

## „СЕП България“ АД

---

София, 1784, бул. „Цариградско шосе“ № 135  
тел.: +359 700 18283, e-mail: [esign@mobisafe.bg](mailto:esign@mobisafe.bg)

# Наръчник на потребителя

## Практика при предоставяне на удостоверителни услуги

Версия: 4.2

Дата на публикуване: 30.03.2009 г.

## Съдържание

<b>1</b>	<b>Въведение</b> .....	<b>10</b>
<b>1.1</b>	<b>Общ преглед</b> .....	<b>10</b>
<b>1.2</b>	<b>Име и идентификация на документа</b> .....	<b>11</b>
<b>1.3</b>	<b>Страни в удостоверителния процес</b> .....	<b>11</b>
<b>1.3.1</b>	<b>Характер и съдържание на документите</b> .....	<b>11</b>
<b>1.3.1.1</b>	<b>Наръчник на потребителя</b> .....	<b>11</b>
<b>1.3.1.2</b>	<b>Характер на „Наръчника на потребителя“</b> .....	<b>12</b>
<b>1.3.1.3</b>	<b>Одобряване на „Наръчника на потребителя“</b> .....	<b>12</b>
<b>1.3.1.4</b>	<b>Детайлност и съдържание</b> .....	<b>12</b>
<b>1.3.2</b>	<b>Удостоверяващи органи</b> .....	<b>12</b>
<b>1.3.2.1</b>	<b>Базов удостоверяващ орган</b> .....	<b>12</b>
<b>1.3.2.2</b>	<b>Оперативен удостоверяващ орган</b> .....	<b>12</b>
<b>1.3.2.3</b>	<b>Удостоверяване на време (TimeStamp)</b> .....	<b>13</b>
<b>1.3.2.4</b>	<b>On-line проверка статуса на УЕП (OCSP)</b> .....	<b>13</b>
<b>1.3.3</b>	<b>Регистриращи органи</b> .....	<b>13</b>
<b>1.3.4</b>	<b>Крайни потребители</b> .....	<b>14</b>
<b>1.3.4.1</b>	<b>Автор</b> .....	<b>15</b>
<b>1.3.4.2</b>	<b>Титуляр</b> .....	<b>15</b>
<b>1.3.4.3</b>	<b>Разграничаване на титуляр/автор</b> .....	<b>15</b>
<b>1.3.4.4</b>	<b>Доверяващи се страни</b> .....	<b>15</b>
<b>1.3.5</b>	<b>Публичен регистър</b> .....	<b>15</b>
<b>1.4</b>	<b>Приложна сфера на УЕП</b> .....	<b>16</b>
<b>1.4.1</b>	<b>Подходяща употреба</b> .....	<b>16</b>
<b>1.4.1.1</b>	<b>Удостоверения за универсален електронен подпис</b> .....	<b>16</b>
<b>1.4.1.2</b>	<b>Специализирани удостоверения за електронен подпис</b> .....	<b>17</b>
<b>1.4.2</b>	<b>Използвани приложения</b> .....	<b>17</b>
<b>1.4.3</b>	<b>Забрана за употреба</b> .....	<b>17</b>
<b>1.5</b>	<b>Администриране на документа</b> .....	<b>18</b>
<b>1.6</b>	<b>Ползвани източници</b> .....	<b>18</b>
<b>1.7</b>	<b>Нормативна уредба</b> .....	<b>18</b>
<b>1.8</b>	<b>Стандарти</b> .....	<b>18</b>
<b>1.9</b>	<b>Определения и съкращения</b> .....	<b>19</b>
<b>1.9.1</b>	<b>Определения</b> .....	<b>19</b>
<b>1.9.2</b>	<b>Съкращения</b> .....	<b>20</b>
<b>2</b>	<b>Публичен регистър</b> .....	<b>21</b>
<b>2.1</b>	<b>Публикувана информация</b> .....	<b>21</b>
<b>2.2</b>	<b>Периодичност на публикуване</b> .....	<b>21</b>
<b>2.3</b>	<b>Достъп до публичния регистър</b> .....	<b>21</b>
<b>2.4</b>	<b>Пазене на публичния регистър</b> .....	<b>22</b>
<b>3</b>	<b>Идентификация и автентификация</b> .....	<b>23</b>
<b>3.1</b>	<b>Използвани имена</b> .....	<b>23</b>
<b>3.1.1</b>	<b>Тип на имената</b> .....	<b>23</b>

3.1.2	Смисъл на имена .....	23
3.1.3	Анонимност и използване на псевдоним .....	24
3.1.4	Правила за интерпретиране на различните именни форми .....	24
3.1.5	Уникалност на имената .....	24
3.1.6	Запазена марка .....	25
3.2	Идентификация и автентификация при първоначална регистрация ....	25
3.2.1	Методи за доказване контрола над частния ключ .....	25
3.2.2	Проверка на идентичността на юридически лица .....	26
3.2.3	Проверка самоличността на физически лица .....	27
3.2.4	Непроверена информация .....	28
3.2.5	Потвърждаване на представителството .....	28
3.3	Идентификация и автентификация при подновяване или модификация на удостоверение .....	29
3.3.1	Подновяване.....	29
3.3.1.1	Подновяване на ключ – (Rekey) .....	29
3.3.1.2	Подновяване на удостоверение – (Renew).....	29
3.3.2	Модификация на удостоверение – (Update).....	30
3.4	Идентификация и автентификация при прекратяване .....	30
3.5	Идентификация и автентификация при спиране и възобновяване.....	30
3.5.1	Спиране на удостоверение.....	30
3.5.2	Възобновяване на удостоверение .....	31
4	Жизнен цикъл на удостоверенията за електронен подпис .....	32
4.1	Подаване на искане.....	32
4.1.1	Искане за първоначална регистрация .....	33
4.1.2	Искане за издаване на удостоверение за електронен подпис ....	33
4.1.3	Искане за подновяване или модификация на удостоверение за електронен подпис.....	34
4.1.4	Искане на прекратяване или спиране .....	35
4.1.5	Искане за възобновяване .....	35
4.2	Обработка на подадените искания .....	36
4.2.1	Обработка на исканията от Регистриращ орган .....	37
4.2.2	Обработка на исканията от Удостоверяващ орган .....	37
4.3	Издаване на удостоверение за електронен подпис.....	38
4.3.1	Забавяне при издаване на УЕП .....	38
4.3.2	Отказ за издаване на УЕП.....	39
4.4	Приемане на удостоверение за електронен подпис.....	39
4.5	Използване на удостоверението и ключовата двойка .....	40
4.6	Подновяване.....	40
4.7	Модификация на удостоверение.....	41
4.8	Прекратяване на удостоверение.....	42
4.8.1	Обстоятелства, при които се допуска прекратяване .....	42
4.8.2	Кой може да иска прекратяване на удостоверение .....	43
4.8.3	Процедура за прекратяване на удостоверение .....	44
4.8.4	Необходимост от проверка статуса на удостоверението.....	45
4.8.5	Периодичност на публикуване на СПУ .....	46
4.8.6	On-line проверка на валидността на удостоверения .....	46

