с удостоверено време на създаването им.

28. Известяване за събития

„СЕП България“ АД 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.

29. Оценка на уязвимостите

„СЕП България“ АД 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.

30. Архивиране на записите

Всички данни и файлове свързани с регистрацията на потребителите на удостоверителни услуги и сигурността на системите, информация предоставена от титуляра/автора, информация за титуляра/автора, издадените удостоверения, генерираните CRL, ключовете използвани от ПО и цялата кореспонденция между „СЕП България“ АД и титуляра/автора или упълномощени представители на „СЕП България“ АД се архивират. Архивират се документите и данните, използвани за идентификация на титуляра/автора и проверка на идентичността съответно самоличността на титуляра/автора. Данни, които не са пряко необходими за процеса на проверка може да не се архивират.

Документите, представени в хартиена форма, са преобразуват в електронна форма и след това се архивират.

„СЕП България“ АД поддържа два вида архиви достъпни on-line (On-line архив) и достъпни off-Line (Off-Line архив).

Архивът се съхранява предимно в електронен вид. При необходимост хартиените документи се преобразуват в електронни и след това се използват.

Хартиените оригинали се съхраняват за срок най-малко от 10 (десет) години след изтичане на ангажиментите на „СЕП България“ АД по отношение събитието, за което се отнасят.

30.1 Типове архивни данни

Следните данни се архивират:

- Информацията от проверките и оценки на логическата и физическа защита на УО и РО и публичния 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“ АД и потребителите на удостоверителни услуги и РО;
- Документи и данни използвани в процеса на проверка на идентичността съответно самоличността на титуляра/автора.

30.2 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“ АД 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 и са достъпни off-Line за период от още 10 (десет) години;

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

30.3 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 подходящи процедури.

30.4 Защита на архива

„СЕП България“ АД поддържа средства и предприема мерки, които позволяват да се поддържа целостта и достъпността на данните от архива. Мерките включват следните основни моменти:

- Само упълномощени лица, на доверени позиции имат право на достъп до архива;
- Архива 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, направени в минали периоди от време.

30.5 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 постигне 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 регистър;
- Данните от публичния регистър, бази данни с потребители на удостоверителни услуги и системни бази данни;
- Други данни свързани с дейността на „СЕП България“ АД, като ДУУ;
- Журналните файлове.

Методите за създаване на резервни копия, използвани от „СЕП България“ АД 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“ АД 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“ АД.

30.6 Изискване за удостоверено време за записите

При възможност, за всички архивирани данни се удостоверява момента, към който те са били създадени.

30.7 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 изключително от системния контролор и се отразява в журнала на системата.

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

31. Смяна на ключовете

Прилага се процедура за случаите, когато УО на „СЕП България“ АД подменя ключовете, с които подписва издаваните удостоверения и списък с прекратени удостоверения.

Процедурата се основава на издаването на специално удостоверение от УО, за потребителите, които имат старото удостоверение на УО, за да се гарантира защитената обмяна на новото удостоверение и да позволи 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 и се изпраща уведомление чрез електронна поща до всички автори/титуляри.

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“ АД използват само новия частен ключ за подписване на издадените удостоверения.

32. Компрометиране и възстановяване след бедствия и аварии

„СЕП България“ АД следва строги процедури при компрометиране на частния ключ и 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.

32.1 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“ АД имат право да правят предложения и 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 посочени в документа “План за действие при извънредни обстоятелства и възстановяване след бедствия”.

32.2 Щети по компютърни ресурси, софтуер и/или данни

Политиката за сигурност прилагана от „СЕП България“ АД, определя следните основни заплахи по отношение на непрекъснатостта на предлагане на услуги от:

- Физическо разрушаване на системите на „СЕП България“ АД, включително мрежови ресурси – тази заплаха адресира разрушения от всякакъв най-често случаен характер;
- Неизправност в работата на софтуера и приложенията, няма достъп до данните – това са неизправности причинени от неправилно функциониране на операционни системи и потребителски приложения, вируси, червеи и троянски коне;
- Загуба на важни мрежови услуги – загуба на запазване и физическо прекъсване на кабели;
- Повреда в използвания хардуер.

За да се предотврати и ограничи влиянието на горните заплахи, политиката по сигурност на „СЕП България“ АД, включва:

32.2.1. 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“ АД 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 двете места;
- Периодично се прави пълно резервно копие на всеки сървър. Това копие съдържа всички подадени искания, журнала на събитията, издадените, подновените и прекратените удостоверения. Копията се съхраняват на сигурно място извън „СЕП България“ АД;
- Ключовете на „СЕП България“ АД, разделение 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.

32.2.2. 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.

32.2.3. Резервни системи

В случай на авария или природно бедствие „СЕП България“ АД 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“ АД:

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

32.2.4. Създаване на резервни копия

„СЕП България“ АД 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“ АД. Копията се правят периодично и се съхраняват извън основните сгради на „СЕП България“ АД. Копията се защитават с пароли и се криптират.

32.3 Допълнителни дейности

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

32.4 Компрометиране на частния ключ на УО

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

- УО генерира нова ключова двойка и ново удостоверение;
- Всички потребители на удостоверения незабавно се информират чрез средствата за масова информация и електронна поща;
- 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“ АД.

Продължаване на дейностите след възстановяване от бедствия и авария

След всяко възстановяване на системата от авария, системния контролър и системния администратор извършват следните дейности:

- При необходимост се 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;

- Преглежда се и се анализира казуса свързан с аварията. Кorigира се и се допълва плана за действие, политиката за сигурност и правилата за физически достъп до помещенията и системните компоненти;
- Информират се потребителите на системата за възстановяване на системните дейности.
- Прекратяване или прехвърляне на дейността

33. Прекратяване или прехвърляне на дейността на УО

„СЕП България“ АД уведомява незабавно Комисията за регулиране на съобщенията в случай на иск за обявяване в несъстоятелност, за обявяване на дружеството за недействително или на друго искане за прекратяване или за започване на процедура по ликвидация.

При прекратяване на своята дейност „СЕП България“ АД прехвърля удостоверенията на друг доставчик или ги прекратява. В изпълнение на това „СЕП България“ АД уведомява писмено Комисията за регулиране на съобщенията и потребителите си най-късно към момента на прекратяване на дейността дали друг доставчик ще поеме удостоверенията и да съобщава неговото име.

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

При невъзможност „СЕП България“ АД 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 „СЕП България“ АД.

Доставчик на удостоверителни услуги, който е поел удостоверенията на „СЕП България“ АД, е длъжен да ги поддържа до оставащия им срок на действие безплатно за титуляра и при същите условия, при които са издадени.

34. Прекратяване или прехвърляне на дейността на РО

Регистриращ орган на „СЕП България“ АД може да прекрати своята дейност при:

- Изтичане на срока по договора, уреждащ отношенията между „СЕП България“ АД и лицето, опериращо като РО;
- При нарушаване на договора и неспазване на Наръчника за потребителя;
- По искане на РО.

35. Техническа и технологична сигурност

Описват се процедурите за генериране и управление на криптографските ключови двойки на УО, РО и титуляра/автора и съпътстващите генерацията технически контроли.

36. Генериране и инсталиране на ключови двойки

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

„СЕП България“ АД притежава всички ключове и удостоверения на УО, функциониращи в информационна система. Това са:

- Базов Удостоверяващ орган на „СЕП България“ АД – SEP Root CA;
- Оперативния Удостоверяващ орган – SEP QES CA.

Частният ключ на SEP Root CA се използва изключително и само за подписване на публичните ключове на: SEP 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, SEP 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.

36.1 Генериране на ключови двойки

Всички ключове на УО се генерират в защитените помещения на „СЕР България“ АД, в присъствието на доверена група лица от персонала, нотариус/юрисконсулт и лица от висшето ръководство на „СЕР България“ АД.

Ключовите двойки се генерират, като използва отделена работна станция, свързана с криптографския модул, съответстващ на FIPS 140-2 Level 3 или 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. За всеки запис имаме описание на действието, дата и подпис на лицето реализирало действието и лицето контролиращо изпълнението на действието. Цялата процедура се подписва от всички присъстващи.

Ключовете на РО се генерират от системния оператор под наблюдението на системния контролор, като се използва криптографския модул, съответстващ на FIPS 140-2 Level 2 или аналогични изисквания за сигурност. Използват се за автентифициране на исканията на титуляра/автора, изпращани от РО към УО.

Титуляра/автора сам генерира своята ключова двойка. Генерацията може да се делегира на РО, в случай че ключовата двойка се генерира на криптографска карта.

„СЕР България“ АД може при искане от страна на титуляра/автора, да генерира ключови двойки след което да му ги достави по сигурен начин. В този случай се ползва криптографския модул, съответстващ на FIPS 140-2 Level 2 или аналогични изисквания за сигурност.

36.1.1. Генериране на ключовете на SEP Root CA

Процедурата се изпълнява всеки път при инициализация на системата за доставка на удостоверителни услуги на „СЕР България“ АД.

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 с прекратени удостоверения на базовия удостоверяващ орган и удостоверението за проверка на удостоверено време.

36.1.2. Смяна на ключовете на SEP Root CA

Реализира се процедура за подмяна на ключовата двойка при изтичане на периода на валидност. Процедурата стартира най-малко една година преди да изтече периода на валидност на старата ключова двойка на „СЕР България“ АД. „СЕР България“ АД издава ново КЕР на SEP Root CA и за период от една година „СЕР България“ АД поддържа новото и старото КЕР, след което старото изтича и остава валидно новото КЕР на SEP Root CA.

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

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

36.1.3. Смяна на ключовете на оперативния УО на ДУУ

Следва се процедурата, описана по-горе като новото оперативно удостоверение се издава от SEP Root CA и се подписва с новия частен ключ.

36.2 Предоставяне на частния ключ на автора

Титулярът/авторът сам генерира своята ключова двойка, като използва SSCD.

В случай, че титуляра/автора поиска ДУУ да генерира вместо него ключовата двойка, то „СЕП България“ АД взема мерки това да стане по сигурен и надежден начин, след което да предостави на титуляра/автора данните за активиране и самите смарт карти при спазване на определено в политиката по предоставяне на удостоверителни услуги.

Едни и същи служители на ДУУ не разполагат по едно и също време с данните за активиране на смарт/сим картите.

36.3 Предоставяне на публичния ключ до УО

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

В определени случаи подадените искания трябва да се одобряват от оператор на РО.

36.4 Предоставяне на публичния ключ на УО до доверяващите се страни

Публичният ключ на УО на „СЕП България“ АД се разпространява изключително като част от удостоверение за електронен подпис. Базовото удостоверение на „СЕП България“ АД е под формата на самоподписано удостоверение.

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

- Чрез публикуване в публичния регистър на ДУУ намиращ се на адрес <http://e-sign.sep.bg> ;
- Заедно с потребителски пакет от определени приложения;
- Новото базово удостоверение се предоставя за изтегляне чрез защитена и криптирана връзка като се ползва все още валидно, преди това издадено удостоверение.

При смяна на ключовете на УО в публичния регистър се публикуват всички удостоверения.

37. 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
SEP QES CA	2048 bit	10 години

Параметри на генерация на публичния ключ и проверка за качество

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

38. Защита на частния ключ

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

„СЕП България“ АД 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.

39. Достъп до частния ключ на доставчика

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

Резервни копия на частния ключ

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

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

40. Архивиране на частния ключ

„СЕП България“ АД 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.

41. Трансфер на частния ключ от и към криптомодула

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

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

При трансфер ключът се защитава като се разделя на части и всяка част се криптира с ключ достъпа, до който е чрез парола известна само на държателя на секретната част.

42. Съхраняване на частния ключ в криптомодула

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

Активиране на частния ключ

Частният ключ на „СЕП България“ АД 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.

Деактивиране на частния ключ

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

43. Унищожаване на частния ключ

Частният ключ на „СЕП България“ АД в криптомодула, се унищожават 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 доставчика.

44. Сертификация на криптомодула

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

45. Други аспекти от управлението на ключовете

45.1 Архивиране на публичния ключ

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

45.2 Период на валидност на удостоверенията и използване на ключовете

Максималния период на валидност на удостоверенията използвани от „СЕП България“ АД при предоставяне на удостоверителни услуги и максималния период на използване на съответните частни ключове е като следва:

удостоверение	период	
	валидност на удостоверението	на ползване на частния ключ
SEP Root CA	20 години	19 години
SEP QES CA	10 години	9 години
SEP TSA	10 години	10 години
SEP OCSP	10 години	10 години
SEP Qualified Private	3 години	3 години
SEP Qualified Organization	3 години	3 години
SEP Qualified Professional	3 години	3 години
SEP Server	3 години	3 години

45.3 Данни за активиране

Данните за активиране на ключовите двойки, ПИН и/или пароли и кодове, на „СЕП България“ АД са разделени на защитени части и се държат от различни служители на доверени позиции. „СЕП България“ АД 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 крайните потребители се генерират по време на процедурата по издаване на удостоверение. Възможно е потребителите сами да генерират своя ПИН за достъп до потребителския криптомодул или да се генерират от „СЕП България“ АД.

В случай, че „СЕП България“ АД генерира данните на активиране, те се предоставят по сигурен и надежден начин до титуляра/автора. Допуска се данните за активиране да се предоставят до автора чрез титуляра или негов пълномощник. Във всички случаи се изисква титуляра/автора да сменят ПИН веднага след като го получат.

46. Управление на компютърната сигурност

46.1 Технически изисквания

Техническите изисквания се отнасят за една компютърна система с инсталиран системен софтуер, която се използва 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 автентификация 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“ АД;
- Криптографски се защитава обмена и базите данни.