4.8.7	Необходимост от проверка валидността On-line .....	46
4.9	Спиране и възобновяване на удостоверение .....	47
4.9.1	Обстоятелства при спиране на удостоверение.....	47
4.9.2	Обстоятелства при възобновяване на удостоверение .....	47
4.9.3	Кой може да иска спиране и възобновяване на удостоверение .....	47
4.9.3.1	Основания за спиране на удостоверение .....	47
4.9.3.2	Основания за възобновяване на удостоверение .....	47
4.9.4	Процедура по спиране и възобновяване на удостоверение .....	48
4.9.4.1	Процедура по спиране на действието на удостоверение .....	48
4.9.4.2	Процедура за възобновяване на действието на удостоверение .....	48
4.9.5	Ограничения на периода на спиране.....	49
4.10	Услуги по валидация .....	49
4.10.1	Експлоатационни характеристики .....	49
4.10.2	Достъпност на услугата .....	49
4.11	Удостоверяване на време.....	50
4.11.1	Процедура по предоставяне на услугата удостоверяване на време .....	50
4.11.2	Уверение за трети страни.....	50
4.12	Прекратяване ползване на удостоверителни услуги .....	50
5	Съоръжения, ръководство и оперативни контроли .....	51
5.1	Съоръжения на доставчика.....	51
5.1.1	Физическа сигурност УО и базов РО .....	51
5.1.1.1	Местоположение и конструкция .....	51
5.1.1.2	Физически достъп.....	51
5.1.1.3	Електрозахранване и климатизация .....	52
5.1.1.4	Наводнение.....	52
5.1.1.5	Противопожарни мерки .....	52
5.1.1.6	Съхраняване на носители .....	52
5.1.1.7	Депозирание на отпадъци .....	52
5.1.1.8	Съхранение на резервните копия .....	52
5.1.2	Съоръжения на РО .....	52
5.1.2.1	Местоположение и конструкция .....	52
5.1.2.2	Физически достъп.....	52
5.1.2.3	Електрозахранване и климатизация .....	53
5.1.2.4	Наводнение.....	53
5.1.2.5	Противопожарни мерки .....	53
5.1.2.6	Съхраняване на носители .....	53
5.1.2.7	Депозирание на отпадъци .....	53
5.1.2.8	Съхранение на резервните копия .....	53
5.1.3	Сигурност на титуляра/автора.....	53
5.2	Контрол на процедурите .....	53
5.2.1	Доверени длъжности.....	53
5.2.2	Разделяне на задълженията .....	54
5.2.3	Идентификация и автентификация за доверени длъжности .....	54

<b>5.3</b>	<b>Управление на персонала</b> .....	<b>54</b>
5.3.1	Квалификация и опит.....	54
5.3.2	Проверка на знанията .....	54
5.3.3	Обучение на персонала.....	55
5.3.4	Непрекъснатост на обучението.....	55
5.3.5	Дисциплинарни мерки .....	55
5.3.6	Договори с външни лица.....	55
5.3.7	Документи предоставяни на персонала .....	55
<b>5.4</b>	<b>Водене на записи и преглеждане на журналите</b> .....	<b>56</b>
5.4.1	Тип на записваните събития .....	56
5.4.2	Преглед на журналите .....	57
5.4.3	Период на съхранение .....	57
5.4.4	Защита на журналните файлове.....	57
5.4.5	Архивиране на журналните файлове .....	58
5.4.6	Известяване за събития .....	58
5.4.7	Оценка на уязвимостите .....	58
<b>5.5</b>	<b>Архивиране на записите</b> .....	<b>58</b>
5.5.1	Типове архивни данни .....	59
5.5.2	Честота на архивиране.....	59
5.5.3	Период на съхраняване в архив .....	59
5.5.4	Защита на архива .....	59
5.5.5	Резервни копия на архива – процедура .....	60
5.5.6	Изискване за удостоверено време за записите.....	60
5.5.7	Процедура за проверка на архивираната информация .....	60
<b>5.6</b>	<b>Смяна на ключовете</b> .....	<b>61</b>
<b>5.7</b>	<b>Компрометиране и възстановяване след бедствия и аварии</b> .....	<b>61</b>
5.7.1	Реакция при нарушения на сигурността.....	61
5.7.2	Щети по компютърни ресурси, софтуер и/или данни.....	61
5.7.3	Компрометиране на частния ключ на УО .....	63
5.7.4	Продължаване на дейностите след възстановяване от бедствия и авария .....	63
<b>5.8</b>	<b>Прекратяване или прехвърляне на дейността</b> .....	<b>64</b>
5.8.1	Прекратяване или прехвърляне на дейността на УО .....	64
5.8.2	Прекратяване или прехвърляне на дейността на РО .....	64
<b>6</b>	<b>Техническа и технологична сигурност</b> .....	<b>65</b>
<b>6.1</b>	<b>Генериране и инсталиране на ключови двойки</b> .....	<b>65</b>
6.1.1	Генериране на ключови двойки.....	65
6.1.1.1	Генериране на ключовете на SEP Root CA .....	66
6.1.1.2	Смяна на ключовете на SEP Root CA .....	66
6.1.1.3	Смяна на ключовете на оперативния УО на ДУУ .....	66
6.1.2	Предоставяне на частния ключ на автора .....	66
6.1.3	Предоставяне на публичния ключ до УО.....	66
6.1.4	Предоставяне на публичния ключ на УО до доверяващите се страни .....	67
6.1.5	Дължина на ключовете .....	67
6.1.6	Параметри на генерация на публичния ключ и проверка за качество.....	67
<b>6.2</b>	<b>Защита на частния ключ</b> .....	<b>67</b>