46.2 Оценка на сигурността

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

46.3 Технически контроли

46.3.1. Управление контролите за информационна сигурност

Целта на управлението на контролите за информационна сигурност е да подпомогне „СЕП България“ АД и даде увереност, че системите функционират правилно в съответствие с направените настройки и по начин, по който са конфигурирани.

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

46.3.2. Мрежова сигурност

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

„СЕП България“ АД 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.

47. Профили на удостоверения, списък с прекратени удостоверения и OCSP

Профилите на удостоверенията за електронен подпис и списъците с прекратени удостоверения са дефинирани в съответствие с RFC 3280 и ITU-T X.509 v.3. Профила за OCSP е в съответствие с RFC 2560, а за удостоверяване на време е в съответствие с RFC 3161.

47.1 Профили на удостоверенията

Прави се преглед на полетата, включени в съдържанието на удостоверенията, тяхната интерпретация и се представят профилите на издаваните удостоверения в цялата йерархия на „СЕП България“ АД.

47.2 Съдържание на удостоверението

„СЕП България“ АД поддържа определен набор от полета и атрибути в издаваните удостоверения при предлагане на удостоверителни услуги. Наличието или отсъствието на определени атрибути в полетата зависи от типа издадено удостоверение. „СЕП България“ АД определя и набор от разширения на удостоверенията. Част от разширенията се отбелязват като критични, за да гарантира правилното използване на удостоверенията. Приложенията, които ползват удостоверенията трябва да отхвърлят всяко удостоверение, което съдържа критично разширение, което неразпознато. По - долу е дадено общо описание на поддържаните полета и разширения от „СЕП България“ АД.

- 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: идентификатора 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 стойностите 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	SEP QES CA
	Street	bul.Shipchenski prohod 18
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 КЕП.	
	*C, Country	определя контекста, в който се разглеждат останалите атрибути
	ST, State or Province	ако се ползват съдържат географска информация свързана с титуляра. Ако присъства organizationName то тази информация се отнася до организацията
	*L, Location	
	O, Organization	ако се ползват 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/псевдоним на автора
	T, Title	ако се използва 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	

име на поле	стойност или ограничение на стойността
	Phone телефон на титуляра
	*EmailAddress е-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}
Certificate Policies	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.30299.2.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text=SEP QES CA [1,2]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://e-sign.sep.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
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	сА: yes/no, Path Length Constraint=None
Subject Alternative Name	адрес на автора
Authority Key Identifier	
Subject Key Identifier	
subjectPublicKeyInfo	публичния ключ на автора и алгоритъма, с който се използва
Qualified Certificate Statements	посочва, че удостоверението е издадено като удостоверение за квалифициран електронен подпис

име на поле	стойност или ограничение на стойността
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” АД 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 политиката;
- 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.

48. Проверка и контрол на дейността

48.1 Честота и обстоятелства на проверките

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

„СЕП България“ АД осъществява постоянен вътрешен контрол, който се извършва от упълномощени 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“ АД осъществява постоянен контрол върху дейността на Регистриращите органи.

Идентификация и квалификация на проверяващите

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

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 Доставчика, изрично оторизирани от „СЕП България“ АД или външна проверяваща организация.

48.2 Избягване конфликт на интереси

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

48.3 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 Доставчика, които могат да включват, но не се ограничават до:

- Съответствието на процедурите и практиките на „СЕП България“ АД 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.
Предприемане на действия за отстраняване на недостатъците

Докладът от проверката се разглежда от висшето ръководство на „СЕП България“ АД. Анализират се несъответствията и се предприемат мерки за отстраняването им.

48.4 Съобщаване на резултатите

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

49. Търговски и правни условия

49.1 Цени на удостоверителните услуги

„СЕП България“ АД в качеството си на ДУУ определя цени на предоставяните от него удостоверителни услуги. Информация за цените на удостоверителните услуги и събираните такси от „СЕП България“ АД са публично достъпна на адрес: <http://e-sign.sep.bg>.

„СЕП България“ АД си запазва правото да променя едностранно цените за предоставяне на удостоверителни. Промените се публикуват на адрес: <http://e-sign.sep.bg>.

С публикуването на новите цени се приема, че ДУУ е уведомил титулярите за новите цени. Промените влизат в сила от деня, следващ публикацията.

Промените се отнасят за бъдеще и не се отнасят за вече платени авансово еднократни или абонаментни такси.

49.2 Цени на услуги

„СЕП България“ АД може да събира плащания за предоставяне на следните услуги за:

- Издаване на удостоверение за електронен подпис;
- Подновяване на удостоверение за електронен подпис;
- Достъп до удостоверения публикувани в публичния регистър;
- Достъп до информация за статуса на издадените удостоверения;
- Други услуги.

Дължимите такси се заплащат, съгласно ценова листа на предоставяните от „СЕП България“ АД удостоверителни услуги или уговореното в договора за предоставяне на удостоверителни услуги.

Ако определени такси са заплатени авансово или като абонамент за услуга, те не се възстановяват, ако услугата не се ползва.

49.3 Възстановяване на суми

При приемане на удостоверението, ако Титулярът посочи грешки или непълноти, които не са по негова вина в срок от 3 (три) дена, „СЕП България“ АД прекратява удостоверението и издава ново безплатно без допълнително заплащане или възстановява направеното плащане.

49.4 Финансова отговорност

49.4.1. Застраховка на дейността

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

Предмет на застраховка е отговорността на „СЕП България“ АД в качеството му на доставчика на удостоверителни услуги, издаващ удостоверения за квалифициран електронен подпис за осъществяваната от него дейност по ЗЕДЕП, съгласно изискванията на чл. 29 от Закона за електронния документ и електронния подпис.

„СЕП България“ АД сключва застраховка преди да подаде документи за регистрация в Комисията за регулиране на съобщенията.

„СЕП България“ АД има застраховка 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 дни, да уведоми писмено „СЕП България“ АД и застрахователя на „СЕП България“ АД.

49.4.2. Застрахователно покритие за крайните потребители

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

Застраховката не покрива и Доставчикът не отговаря 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 не полагане на дължимата грижа за опазването или ползването му;
- Неспазване на изискванията относно полагане на дължимата грижа за проверка валидността на електронния подпис и на издаденото от Доставчика удостоверение от Доверяващите се страни;
- Форсмажор, аварии и други събития, които са извън контрола на Доставчика.

50. Конфиденциалност на информацията

„СЕП България“ АД спазва всички приложими правила за защитата на личните данни и на конфиденциалната информация, събирана с оглед на дейността му, като доставчик на удостоверителни услуги и както са описани в Наръчника за потребителя.

50.1 Обхват на конфиденциалната информация

„СЕП България“ АД 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 действието на удостоверения, извън публикуваната информация за статуса на удостоверението;
- Кореспонденция, свързана с дейността на „СЕП България“ АД, като доставчик на удостоверителни услуги;
- Частните ключове на „СЕП България“ АД;
- 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.

50.2 Информация извън обхвата на конфиденциалната информация

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

- Удостоверенията, публикувани в регистъра на доставчика;
- Данните, които се съдържат в удостоверенията;
- Данните за статуса на удостоверенията, публикувани в Списъка на прекратени удостоверения.

50.3 Задължение за пазене на конфиденциалната информация

„СЕП България“ АД 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, титуляра/автора 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“ АД, без предварително изрично писмено разрешение.

51. Защита на личните данни

„СЕП България“ АД събира данни и информация за титуляра/автора, само за целите на издаване и управление на удостоверения за електронен подпис.

„СЕП България“ АД събира, обработва, съхранява и предоставя достъп до тези лични данни на трети лица при спазване изискванията на Закона за защита на личните данни.

„СЕП България“ АД е регистриран като администратор на лични данни от Комисията за защита на личните данни по реда на Закона за защита на личните данни.

„СЕП България“ АД предварително информира лицата за видовете информация, която събира за тях, начина на нейното съхранение и достъпа до нея на трети лица.

52. Права върху интелектуалната собственост

„СЕП България“ АД притежава и си запазва всички права на интелектуална собственост върху бази данни, интернет страници, удостоверения за електронен подпис, издадени от „СЕП България“ АД, както и всякакви други документи, които разработва и поддържа.

„СЕП България“ АД 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“ АД 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“ АД са собственост на „СЕП България“ АД.

53. Задължения и отговорности

53.1 Задължения и отговорности на „СЕП България“ АД

„СЕП България“ АД е ДУУ регистриран от КРС и действащ съгласно ЗЕДЕП и подзаконовите актове по неговото прилагане. В това свое качество „СЕП България“ АД 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 електронен подпис, както са одобрени от 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“ АД е отговорен пред титуляра и доверяващите се страни за вредите:

- От неизпълнение на изискванията по чл. 21 от ЗЕДЕП и на задълженията му по чл. 22 и 25 от ЗЕДЕП и Наръчника за потребителя;
- 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, включен в издадено от Доставчика удостоверение, ако Доставчикът не е положил дължимата грижа при проверка на това обстоятелство;
- От несъответствие между данните за установяване използването на частния ключ и данните, предоставени на лицето, използващо публичния ключ.

53.2 Задължения и отговорности на регистриращите органи

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

„СЕП България“ АД гарантира, че РО:

Спазва всички разпоредби на ЗЕДЕП и подзаконовите актове по неговото прилагане;

Изпълнява стриктно определените процедури и спазва политиките по издаване управление на удостоверения за електронен подпис, както са одобрени от Комисията за регулиране на съобщенията;

Идентифицират физически лицата, на които се издава удостоверение за КЕП;

Потвърдената от оператор РО информация и включена в издаденото удостоверение е точна и пълна и съответства на състоянието към момента на извършване на проверката.

53.3 Задължения и отговорности на титуляра/автора

Титулярът сключва договор за удостоверителни услуги със „СЕП България“ АД и е собственик на удостоверенията, за които е подал искане за издаване пряко или чрез посредник. Може да подава и исканията за последващо управление на удостоверения за електронен подпис.

Титулярът гарантира:

За действията на авторите, за които е поискал издаване на удостоверение за електронен подпис;

Че автора е овластен извършва електронни изявления от негово име и държи частния ключ, съответстващ на посочения в удостоверението публичен ключ;

Да подаде точна и пълна информация на ДУУ в съответствие с изискванията на тази политика и специално що се отнася до регистрацията;

Да използва ключовата двойка само за електронен подпис и в съответствие с всяко друго ограничение, за което титулярът е информиран ;

Да упражнява разумна грижа за избягване на неоторизирано използване на частния ключ на автора;

Ако титуляра/автора генерират сами двойката ключове:

Да използват алгоритми одобрени като подходящи за целите на универсалния електронен подпис;

Да използват дължина на ключовете одобрена като подходяща за целите на универсалния подпис за времето на валидност на КЕП;

Частният ключ на автора да бъде използван единствено под контрола на автора;

Ако политиката по предоставяне на удостоверителни услуги изисква използването на SSCD, да използва КЕП само с електронни подписи създадени с използването на такова устройство;

Да 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 резултат на компрометирането използването на частния ключ на автора е прекъснато незабавно и завинаги;

В случай, че бъде информиран, че ДУУ, издал удостоверението на автора, е бил компрометиран, да осигури, че удостоверението няма да се използва от автора.

Автора гарантира, че е овластен от титуляра да го представлява.

Титулярът, съответно Авторът отговаря спрямо Доставчика, ако е приел удостоверението, издадено от Доставчика въз основа на неверни данни, предоставени от него, съответно въз основа на премълчани или липсващи данни.

Във всички случаи на неизпълнение на задълженията от страна на Титуляра, съответно Автора, произтичащи от Наръчника за потребителя или от Договора за удостоверителни услуги, Доставчикът ще ангажира отговорността на Титуляра за вреди.

53.4 Задължения и отговорности на доверяващата се страна

Доверяващата се страна проверява електронни подписи и в резултат на проверката взема решение дали да се довери или не на подписаното изявление. Трябва да извършват проверките на валидността, спирането или прекратяването на действието на удостоверение посредством предоставената от ДУУ, информация за техния статус и да вземат под внимание и да съобразяват действията си с всички ограничения на ползването на удостоверението, включени в самото удостоверение.

Лицата, които се доверяват на удостоверителните услуги за квалифициран електронен подпис на Доставчика, следва да полагат дължимата грижа, като:

Имат технически умения да ползват удостоверения за електронен подпис;

Информирани са за условията, при които трябва да се доверяват на удостоверенията, съобразно политиките, при които са издадени и процедурите за извършваните проверки на информацията от ДУУ;

Проверяват издадени удостоверения чрез публично достъпните данни за статуса на удостоверенията – Списък с прекратените удостоверения;

Се доверяват на издадени от ДУУ удостоверения, само ако резултатът от направените проверки е положителен.

53.5 Ограничаване на отговорността

Освен в случай на небрежност „СЕП България“ АД не носи отговорност за:

Пропуснати ползи или други косвени вреди, произтичащи от или във връзка с използването, или невъзможността за използване на 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 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 титуляра/автора 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 следствие от небрежност, не полагане 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.

54. Лимит на отговорността

„СЕП България“ АД ограничава действието на електронните подписи, за които издава удостоверения за електронен подпис до определен лимитиран имуществен интерес. „СЕП България“ АД ограничава своята отговорност до рамките на посочения по долу лимити:

тип удостоверени за електронен подпис	максимален лимит на отговорност
SEP Private	60 000 лева
SEP Organization	60 000 лева
SEP QES Professional	60 000 лева
SEP Server	60 000 лева

Посочените лимити на отговорност се считат за ограничения на отговорността на Доставчика по смисъла на чл.24, ал.1, т.10 във връзка с чл.29, ал.3 на ЗЕДЕП.