6.2.1	Криптографски модули – стандарти и контроли .....	68
6.2.2	Достъп до частния ключ на доставчика .....	68
6.2.3	Резервни копия на частния ключ .....	68
6.2.4	Архивиране на частния ключ .....	68
6.2.5	Трансфер на частния ключ от и към криптомодула .....	68
6.2.6	Съхраняване на частния ключ в криптомодула .....	68
6.2.7	Активиране на частния ключ .....	68
6.2.8	Деактивиране на частния ключ .....	69
6.2.9	Унищожаване на частния ключ .....	69
6.2.10	Сертификация на криптомодула .....	69
6.3	Други аспекти от управлението на ключовете .....	69
6.3.1	Архивиране на публичния ключ .....	69
6.3.2	Период на валидност на удостоверенията и използване на ключовете .....	69
6.4	Данни за активиране .....	70
6.5	Управление на компютърната сигурност .....	70
6.5.1	Технически изисквания .....	70
6.5.2	Оценка на сигурността .....	70
6.6	Технически контроли .....	70
6.6.1	Разработка на информационна система .....	70
6.6.2	Управление контролите за информационна сигурност .....	70
6.7	Мрежова сигурност .....	71
7	Профили на удостоверения, списък със спрени и прекратени удостоверения и OCSP .....	72
7.1	Профили на удостоверенията .....	72
7.1.1	Съдържание на удостоверението .....	72
7.1.1.1	Базови полета .....	72
7.1.1.2	Стандартни разширения .....	74
7.1.1.3	Идентификаторите на обекти .....	75
7.1.2	Базово удостоверение на УО .....	76
7.1.3	Удостоверение на оперативния УО .....	77
7.1.4	Потребителски удостоверения .....	79
7.1.4.1	Профил на MobiSafe Private .....	79
7.1.4.2	Профил на MobiSafe Organization .....	81
7.1.4.3	Профил на MobiSafe Profession .....	83
7.1.5	Идентификатор на подписващия алгоритъм .....	85
7.1.6	Поле с електронен подпис .....	86
7.2	Профил на списъка със спрени и прекратени удостоверения .....	86
7.3	MobiSafe TSA профил .....	87
7.4	OCSP профил .....	89
8	Проверка и контрол на дейността .....	91
8.1	Честота и обстоятелства на проверките .....	91
8.2	Идентификация и квалификация на проверяващите .....	91
8.3	Избягване конфликт на интереси .....	91
8.4	Обхват и детайлност на проверките .....	91

<b>8.5</b>	<b>Предприемане на действия за отстраняване на недостатъците .....</b>	<b>92</b>
<b>8.6</b>	<b>Съобщаване на резултатите .....</b>	<b>92</b>
<b>9</b>	<b>Търговски и правни условия .....</b>	<b>93</b>
<b>9.1</b>	<b>Цени на удостоверителните услуги .....</b>	<b>93</b>
9.1.1	Цени на услуги .....	93
9.1.2	Възстановяване на суми .....	93
<b>9.2</b>	<b>Финансова отговорност .....</b>	<b>93</b>
9.2.1	Застраховка на дейността .....	93
9.2.2	Застрахователно покритие за крайните потребители .....	94
<b>9.3</b>	<b>Конфиденциалност на информацията .....</b>	<b>94</b>
9.3.1	Обхват на конфиденциалната информация .....	94
9.3.2	Информация извън обхвата на конфиденциалната информация .....	95
9.3.3	Задължение за пазене на конфиденциалната информация .....	95
<b>9.4</b>	<b>Защита на личните данни .....</b>	<b>95</b>
<b>9.5</b>	<b>Права върху интелектуалната собственост .....</b>	<b>96</b>
<b>9.6</b>	<b>Статут и гаранции .....</b>	<b>96</b>
9.6.1	Статут и гаранции на „СЕП България“ АД .....	96
9.6.2	Статут и гаранции на регистриращите органи .....	96
9.6.3	Статут и гаранции на титуляра/автора .....	97
9.6.4	Статут и гаранции на доверяващата се страна .....	97
<b>9.7</b>	<b>Ограничаване на отговорността .....</b>	<b>98</b>
<b>9.8</b>	<b>Ограничение на отговорността .....</b>	<b>98</b>
<b>9.9</b>	<b>Обезщетения и компенсации .....</b>	<b>99</b>
<b>9.10</b>	<b>Срок на действие и прекратяване на действието .....</b>	<b>99</b>
9.10.1	Срок на действие .....	99
9.10.2	Прекратяване действието на ППУУ .....	99
9.10.3	Последствия от прекратяване действието на ППУУ .....	99
<b>9.11</b>	<b>Уведомяване и комуникация .....</b>	<b>99</b>
<b>9.12</b>	<b>Изменения и допълнения .....</b>	<b>100</b>
<b>9.13</b>	<b>Разрешаване на спорове .....</b>	<b>100</b>
<b>9.14</b>	<b>Приложимо законодателство .....</b>	<b>101</b>
<b>9.15</b>	<b>Съответствие със законовите изисквания .....</b>	<b>101</b>
<b>9.16</b>	<b>Допълнителни разпоредби .....</b>	<b>101</b>
9.16.1	Правоприемство .....	101
9.16.2	Отделяне на условията .....	101
9.16.3	Тълкуване .....	101
9.16.4	Отказ от изпълнение .....	101
9.16.5	Форсмажор .....	101
9.16.6	Юрисдикция .....	102

Вие можете да изпращате Вашите коментари по тази „Практика при предоставяне на удостоверителни услуги“ на e-mail адрес или да ги изпратите по пощата на адрес:

„СЕП България“ АД  
Гр. София, 1784,  
бул. „Цариградско шосе“ № 135  
тел.: + 359 700 18283  
e-mail: [esign@mobisafe.bg](mailto:esign@mobisafe.bg)

“СЕП България” АД  
гр. София, 1784,  
бул. „Цариградско шосе“ № 135  
Тел.: + 359 700 18283  
e-mail: [esign@mobisafe.bg](mailto:esign@mobisafe.bg)  
БУЛСТАТ: 131107204

Авторското право върху настоящата „Практика при предоставяне на удостоверителни услуги“ принадлежи на “СЕП България” АД.  
Всяко използване на цялата или на част от „Практика при предоставяне на удостоверителни услуги“, извършено без съгласието на “СЕП България” АД, представлява нарушение на Закона за авторското право и сродните му права.

## 1 Въведение

Практика 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 „Политика 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.

Практиката съдържа важна информация за титулярите/авторите на УЕП 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 УЕП, процедурите по проверка на идентичността съответно на самоличността на титуляр.автор, областта на приложение на УЕП.

Политиката определя нивото на доверие в издаваните УЕП 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 УЕП на физически, юридически лица и лица упражняващи свободни професии. Приложимостта на тези УЕП и отговорностите на получателите на УЕП, ДУУ и доверяващите се страни.

Настоящата „Практика при предоставяне на удостоверителни услуги“ е разработена 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.

### 1.1 Общ преглед

Практиката при предоставяне на удостоверителни услуги е описание и основен документ 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 УЕП издавани от ДУУ – „СЕП България“ АД и удостоверението за On-line валидация. Базовия удостоверяващ орган подписва оперативния удостоверяващ орган и удостоверението за валидация на удостоверено време.

УЕП 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 УЕП.

„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.

№	ИМЕ НА ДОКУМЕНТА	ДОСТЪП
1.	Наръчник на потребителя:	публичен
	• Политика по предоставяне на удостоверителни услуги	публичен
	• Практика при предоставяне на удостоверителни услуги	публичен
2.	Правила за издаване на удостоверения, включително правилата за установяване идентичността на титуляра на универсалния електронен подпис	публичен
3.	Условия и ред за използване на универсалния електронен подпис, включително изискванията за съхраняване на частния ключ	публичен
4.	Договор за предоставяне на удостоверителни услуги	публичен
5.	Процедури за сигурност, прилагани при издаването и ползването на универсалния електронен подпис	ограничен

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

## 1.2 Име и идентификация на документа

Настоящия документ е „Практика при предоставяне на удостоверителни услуги“ на „СЕП България“ АД и е достъпен:

- В електронна форма в директорията на „СЕП България“ АД на електронен адрес <http://e-sign.mobisafe.bg>;
- На хартиен носител в регистриращите органи и офисите на „СЕП България“ АД.

## 1.3 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, титуляри/автори 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, MobiSafe CA;
- Регистриращите органи;
- Титулярите/авторите на УЕП за универсален електронен подпис;
- 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.

### 1.3.1 Характер и съдържание на документите

#### 1.3.1.1 Наръчник на потребителя

В качеството си на ДУУ „СЕП България“ АД, опериращ на територията на република България, разработва „Наръчник на потребителя“, който включва:

- „Политика по предоставяне на удостоверителни услуги“

- „Практика при предоставяне на удостоверителни услуги“

#### **1.3.1.2 Характер на „Наръчника на потребителя“**

„Наръчник на 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 за одобряване съгласно чл. 32, ал. 1, т. 2 ЗЕДЕП.

#### **1.3.1.3 Одобряване на „Наръчника на потребителя“**

„СЕП България“ АД представя пред Комисията за регулиране на съобщенията, „Наръчник на потребителя“ при всяка промяна в него. Промените се отразяват след одобрение от страна на КРС, след което се съобщават на заинтересуваните страни.

#### **1.3.1.4 Детайлност и съдържание**

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

Документа „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.

### **1.3.2 Удостоверяващи органи**

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

#### **1.3.2.1 Базов удостоверяващ орган**

SEP Root CA издава базово УЕП на себе си и оперативни УЕП 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 УЕП 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 – MobiSafe CA;
- MobiSafe TSA – удостоверението за проверка на обекти с удостоверено време (TimeStamp).

#### **1.3.2.2 Оперативен удостоверяващ орган**

Оперативен УО на „СЕП България“ АД е MobiSafe CA. Оперативния УО издава УЕП в съответствие с „Политика по предоставяне на удостоверителни услуги“ на „СЕП България“ АД на физически и/или юридически лица. Включва в издадените УЕП идентификатори на обекти, за да идентифицира издадените

удостоверения от определен тип, в съответствие с тази политика.  
Идентификаторите на обекти са:

ОБЕКТ	ИДЕНТИФИКАТОР НА УЕП/ПОЛИТИКА
<b>MobiSafe Private</b>	1.3.6.1.4.1.30299.1.1.1
<b>MobiSafe Organization</b>	1.3.6.1.4.1.30299.1.1.2
<b>MobiSafe Profession</b>	1.3.6.1.4.1.30299.1.1.3
<b>MobiSafe Server</b>	1.3.6.1.4.1.30299.1.1.4

УЕП издавани от оперативния УО съдържат идентификатор на политиката, спрямо която са издадени. Оперативният УО не издават УЕП на други УО.

### **Оперативният УО издават УЕП на потребители на удостоверения за електронен подпис.**

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

#### **1.3.2.3 Удостоверяване на време (TimeStamp)**

„СЕП България“ АД предоставя услугата по удостоверяване на време, SEP Root CA, издава удостоверение за електронен подпис, което се използва за проверка на обекти с удостоверено време. Удостоверението включва идентификатор на политика посочен в таблицата:

ОБЕКТ	ИДЕНТИФИКАТОР НА ПОЛИТИКА
<b>MobiSafe TSA</b>	1.3.6.1.4.1.30299.1.1.5

#### **1.3.2.4 On-line проверка статуса на УЕП (OCSP)**

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

ОБЕКТ	ИДЕНТИФИКАТОР НА ПОЛИТИКА
<b>MobiSafe OCSP</b>	1.3.6.1.4.1.30299.1.1.6

### **1.3.3 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 титуляра/автора и регистриране на постъпилите искания за издаване или управление на УЕП.

ДУУ издава УЕП 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 УЕП;
- Приемат, проверяват, одобряват или отхвърлят исканията за управление на УЕП;
- 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 и за сметка 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 УЕП, подновяване, спиране/възобновяване и прекратяване на УЕП. 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. РО могат да изпратят искането към съответния УО за анулиране на регистрацията на титуляра/автора и оттегляне на УЕП. Начина на проверка и необходимите документи придружаващи искането се определят от заявените УЕП.

При проверка на идентичността съответно самоличността на титуляра/автора операторите на РО пряко или непряко идентифицират лицата, на които ще се издават УЕП, 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 на потребителя на ДУУ е част от този договор.

УО на ДУУ „СЕП България“ АД делегира част от своите дейности на два типа регистриращи органи:

- Регистриращ орган (РО);
- Базов регистриращ орган (БРО).

РО регистрират исканията на крайните клиенти за всички видове дейности и УЕП или само за определена част от тях в зависимост от оторизацията, която имат от ДУУ.

БРО регистрира РО, нови УО и исканията на крайните клиенти без ограничения и определя Distinguished Name на РО. БРО се намира на територията на „СЕП България“ АД и част от инфраструктурата за предоставяне на удостоверителни услуги.

Всяко юридическо лице може да функционира, след оторизация, като РО на ДУУ – „СЕП България“ АД, стига да заяви това пред Базовия регистриращ орган и да изпълни условията произтичащи от регламентиращите документи на ДУУ.

Списък на РО, които са оторизирани от БРО на ДУУ е публичен и е достъпен чрез публичния регистър на ДУУ на адрес: <http://e-sign.mobisafe.bg> .

### **1.3.4 Крайни потребители**

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

Титуляра/автора се вписва в съответни полета на УЕП и се идентифицират от тази вписана информация.

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

Когато крайния потребител е юридическо лице то може да подава искания до ДУУ, чрез свой упълномощен представител за своите служители. Когато крайния потребител е физическо лице то трябва да подава искания до ДУУ лично.