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

55. 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“ АД ще предприеме мерки, за да бъде обезщетен за претърпени щети.

III. Политика при предоставяне на удостоверителни услуги

1. Обхват

Тази част от документа прави общ преглед на политиката по предоставяне на удостоверителни услуги на „СЕП България“ АД в качеството му на регистриран доставчик на удостоверителни услуги(ДУУ). Представя общата концепция на „СЕП България“ АД, относно предоставяне на удостоверителни услуги. Документът дефинира страните участници в процеса по предоставяне на удостоверителни услуги, техните задължения, типовете удостоверения за електронен подпис, процеса по проверка на самоличността съответно идентичността и областта на приложени на издадените удостоверения за квалифициран електронен подпис(КЕП).

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

2. Общ преглед

„СЕП България“ АД 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 трето 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“ АД предоставя удостоверителни услуги посредством удостоверяващ орган и упълномощени регистриращи органи.

Удостоверяващият орган и регистриращите органи извършват дейностите си по предоставяне на удостоверителните услуги от името на „СЕП България“ АД.

3. Модел на удостоверителни услуги

„СЕП България“ АД следва следния технологичен модел за предоставяне на удостоверителни услуги. Дефинирани са следните услуги от технологична гледна точка:

3.1 Регистриране.

Приемане на искането за издаване на КЕП, проверка чрез допустимите средства самоличността, съответно идентичността, на автора и на титуляра и ако е необходимо - други данни за тези лица, включени в удостоверението. Обработване на подадените искания за управление за отразяване на промените, спиране, възобновяване, прекратяване на издадени КЕП. Проверява самоличност съответно идентичност и специфични данни за заявителите на КЕП. Резултата от тази услуга се изпраща към услугата по създаване на КЕП;

3.2 Създаване на удостоверения.

Създаване и подписване на удостоверение, базирано на данните проверени от услугите по регистриране. Публикуване в списък с издадените удостоверения.

Публикуване и разпространение – предоставяне на КЕП на авторите/ титулярите и при съгласие на автора предоставя на информация за КЕП на доверяващите се страни. Тази услуга публикува политиките и практиките на доставчика по отношение на удостоверителните услуги и списъка с прекратените удостоверения;

3.3 Прекратяване на удостоверения

Управляване исканията и реагиране при докладване на сведения, свързани със спиране и/или прекратяване на КЕП. В резултат се предприемат действия по прекратяване или спиране/възобновяване на КЕП;

3.4 Статус на издадените удостоверения

Предоставяне на информация за статуса на КЕП на доверяващите се страни. Използват се списъци с прекратени удостоверения или услуги предоставящи информация за статуса на КЕП в реално време. Информацията за статуса на КЕП се обновява на зададен период;

3.5 Предоставяне на устройства

Това може да бъдат смарт карти или други устройства за сигурно създаване на електронен подпис. Устройствата се подготвят и предоставят на авторите пряко или по сигурен начин чрез титуляра. Това може да бъдат услуги по създаване и предоставяне на ключова двойка на авторите или по подготовка, генериране и предоставяне на авторите/титулярите на устройства и необходимите данни за активиране;

3.6 Удостоверяване на време

Издаване на удостоверение за времето на представяне на електронен подпис, създаден за определен електронен документ.

4. Предназначение

Документът „Политика за предоставяне на удостоверителни услуги” описва политиката на издаване на удостоверения от доставчика и видовете услуги, предоставяни от „СЕП България” АД.

5. Ниво на детайлност

Политиката по предоставяне на удостоверителни услуги представя общите изисквания, които се реализират от ДУУ.

„СЕП България” АД при нужда разработва, внедрява и документира вътрешни оперативни указания, инструкции или правила свързани с посочените практики, 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.

6. Подход

Политиката по предоставяне на удостоверителни услуги е дефинирана независимо от специфичните детайли свързани с операционната среда на ДУУ.

7. Документи по отношение на трети страни

„СЕП България” АД поддържа в съответствие с тази политика и в съответствие със ЗЕДЕП и подзаконовите нормативни актове, издадени по неговото прилагане, следните документи:

- „Наръчник за потребителя”;
- „Договор за предоставяне на удостоверителни услуги”.

Документите са публични и достъп до тях имат всички заинтересовани лица.

8. Изисквания към дейността на ДУУ

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

Настоящата политика отразява дейностите на ДУУ издаващ удостоверения за квалифициран електронен подпис. Това включва услуги по Регистриране, Създаване на КЕП, Публикуване и разпространение, Прекратяване на КЕП, Статус на КЕП, Предоставяне на устройства, Удостоверяване на време.

При осъществяване на дейността по предоставяне на удостоверителни услуги, „СЕП България“ АД се задължава да спазва условията на настоящата политика и закона за електронния документ и електронен подпис и подзаконовите актове по неговото прилагане.

„СЕП България“ АД 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“ АД 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 всички 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 КРС 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“, одобрението съгласно;
- Документира използваните алгоритми и техните параметри.

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

9.1 Генериране на ключовете на ДУУ

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

9.1.1. Защитена среда

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

9.1.2. Упълномощен персонал

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

9.1.3. Поделяне на секретни части

„СЕП България“ АД използва поделяне на секретни части и ги разпределя между упълномощени лица, които се грижат за съхраняването на секретните части.

9.1.4. Надеждни системи

„СЕП България“ АД използва надеждни системи при предоставяне на своите удостоверителни услуги и генерация 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.

9.2 Генериране на ключовете на „СЕП България“ АД

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

9.2.1. Стартова процедура

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

9.2.2. Криптографски хардуер

Генерацията на ключовете на „СЕП България“ АД 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.

9.2.3. Използвани алгоритми

Ключовете на „СЕП България“ АД 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 усъвършенстван електронен подпис“.

9.2.4. Дължина на ключа

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

9.2.5. Гарантиране непрекъснатост на операциите

Достатъчно време преди края на периода на валидност на ключовете, подписващи издаваните КЕП, „СЕП България“ АД 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.

9.3 Съхраняване, архивиране и възстановяване ключове на ДУУ

„СЕП България“ АД осигурява конфиденциалност и интегритет на своите частни ключове.

9.3.1. Държане и ползване на частния ключ

Частните ключове на ДУУ, използвани за подписване на 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.

9.3.2. 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.

9.3.3. Архивиране на частния ключ

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

9.3.4. Копия на частния ключ

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

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.

9.3.5. Разпространяване на публичните ключове на ДУУ

„СЕП България“ АД 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.

9.3.6. 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.

9.3.7. 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.

9.4 Използване на ключовете на ДУУ

„СЕП България“ АД, като ДУУ осигурява подходящо използване на своите частните ключове.