#### **1.3.4.1 Автор**

Автор на електронното изявление е физическото лице, което в изявлението се сочи като негов извършител. Автора се идентифицира в УЕП като притежател на частния ключ, съответстващ на публичния ключ в УЕП и контролира ползването на частния ключ.

#### **1.3.4.2 Титуляр**

Титуляр на електронното изявление е лицето, от името, на което е извършено електронното изявление. Титуляра подава искане за издаване на УЕП, от свое име или от името на други лица, които упълномощава да извършват електронни изявления от негово име и сключва договор с ДУУ, носи отговорността за правилното ползване на частния ключ от автора.

#### **1.3.4.3 Разграничаване на титуляр/автор**

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

Когато УЕП 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.

#### **1.3.4.4 Доверяващи се страни**

Доверяващите се страни използват удостоверителните услуги на ДУУ, когато трябва да вземе решение зависещо от валидността на връзката между идентичността съответно самоличността на титуляра/автора и неговия публичен ключ.

Доверяващата се страна е отговорна за проверката на текущия статус на УЕП, 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 УЕП, за да провери електронен подпис, да идентифицира източника или автора на съобщение, или да изгради защитен комуникационен канал с притежателя на УЕП. Доверяващата се страна трябва да използва информацията от УЕП (идентификатор на политиката) за да определи дали определено УЕП се използва правилно и в съответствие с определена политика по предоставяне на удостоверителни услуги.

#### **1.3.5 Публичен регистър**

Публичния регистър е набор от публично достъпни каталози и директории съдържащи:

- УЕП на всички УО от инфраструктурата на ДУУ;
- УЕП на крайните потребители на удостоверителни услуги с наложени ограничения в зависимост от указанията на авторите;
- Списъците с прекратени УЕП;
- 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 само един публичен регистър, който е общ за всички УО от неговата йерархията.

Съдържанието на регистъра е достъпно на адрес: <http://e-sign.mobisafe.bg>.

## 1.4 Приложна сфера на УЕП

Удостоверението за електронен подпис, представлява форматиранни данни, които свързват титуляра/автора с публичния му ключ.

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

УЕП 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.

УЕП дава възможност на участниците в електронния обмен да докажат самоличността си.

Доверяващите се страни преценяват дали типа на УЕП 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 УЕП.

### 1.4.1 Подходяща употреба

Според тази политиката на „СЕП България“ АД се издават удостоверения за универсален електронен подпис и специализирани удостоверения за електронен подпис.

#### 1.4.1.1 Удостоверения за универсален електронен подпис

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

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

#### **MobiSafe Private удостоверение**

За доказване 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.

Изявленията са от името и за сметка на лицето.

Проверява се самоличността на лицето, което е титуляр и автор на изявленията.

#### **MobiSafe Organization удостоверение**

За доказване на самоличността, съответно на идентичността, на автора и на титуляра 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. Титуляра и автора се различават, като автора е физическо лице, а титуляра - юридическо.

Автора върши изявленията от името и за сметка на титуляра.

Проверява се самоличността, съответно на идентичността, на автора и на титуляра и правото на автора да представлява титуляра.

### **MobiSafe Profession удостоверение**

За доказване 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.

Проверява се самоличност принадлежността на лицето към съответната професионална група.

#### **1.4.1.2 Специализирани удостоверения за електронен подпис**

### **MobiSafe Server удостоверение**

За доказване на идентичността и контрола върху техническите средства от страна на титуляра, при участие в електронен обмен през Web-базирани приложения, както и за осигуряване на защитени комуникации. Титуляра носи цялата отговорност за функционирането на информационната система в автоматичен режим. Титуляра изрично упълномощава свой/и представител/ли да следят за правилно и надеждно функциониране на информационната система.

Проверява се самоличността, съответно идентичността, на представителя на титуляра и правото на представителя да управлява информационната система на титуляра.

### **1.4.2 Използвани приложения**

УЕП издадени в съответствие с политика по предоставяне на удостоверителни услуги се използват с приложения, които отговарят най-малко на следващите изисквания:

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

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

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

### **1.4.3 Забрана за употреба**

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

## 1.5 Администриране на документа

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

Данните за контакт със „СЕП България“ АД са:

Адрес: „СЕП България“ АД, гр. София, 1784,  
бул. „Цариградско шосе“ № 135  
Телефон: +359 700 18283  
Електронен адрес: [esign@mobisafe.bg](mailto:esign@mobisafe.bg)  
Интернет сайт: <http://e-sign.mobisafe.bg>

Практиката при предоставяне на удостоверителни услуги се одобрява от Комисията за регулиране на съобщенията.

## 1.6 Ползвани източници

При разработката на „Практика при предоставяне на удостоверителни услуги“ 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.

## 1.7 Нормативна уредба

При разработката на настоящата политика по предоставяне на удостоверителни услуги 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] НИАУСЕП: „Наредба за изискванията към алгоритмите за усъвършенстван електронен подпис“;
- [5] Директива: „Directive 1999/93/EC of the European Parliament and OF the Council, of 13 December 1999, on a Community framework for electronic signatures“;
- [6] 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“.

## 1.8 Стандарти

При разработката на настоящата политика по предоставяне на удостоверителни услуги 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 3647: „Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework“;
- [3] RFC 3739: „Internet X.509 Public Key Infrastructure: Qualified Certificates Profile“;
- [4] ETSI TS 101 456 V1.4.3: “Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates” technical specification (2007-05);
- [5] ETSI TS 101 862 V1.3.3: “Qualified Certificate profile” technical specification (2006-01);
- [6] ANSI X9.79: "Public Key Infrastructure (PKI) - Practices and Policy Framework";
- [7] CWA 14167-1: "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1 System Security Requirements".

## 1.9 Определения и съкращения

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

### 1.9.1 Определения

В настоящия документ са използвани следните определения:

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

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

**Доверяваща се страна:** получатели на УЕП, 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.

**Защитен механизъм за 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 да подаде искане за издаване на УЕП или да предприема други дейности свързани с промяна статуса на издадените УЕП.

**Титуляр:** титуляр на електронното изявление е лицето, от името, на което е извършено електронното изявление. Титуляра подава искане за издаване на УЕП, 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 електронен подпис:** е електронен документ, издаден и подписан от доставчик на удостоверителни услуги, който съдържа реквизитите определени в чл.24 ал.1 от ЗЕДЕП.

**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.

### 1.9.2 Съкращения

В настоящия документ са използвани следните съкращения:

SSCD	Защитен механизъм за създаване на електронен подпис
ДУУ	Доставчик на удостоверителни услуги
ЕП	Електронен подпис
УО	Удостоверяващ орган
Политика	Политика по предоставяне на удостоверителни услуги
Практика	Практика при предоставяне на удостоверителни услуги; ППУ
РО	Регистриращ орган
УД	Удостоверителна дейност
УЕП	Удостоверение за електронен подпис
УнЕП	Универсален електронен подпис
УсЕП	Усъвършенстван електронен подпис
УУ	Удостоверителни услуги
УУнЕП	Удостоверение за универсален електронен подпис
УУсЕП	Удостоверение за усъвършенстван електронен подпис
OID	Object Identifier
OCSP	Online Certificate Status Protocol
SEP ROOT	Базов удостоверяващ орган на „СЕП България“ АД
КИК	Код за идентификация на клиента

## 2 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.

### 2.1 Публикувана информация

„СЕП България“ АД публикува в регистъра информация за:

- Своите удостоверения за електронен подпис;
- Издадените удостоверения за електронен подпис;
- Отделен Списък с прекратените удостоверения;
- Наръчник на потребителя;
- Условието и реда за издаване на удостоверение, включително за правилата за установяване идентичността на титуляра на електронен подпис;
- Начина на използване на електронен подпис;
- Условието и реда за използване на електронен подпис, включително изискванията за съхраняване на частния ключ;
- Условието за достъп до удостоверението и начина на проверка на електронен подпис;
- Цената за получаване и използване на удостоверение, както и цените на останалите услуги, предоставяни от доставчика на удостоверителни услуги;
- Отговорността на доставчика на удостоверителни услуги и на титуляра на електронен подпис;
- Условието и реда, по които титулярът прави искане за прекратяване действието на електронен подпис.

### 2.2 Периодичност на публикуване

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

- Наръчник на потребителя – след одобрение от КРС;
- Списъците на спрените и прекратените удостоверения извършва автоматично или поне през 3 часа;
- При всяко издаване на удостоверение за електронен подпис за УО, РО и краен клиент;
- Данни за проведени одити – след приключването им;
- Актуална и допълнителна информация относно предоставянето на удостоверителни услуги – при необходимост.

### 2.3 Достъп до публичния регистър

„СЕП България“ АД води електронен регистър на издадените от него удостоверения с 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 или на по-късен етап. 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 на титуляра/автора;
- Адрес и уникален идентификатор на титуляра юридическо лице;
- Сериен номер на удостоверението;
- Период на валидност на удостоверението;
- Статус на удостоверението.

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

Достъпа до „Списъка със спрени и прекратени удостоверения“ не се ограничава по никакъв начин.

## 2.4 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.

## 3 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 УЕП 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 УЕП или постъпване на искане за управление на УЕП.

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

### 3.1 Използвани имена

#### 3.1.1 Тип на имената

УЕП 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 УЕП 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 електронен подпис съдържат информация както е определено в чл.24 от ЗЕДЕП. Минималната информация, която се включва е както следва:

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

Списъка с данните, които се включват в УЕП и тяхната интерпретация е в съответствие с X.509 v3 и е представена в глава 7 Профили на удостоверения, списък със спрени и прекратени удостоверения и OCSP.

#### 3.1.2 Смисъл на имена

Имената включени в потребителския Distinguished Name имат конкретен смисъл и съдържа идентифициращата информация за титуляра/автора и издателя на УЕП.

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

<b>C, Country</b>	-	страната, на чиято територия ДУУ осъществява своята на дейност;
<b>ST, State or Province</b>	-	областен град, където е седалището по регистрацията титуляра или постоянен адрес на автора;
<b>L, Location</b>	-	населено място, където е седалището по регистрацията титуляра или постоянен адрес на автора;
<b>O, Organization</b>	-	името на титуляра, който се представлява от автора идентифициран в <b>CommonName</b> ;
<b>OU, Organization Unit</b>	-	името на организационната единица на титуляра, която представлява автора идентифициран в <b>CommonName</b> ;
<b>CN, Common Name</b>	-	името на титуляра/автора или името на автора, който представлява титуляра;
<b>T, Title</b>	-	позиция или функция на автора в организацията на титуляра;
<b>UID, Unique Identifier</b>	-	за гарантиране посредством това поле, уникалността на удостоверението;
<b>PostalAddress</b>	-	адрес на титуляра;
<b>PostalCode</b>	-	пощенски код;
<b>Phone</b>	-	телефон на титуляра;

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

### 3.1.3 Анонимност и използване на псевдоним

Поради ограничения наложени от ЗЕДЕП, „СЕП България“ АД не издава анонимни УЕП и удостоверения с вписан псевдоним.

### 3.1.4 Правила за интерпретиране на различните именни форми

Интерпретацията на имената на полетата в УЕП издадени от „СЕП България“ АД е в съответствие с профилите на удостоверенията описани в глава 7 от тази практика. При създаването и интерпретирането на различните Distinguished Name се прилагат общите правила описани в точка 3.1.2.

### 3.1.5 Уникалност на имената

Потребителското Distinguished Name се предлага от титуляра/автора. Ако името съответства на общите изисквания точки 3.1.1 и 3.1.2 изпратеното предложение отначало се приема.

За да осигури уникалност на издадените УЕП, „СЕП България“ АД присвоява уникален серийен номер за всяко издадено удостоверение. Серийният номер в комбинация с Distinguished Name на титуляра/автора, 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.

### **3.1.6 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.

## **3.2 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 титуляра подава искане за издаване на УЕП и не притежава валидно УЕП издадено от „СЕП България“ АД.

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

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 титуляр желаещ ползването на удостоверителна услуга и искащ издаването на УЕП трябва, преди да му бъде издадено удостоверението да:

- Попълни регистрационна форма на интернет сайта на ДУУ или да изпрати/предостави данните необходими за издаване на УЕП;
- Генерира ключова двойка и да предостави доказателство пред РО, че контролира частния ключ;
- Предложи съдържанието на името, с което ще се идентифицира – Distinguished Name;
- 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 титуляра да бъде физически идентифициран от оператор РО. Идентификацията може да се осъществи пряко или непряко. При пряката идентификация титуляра посещава офис на РО или оператор РО посещава титуляра. При непряката идентификация оператор РО използва документи и други средства които дават същата степен на сигурност както при пряката идентификация.

### **3.2.1 Методи за доказване контрола над частния ключ**

Ако лице контролира частния ключ, когато заявява издаване на УЕП, 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 титуляра/автора съответства на частния ключ, намиращ се под изключителния контрол на титуляра/автора.

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

Частния ключ трябва да се генерира от клиентския криптомодул – SSCD например електронна криптографска карта(смайт/сим ката). Титуляра/автора може да контролира потребителския криптомодул по всяко време на генерация на ключовата двойка или модула(смайт/им картата) да се предаде на титуляра/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.