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

9.5 Физическа защита

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

9.6 Прекратяване на жизнения цикъл на ключове на ДУУ

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

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

9.7 Жизнен цикъл на криптографския хардуер ползван за подписване на КЕП

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

9.7.1. Доставка на криптографски хардуер

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

9.7.2. Съхранение на криптографски хардуер

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

9.7.3. Съвместен контрол

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

9.7.4. Функциониране на криптографския хардуер

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

9.7.5. Унищожаване на частните ключове в криптографския хардуер

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

10. Осигуряване на титуляра/автора услуги по управление на ключовете

В случай, че „СЕП България“ АД предоставя услуги на титуляра/автора по управление на ключовете, то „СЕП България“ АД предприема мерки така, че всички генерирани от ДУУ ключове за автори са генерирани по сигурен начин и е осигурена секретността на частния ключ на автора.

10.1 Използвани алгоритми

В случаите, в които ДУУ генерира ключове за автора, използва алгоритми признати за подходящи за използване за целите на универсалния електронен подпис за времето на валидност на издаденото за него удостоверение.

10.2 Дължина на ключовете

В случаите, в които ДУУ генерира ключове за автора, дължината на ключовете използвана заедно с алгоритмите са признати за подходящи за използване за целите на универсалния електронен подпис за времето на валидност на издаденото за него удостоверение.

10.3 Съхраняване на генерираните ключове

В случаите, в които ДУУ генерира ключове за автора, ДУУ осигурява необходимите средства за надеждно генериране и съхраняване на ключове за автора до предаването им на автора по сигурен начин, като SSCD.

10.4 Предоставяне на ключовете

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

10.4.1 Подготовка на SSCD

ДУУ осигурява сигурно и надеждно издаване на КЕП чрез SSCD.

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.

10.4.2 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.

10.4.3 Деактивация и реактивация на SSCD

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

10.5 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.

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

11.1 Регистрация на титуляра/автора

„СЕП България“ АД предприема мерки за осигуряване на правилна идентификация и автентификация на заявителите на КЕП и пълни, точни и надлежно упълномощени искания за издаване на КЕП.

11.1.1. Предоставяне на информация за удостоверителните услуги

Преди да се подпише договор за удостоверителни услуги с титуляра, ДУУ информира титуляра за реда и условията относно използването на удостоверението.

11.1.2. Канали за информиране

ДУУ съобщава информацията за реда и условията относно използването на удостоверението за квалифициран електронен подпис, чрез надеждна комуникационна среда включително и електронна, като използва ясен и точен език.

11.1.3. Проверка регистрация

ДУУ проверява по време на регистрацията чрез допустими средства, в съответствие с националното законодателство, самоличността съответно идентичността и ако е приложимо и 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. Представените доказателства може да са както в хартиена, така и под форма на електронен документ.

11.2 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.

11.3 Идентификация на юридически лица

Когато за целите на издаване на 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 свързаното 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.

11.4 Съхранявана информация

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

11.4.1. Данни за представителство

Ако заявката за издаване на КЕП се подава от страна различна от автора/титуляра, тогава трябва да се представят доказателства, че подалия искането е упълномощен да действа от името на идентифицирания в КЕП автор/титуляр.

11.4.2. Данни за обратна връзка

Титулярът предоставя адрес или други данни, които посочват как може да се установи връзка с него.

11.5 Договорни отношения

ДУУ пази подписан договор с абоната, който включва:

- Съгласие със задълженията на абоната;
- Съгласие за ползване на SSCD;
- Съгласие ДУУ да съхранява записи от информация използвана за регистрация, предоставяне на SSCD и следващи действия по прекратяване, идентичността и специфични атрибути на субекта поместени в удостоверението и предоставянето на тази информация на трета страна при същите условия, както се изисква в тази политика, в случай че ДУУ прекратява своята дейност;
- Дали и при какви условия титуляра изисква и автора дава съгласие за публикуване на удостоверението;
- Потвърждение, че информацията съдържаща се в удостоверението е вярна и точна.

11.6 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.

11.7 Притежание на частния ключ

Ако ДУУ не е генерирал частния ключ на автора, процеса по заявяване издаване на удостоверение гарантира, че автора държи частния ключ съответстващ на публичния ключ предоставен за удостоверяване.

11.8 Притежание на SSCD

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

11.9 Подновяване, смяна на ключове и актуализиране

ДУУ се уверява, че заявките за подновяване, смяна на ключове или актуализиране на удостоверение са пълни и изхождат от титуляра или надлежно упълномощено от него лице. Това включва подновяване на удостоверения, смяна на ключове след прекратяване или преди изтичане периода на валидност на удостоверението или актуализиране поради промяна в данните на автора.

11.9.1. Актуален КЕП

ДУУ проверява наличието и валидността на удостоверението, което ще се подновява и валидността на информацията използвана за проверка на идентичността и данните за автора.

11.9.2. Променени условията на „СЕП България“ АД

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.

11.9.3. Променено съдържание на КЕП

Ако някое от имената в удостоверението или данни са променени или предишното удостоверение е било прекратено то информацията за регистрацията се проверява, записва и титуляра ги приема в съответствие с този Наръчник.

11.9.4. Запазване на ключовата двойка

ДУУ издава ново удостоверение използвайки предишния удостоверен публичен ключ на автора само ако криптографската сигурност на ключа е все още достатъчна за новия период и няма индикации за компрометиране на съществуващия частен ключ на автора.

11.10 Създаване на удостоверение

„СЕП България“ АД предприема мерки, за да осигури сигурна и надеждна генерация на удостоверенията за квалифициран електронен подпис.

12. Идентификация

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

Посредством включване на съответните идентификатори в издаваните КЕП, „СЕП България“ АД, демонстрира съответствие с идентифицираната удостоверителна политика.

12.1 Идентификатор на политиката

Идентификатора 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 се включват в съдържанието на всяко издадено удостоверение в съответствие с тази политика и конкретен тип удостоверение.

12.2 Потребителска общност и приложение на КЕП

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

Електронният подпис, за които е издадено удостоверение отговарящо на изискванията на тази политика, има значението на саморъчен подпис по отношение на всички включително и държавен орган или орган на местното самоуправление.

Удостоверенията за КЕП издадени според тази политика, могат да се използват за потвърждаване на КЕП, които удовлетворяват изискванията за подпис свързан с данни в електронна форма по същия начин, както саморъчния подпис удовлетворява тези изисквания по отношение на данните в хартиен формат.

12.3 Спазване на политиката

12.3.1. Общи сведения

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

12.3.2. Съответствие с политиката

Спазването на тази политика от ДУУ означава, че:

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

12.4 Профил на 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.

13. Мерки срещу фалшифициране на 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.

14. Сигурна генерация

Ако ДУУ генерира ключовете на автора то:

- Процедурата по издаване на удостоверение се разглежда заедно с процедурата по генериране на ключова двойка от ДУУ;
- Частния ключ (или SSCD – виж 0) по сигурен начин се предава на автора.

15. Конфиденциалност и интегритет на данните за регистрация

Конфиденциалността и интегритета на данните за регистрация са защитени и в случаите, когато се обменят с титуляра, автора или помежду различни компоненти от инфраструктурата на ДУУ.