### **3.2.2 Проверка на идентичността на юридически лица**

РО изисква представянето на подходящи документи, които по категоричен начин и без никакво съмнение да потвърждават идентичността на юридическото лице, което ще 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 представляващият го или чрез упълномощено лице, като изрично посочи на кои лица - автори, иска да се издаде УЕП.

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

Проверката на идентичността на юридическото лице има за цел да докаже, че в момента на проверката лицето посочено в искането съществува и че физическото лице заявило издаването на УЕП или получаващо УЕП е упълномощено от юридическото лице да го представлява. От предоставените документи или събраните данни, трябва да стават ясни:

- Самоличността, съответно идентичността, на автора и на титуляра;
- Съществуването на юридическото лице, организация или институция;
- Правото автора да представлява юридическото лице, организация или институция.

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.

Детайлно описание на процедурата по проверка идентичността на юридическото лице е представена в „Правилата за издаване на удостоверения,

*включително правилата за установяване идентичността на титуляра на универсалния електронен подпис”.*

РО е отговорен за проверката на коректността и истинността на данните предоставени в искането за издаване на УЕП.

Ако проверката е успешна, упълномощен оператор на РО:

- Присвоява Distinguished Name на юридическото лице или одобрява името предложено в искането;
- Изпраща потвърдените данни 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 УЕП 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.

### **3.2.3 Проверка самоличността на физически лица**

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

- Самоличността на физическото лице – автор;
- Съществуването на физическото лице – автор.

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 в искането.

Детайлно описание на процедурата по проверка самоличността на физическото лице е представена в *„Правилата за издаване на удостоверения, включително правилата за установяване идентичността на титуляра на универсалния електронен подпис”.*

РО е отговорен за проверката на коректността и истинността на данните предоставени в искането за издаване на УЕП.

Ако проверката е успешна, упълномощен оператор на РО:

- Присвоява Distinguished Name на физическото лице или одобрява името предложено в искането;
- 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 УЕП 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.

### **3.2.4 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 проверява от ДУУ, може да бъде но не се ограничава само до:

- Електронен адрес за кореспонденция;
- Телефонни номера;
- Пощенски код.

Не потвърдената информация се включват в съдържанието на удостоверението на база декларация от страна на подалия искане за регистрация титуляр.

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

### **3.2.5 Потвърждаване на представителството**

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

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

От проверката на представителството става видно:

- Лицата, които имат право да представляват титуляра;
- Обема на представителната власт на всяко лице.

„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 *„Правилата за издаване на удостоверения, включително правилата за установяване идентичността на титуляра на универсалния електронен подпис“*.

РО е отговорен за проверката на коректността и истинността на данните.

### **3.3 Идентификация и автентификация при подновяване или модификация на удостоверение**

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

Автентификацията на титуляра се осъществява чрез:

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

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

#### **3.3.1 Подновяване**

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

##### **3.3.1.1 Подновяване на ключ – (Rekey)**

Подновяване на ключова двойка може да се осъществи от титуляр, който има издадено преди това удостоверение за електронен подпис. Новото удостоверение съдържа данните от предишното и нови ключова двойка, сериен номер и период на валидност.

Титуляра 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.

##### **3.3.1.2 Подновяване на удостоверение – (Renew)**

Подновяване на удостоверение може да се осъществи от титуляр, който има издадено преди това удостоверение за електронен подпис. Новото удостоверение съдържа данните от предишното и нови сериен номер и период на валидност.

Титуляра 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 нови сериен номер и период на валидност.

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

### **3.3.2 Модификация на удостоверение – (Update)**

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

При модификация на удостоверение се издава ново на базата на съществуващо, което се притежава от титуляра.

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 регистриращ орган.

Издава се ново удостоверение, съдържащо данните за 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 не потвърдена информация за титуляра. Изходното модифицирано удостоверение се прекратява.

## **3.4 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 се автентифицира чрез своя електронен подпис или предварително договорен, между него и доставчика, код за управление.

Ако титулярът 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 3.2 Идентификация и автентификация при първоначална регистрация.

## **3.5 Идентификация и автентификация при спиране и възобновяване**

### **3.5.1 Спиране на удостоверение**

Искането за спиране може да се подаде от:

- Титуляра на удостоверението за електронен подпис;
- Комисията за регулиране на съобщенията;
- Други държавни органи, определени със закон.

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.

### **3.5.2 Възобновяване на удостоверение**

Искането за възобновяване може да се подаде от:

- Титуляра 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, подалия 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 точка 3.2 Идентификация и автентификация при първоначална регистрация.

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

## 4 Жизнен цикъл на удостоверенията за електронен подпис

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 УЕП, подновяване на УЕП, модификация на УЕП, спиране и възобновяване на УЕП и прекратяване на УЕП.

Всяка процедура стартира с подаване на искане от титуляра. 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 и най-вече с данните за идентичността съответно самоличността на титуляра/автора.

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

### 4.1 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 регистриращ орган.

Исканията се подават в електронна или хартиена форма. Хартиената форма изисква да се попълнят необходимите формуляри и се предоставят на оператор регистриращ орган. 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 HTTP, 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 УЕП;
- Подновяване на УЕП;
- Модификация на УЕП;
- Спиране на УЕП;
- Възобновяване на УЕП;
- Прекратяване на УЕП.

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 регистриращ орган.

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

#### **Оператора 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 УЕП след първоначална регистрация и постъпване на искане за издаване на УЕП, подновяване на УЕП или модификация на УЕП.

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

#### **4.1.1 Искане за първоначална регистрация**

Искането за регистрация се подава от титуляра или негов пълномощник, ако титулярът е юридическо лице, 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, някои 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.

#### **4.1.2 Искане за издаване на удостоверение за електронен подпис**

Искането за издаване на удостоверение за електронен подпис се подава от титуляра потребител. Когато титулярът е юридическо лице, искането изхожда от представляващият 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 електронен подпис и броя автори и включва:

- Пълното име на титуляра потребител на удостоверителна услуга;
- 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 електронен подпис;
- 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 УЕП, някои от посочената информация може да не бъде включена в искането за издаване на УЕП.

Необходимите данни и документи са посочени в *„Правилата за издаване на удостоверения, включително правилата за установяване идентичността на титуляра на универсалния електронен подпис“* и на интернет адрес

<http://e-sign.mobisafe.bg>.

При налична регистрация и валидно УЕП на титуляра, част или всички данните могат да се автентифицират чрез електронен подпис за останалите данни, титуляра представя оригинални документи пред оператор регистриращ орган.

Оператор регистриращ орган проверява:

- Представените данни и придружаващи документи;
- Идентичността съответно самоличността на титуляра/автора;
- Потвърждава данните от искането за издаване на УЕП;

след което предава искането на УО на ДУУ за обработка.