16. 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 автентифицирана.

17. Разпространяване на реда и условията

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

18. Публикувана информация

ДУУ предоставя за ползване от абонатите и доверяващите се страни реда и условията на своята дейност и реда за ползване на удостоверенията, които показват:

- Приложението на удостоверителна политика за издаване на удостоверения за квалифициран електронен подпис с използване на SSCD;
- Ограничения в използването;
- Задълженията на абоната, включително дали прилагането на политиката изисква използването на SSCD;
- Информация как да се провери удостоверението, включително изискването да се проверява списъка с прекратени удостоверения, така че доверяващите се страни 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 юридически спорове;
- Приложимото законодателство;
- Информация за регистрация на ДУУ от КРС или други сертификации за съответствие с тази политика, като се посочи и според коя схема.

19. Достъпност и разпространение на информацията

Информацията, посочена по-горе, е достъпна през цялото време за целите на комуникацията, може да бъде предавана електронно и използва ясен и разбираем език.

19.1 Достъп при генерация

След генерацията, цялото и вярно удостоверение е достъпно за автора/титуляра.

19.2 Ограничаване на достъпа

Удостоверението е достъпно за извличане само в тези случаи, за които е получено съгласието на автора.

19.3 Информация за доверяваща се страна

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

19.4 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 други поради други фактори, които не са под контрола на ДУУ, ДУУ ще положи мак-

сигурни усилия, за да осигури престой на тези информационни услуги не повече, отколкото е максималният период от време посочен в практиката при предоставяне на удостоверителни услуги.

19.5 Публичност и достъпност на информацията за КЕП

Информацията, определена в т.17, 18 и 19, е публична и достъпна за всички.

20. Прекратяване, спиране и възобновяване на КЕП

ДУУ прекратява удостоверенията своевременно базирайки се на оторизирани и валидирани заявки за прекратяване на удостоверения.

20.1 Документиране на процедурата

ДУУ документира като част от своята практика на доставчика при предоставяне на удостоверителни услуги процедурите по прекратяване на удостоверения, включително:

- Кой може да подава сведения и искане за прекратяване;
- Как се подават сведения и искания за прекратяване;
- Изисквания за допълнителни 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;
- Максималното закъснение, между приемане на искане за прекратяване или сведение за компрометиране и промяната в информацията за статуса на прекратените удостоверения, след което информацията става достъпна за доверяващите се страни.

20.2 Приемане на искания за прекратяване/спиране

Исканията и сведенията относно прекратяването се обработват веднага при постъпването.

20.3 Проверка на заявките

Исканията и сведенията относно прекратяването се автентифицират и проверяват дали са постъпили от оторизиран източник. Тези искания и сведения трябва да бъдат потвърдени.

20.4 Спиране на КЕП преди прекратяване

Удостоверение може да бъде спряно докато се потвърди дали ще бъде прекратено или не. ДУУ не държи спряно удостоверението по-дълго от необходимото време за потвърждаване на неговия статус, нито по-дълго от указаното в нормативната уредба максимално време за спиране.

20.5 Информирание за промяна на статуса

Авторът и титулярът биват информирани за всяка промяна в статуса на удостоверението.

20.6 Необратимост на прекратяването

Когато удостоверението бъде прекратено то не може повече да се върне към нормален статус.

21. Списък с прекратени удостоверения

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

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

21.1 Достъпност на списъка с прекратени удостоверения

Услугите по управление на статуса на прекратените удостоверения са достъпни 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 престой на тези информационни услуги не повече, отколкото е максималният период от време посочен в практиката при предоставяне на удостоверителни услуги.

21.2 Статус на удостоверенията за електронен подпис

Информацията за статуса на удостоверения 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 престой на тези информационни услуги не повече, отколкото е максималният период от време посочен в практиката при предоставяне на удостоверителни услуги.

22. Интегритет и автентичност на информацията за статуса на КЕП

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

22.1 Публикуване на информация за статуса на КЕП

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

22.2 Период на съхранение на прекратените КЕП в CRL

Информацията за статуса на удостоверенията включва информация за статуса на удостоверение най-малко докато изтече срока на валидност на удостоверението.

23. Базово удостоверение на УО

Базовото удостоверение „СЕП България“ АД е първо в йерархията от удостоверения на ДУУ. Удостоверението се издава от SEP Root CA удостоверяващ орган и е самоподписано. При генерацията 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“ АД има смисъла на удостоверение за квалифициран подпис по смисъла на 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 (Distinguished Name)	C	BG
	L	Sofia
	O	System for Electronic Payments /SEP Bulgaria JSC
	OU	SEP

име на поле	стойност или ограничение на стойността	
	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)	
Certificate Policies	<p>[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.30299.2.1.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=User Notice Notice Text=SEP Bulgaria JSC – accredited certification service provider</p> <p>[1,2]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.crc.bg/</p> <p>[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</p> <p>[2,2]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://e-sign.sep.bg</p>	
CRL Distribution Points	<p>[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.sep.bg/SEP_root_ca.crl</p>	
Authority Information Access	<p>[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</p>	
Basic Constraints	Subject Type=CA Path Length Constraint=None	
Issuer Alternative Names		
Subject Alternative Name		

име на поле	стойност или ограничение на стойността
Authority Key Identifier	
Subject Key Identifier	
subjectPublicKeyInfo	публичния ключ на автора и алгоритъма, с който се използва
signatureAlgorithm	sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5)
signatureValue	електронен подпис на ДУУ

24. Удостоверение на оперативния УО

Оперативният УО на „СЕП България“ АД подписва издаваните удостоверения за 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 оперативните удостоверения е 10 (десет) години. Дължината на ключа е 2048 бита за RSA алгоритъм.

Оперативното удостоверение на „СЕП България“ АД има смисъла на удостоверения за квалифициран подпис по смисъла на чл. 33. (1) т.2 от ЗЕДЕП.

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

Профил на удостоверението на SEP QES 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 (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	SEP QES
	CN	SEP QES CA

име на поле	стойност или ограничение на стойността
	Street bul.Shipchenski prohod 18
Key Usage	Certificate Signing, Off-line CRL Signing, CRL Signing (06)
Enhanced Key Usage	
Certificate Policies	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.30299.2.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text=SEP QES CA [1,2]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://e-sign.sep.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
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	публичния ключ на автора и алгоритъма, с който се използва
signatureAlgorithm	sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5)
signatureValue	електронен подпис на ДУУ

25. Потребителски удостоверения

Потребителските удостоверения 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.

25.1 Профил на SEP Qualified Private

Удостоверението за КЕП, SEP Qualified Private служи за потвърждаване на самоличността на лице при участие в електронен обмен, като Web-базирани приложения, подписване на електронни документи и/или договори, банкови трансакции 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 SEP Qualified Private 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	bul.Shipchenski prohod 18
	L	Sofia
	O	System for Electronic Payments /SEP Bulgaria JSC
	OU	SEP QES
	CN	SEP 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)	EГNxxxxxxx[EГН/ЛНЧ/ггммдд на титуляра]
	*E	e-mail адрес 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=1.3.6.1.4.1.30299.2.1.1 [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://e-sign.sep.bg
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.sep.bg/SEP_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
subjectPublicKeyInfo	публичният ключ на титуляра/автора и алгоритъма, 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

25.2 Профил на SEP Qualified Organization

Удостоверението за КЕП SEP Qualified Organization служи за потвърждаване на самоличността, съответно на идентичността, на автора и на титуляра при участие в електронен обмен, като Web-базиран приложения, подписване на електронни документи и/или договори, банкови транзакции и извършване на изявления по смисъла на ЗЕДЕП. Титулярът и авторът се различават, като автор е физическо лице, а титуляр юридическо. Авторът върши изявленията от името и за сметка на титуляра.

Профил на SEP Qualified 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

име на поле	стойност или ограничение на стойността	
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	bul.Shipchenski prohod 18
	L	Sofia
	O	System for Electronic Payments /SEP Bulgaria JSC
	OU	SEP QES
	CN	SEP 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	EIKxxxxxxxx[EИК на титуляра] / друг идентификатор
	*E	служебен e-mail адрес на автора за водене на кореспонденция от името на титуляра
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)	
Certificate Policies	<p>[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.30299.2.1.2 [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</p> <p>[1,2]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://e-sign.sep.bg</p>	

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/SEP_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
subjectPublicKeyInfo	публичният ключ на титуляра/автора и алгоритъма, 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 КЕП е само и единствено за провеждане на тестове.

25.3 Профил на SEP Qualified Profession

Удостоверението за електронен подпис, SEP Qualified Profession служи за потвърждаване на самоличност и професионална принадлежност на 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. Лицето е титуляр и автор на изявленията. Изявленията са от името и за сметка на лицето.

Профил на SEP Qualified 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	bul.Shipchenski prohod 18
	L	Sofia

име на поле	стойност или ограничение на стойността	
	O	System for Electronic Payments /SEP Bulgaria JSC
	OU	SEP QES
	CN	SEP 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)	EGNxxxxxxxx[EГН/ЛНЧ/ггммдд на автора]/ друг идентификатор
	*CN	Име/псевдоним на автора
	T	позиция на автора/овластяване
	OU	EIKxxxxxxxx[EИК на титуляра] / друг идентификатор
*E	служебен e-mail адрес на автора за водене на кореспонденция от името на титуляра	
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)	
Certificate Policies	<p>[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.30299.2.1.3 [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</p> <p>[1,2]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://e-sign.sep.bg</p>	

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/SEP_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
subjectPublicKeyInfo	публичният ключ на титуляра/автора и алгоритъма, 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 QES Profession. Предназначението на такива КЕП е само и единствено за провеждане на тестове.

26. Идентификатор на подписващия алгоритъм

Полето signatureAlgorithm съдържа идентификатор на алгоритъма използван за създаване на електронен подпис от УО. „СЕП България“ АД използва следните алгоритми:

sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5)

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

27. 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.

28. Профил на списъка с прекратени удостоверения

Списъкът с прекратени удостоверения (CRL) съдържа следните полета:

- tbsCertList: съдържа информация за прекратените удостоверения;
- signatureAlgorithm: идентификатор на алгоритъма използван за подписване на списъка с прекратени удостоверения;
- signatureValue: електронния подпис на УО, издал списъка с прекратени удостоверения.

Смисълът на `signatureAlgorithm` и `signatureValue` е като при 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“ АД, 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 от прекратени удостоверения като полето е празно ако няма прекратени удостоверения. Информацията се съдържа в следните подплетта:
 - `userCertificate`: сериен номер на прекратеното удостоверение;
 - `revocationDate`: дата на която е прекратено удостоверението;
 - `crEntryExtensions`: допълнителна информация за прекратеното удостоверение.
- `crExtensions`: допълнителна информация относно CRL;
- `AuthorityKeyIdentifier`: позволява да се идентифицира публичния ключ съответстващ за 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 с прекратени удостоверения:

поле	стойност, подполе стойност	
<code>version</code>	Version 2	
<code>issuer (Distinguished Name)</code>	C	BG
	S	Sofia
	L	Sofia
	O	System for Electronic Payments /SEP Bulgaria JSC
	OU	SEP
	CN	{SEP Root CA, SEP QES CA}
	Street	bul.Shipchenski prohod 18

	E	esign@SEP.bg
thisUpdate	дата на издаване на списъка с прекратени удостоверения	
nextUpdate	дата на издаване на следващ списък с прекратени удостоверения	
signature	електронен подпис на издателя на списъка с прекратени удостоверения	
CRLNumber	число от монотонно нарастваща редица	
AuthorityKeyIdentifier		
revokedCertificates	userCertificate	сериен номер
	revocationDate	дата на поставяне в списъка с прекратени удостоверения
	crlEntryExtensions	{unspecified, keyCompromise, cACompromise, affiliationChanged, superseded, cessationOfOperation, certificateHold, removeFromCRL, privilegeWithdrawn}

29. 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 според 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)	
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

име на поле	стойност или ограничение на стойността
	E esign@sep.bg
Key Usage	digitalSignature, nonRepudiation
Enhanced Key Usage	timeStamping
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	URL: http://tsa.sep.bg
Authority Key Identifier	
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

30. OCSP профил

Услугата по проверка статуса на издадените удостоверения, „СЕП България“ АД предоставя освен чрез достъп по CRL и чрез On-line 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“ АД.

Удостоверението, с което се проверява On-line отговора, се издава от SEP QES CA. SEP QES CA подписва със своя частен ключ, резултата от проверката преди да го изпрати на крайния потребител. OCSP удостоверението е съгласно RFC 3280 а заявките и отговорите към SEP QES CA, за удостоверяване на статуса на издадено от „СЕП България“ АД удостоверение, са съгласно RFC 2560.

Профил на удостоверението на SEP 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	bul.Shipchenski prohod 18
	L	Sofia
	O	System for Electronic Payments /SEP Bulgaria JSC
	OU	SEP QES
	CN	SEP QES CA
	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	SEP QES
	CN	SEP OCSP
	E	esign@sep.bg
Key Usage	digitalSignature, nonRepudiation	
Enhanced Usage Key	OCSPSigning	
Certificate Policies	<p>[1] Certificate Policy: Policy Identifier=1.3.6.1.4.1.30299.2.1.6 [1,1]Policy Qualifier Info: Policy Qualifier Id=User Notice explicitText: SEP OCSP [1,2]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://e-sign.sep.bg</p>	
CRL Distribution Points	<p>[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.sep.bg/SEP_QES_CA.crl</p>	

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	сА: no pathLenConstraint: 0
Issuer Alternative Names	
Subject Alternative Name	
Authority Identifier Key	
Subject Identifier Key	
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

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