#### **4.1.3 Искане за подновяване или модификация на удостоверение за електронен подпис**

Искането за подновяване или модифициране на удостоверение за електронен подпис се подава от титуляра или негов пълномощник, ако титулярът е юридическо лице.

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

Информацията, която се съдържа в искането трябва да съдържа:

- Distinguished Name на титуляра подал искането;
- Distinguished Name на УЕП, за което е подадени искането;
- Тип на УЕП, за което е подадено искането;
- Нов публичен ключ или искане за генерация на такъв от ДУУ;
- Име и парола зададени при първоначална регистрация на титуляра;
- 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 в *„Правилата за издаване на удостоверения, включително правилата за установяване идентичността на титуляра на универсалния електронен подпис“* и на интернет адрес <http://e-sign.mobisafe.bg>.

При налична регистрация и валидно УЕП на титуляра, част или всички данните могат да се автентифицират чрез електронен подпис за останалите данни, титуляра представя оригинални документи пред оператор регистриращ орган.

Оператор регистриращ орган проверява:

- Представените данни и придружаващи документи;
- Идентичността съответно самоличността на титуляра/автора;
- Потвърждава данните от искането за подновяване или модифициране на УЕП;

след което предава искането на УО на ДУУ за последваща обработка.

#### **4.1.4 Искане на прекратяване или спиране**

Искането за прекратяване или спиране на удостоверение за електронен подпис се подава от автора или титуляра или пълномощник на титуляра, ако той е юридическо лице.

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

Информацията, която се съдържа в искането трябва да съдържа:

- Distinguished Name на титуляра подал искането;
- Списък с удостоверенията, които да се прекратят или спрат, съдържащ сериен номер и причина за прекратяване;
- Име и парола или код за управление, зададени при първоначална регистрация на титуляра;
- 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 в *„Правилата за издаване на удостоверения, включително правилата за установяване идентичността на титуляра на универсалния електронен подпис“* и на интернет адрес <http://e-sign.mobisafe.bg>.

При налична регистрация и валидно УЕП на титуляра, част или всички данните могат да се автентифицират чрез електронен подпис за останалите данни, титуляра представя оригинални документи пред оператор регистриращ орган.

Оператор регистриращ орган проверява:

- Представените данни и придружаващи документи;
- Идентичността съответно самоличността на титуляра/автора при прекратяване на удостоверение за електронен подпис;
- Потвърждава данните от искането за прекратяване или спиране на УЕП;

след което предава искането на УО на ДУУ за последваща обработка.

#### **4.1.5 Искане за възобновяване**

Искането за възобновяване на удостоверение за електронен подпис се подава от титуляра или негов пълномощник, ако титулярът е юридическо лице.

Титуляра на удостоверението за електронен подпис, 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 трябва да съдържа:

- Distinguished Name на титуляра подал искането;
- Декларация, че 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 в „Правилата за издаване на удостоверения, включително правилата за установяване идентичността на титуляра на универсалния електронен подпис“ и на интернет адрес <http://e-sign.mobisafe.bg>.

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

Оператор регистриращ орган 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 УЕП;

след което предава искането на УО на ДУУ за последваща обработка.

## 4.2 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.

### On-line искания

On-line исканията се приемат през портала на ДУУ на адрес <https://e-sign.mobisafe.bg>. Титуляра или негов пълномощник, ако титулярът е юридическо лице, 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 удостоверителна услуга. Ако е необходимо в зависимост от следваната процедура се посочва регистриращ орган пред който ще се представят допълнителните данни и документи за получаване на удостоверителната услуга.

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

Искането се обработва от оператор регистриращ орган, 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 удостоверителната услуга.

### **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 регистриращ орган. Off-Line искане имаме и когато допълнителните данни и документи за получаване на удостоверителната услуга се изпратят по сигурен начин до РО на ДУУ. Проверката на документите и лицата се осъществява според *„Правилата за издаване на удостоверения, включително правилата за установяване идентичността на титуляра на универсалния електронен подпис“*.

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

#### **4.2.1 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:

- Оператора получава искането в електронна форма или на хартия;
- Оператора 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, оператора 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;
- При издаване на удостоверение, представя за одобрение и приемане УЕП на титуляра/автора преди да се публикува;
- Води записи за процедурата в базата данни и системните журнали;
- Комплектува и изпраща за съхранение хартиените документи до УО, след приключване на процедурата.

#### **4.2.2 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.

### 4.3 Издаване на удостоверение за електронен подпис

При получаване на одобрено искане за издаване, УО издава удостоверение за електронен подпис. Удостоверението се смята за валидно от момента на приемане от страна на титуляра/автора. Периода на валидност на издаденото удостоверение зависи от неговия тип, и е както е посочено в таблицата:

ТИП УДОСТОВЕРЕНИЕ	ПЕРИОД НА ВАЛИДНОСТ
<b>MobiSafe Private</b>	3 години
<b>MobiSafe Organization</b>	3 години
<b>MobiSafe Profession</b>	3 години
<b>MobiSafe Server</b>	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 криптомодул;
- Качеството на публичните ключове, генерирани от УО 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 УЕП и го представя On-line или чрез РО, на титуляра/автора за одобрение. Удостоверението не се публикува в публичния регистър, докато не се получи потвърждение от титуляра/автора за приемане на удостоверението.

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

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

„СЕП България“ АД публикува удостоверението в публичната си директория след приемането му от страна на титуляра/автора.

Публикуването на УЕП 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 УЕП.

#### 4.3.1 Забавяне при издаване на УЕП

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 от 7 дни.

Периода 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 УЕП и са свързани с необходимостта от уточняване на данните вписвани в УЕП. В този случай е възможно да се увеличи периода на изчакване над посочената по-горе стойност.

#### 4.3.2 Отказ за издаване на УЕП

Отказ за издаване може да се получи, когато:

- Титуляра/автора не може да докаже своите права по отношение на поисканото Distinguished Name;
- При съмнения или несъмнени доказателства, че титуляра/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 УЕП;
- По други причини.

Информацията за отказа за издаване на УЕП и причините свързани с този отказ се изпращан на заявителя. Лицето, на което е отказано да му бъде издадено УЕП може да подаде жалба в 7 дневен срок, както е посочено в точка 9.13 Разрешаване на спорове.

### 4.4 Приемане на удостоверение за електронен подпис

УЕП може да се приеме от титуляра/автора по време на On-line процедурата по регистрация/издаване или подновяване след генериране на УЕП и преди да се публикува. На титуляра/автора се представя съдържанието на генерираното удостоверение. Титуляра/автора проверява съдържанието и коректността на данните.

Ако титуляра притежава валидно удостоверение за електронен подпис, различно от представеното за приемане, приемането на съдържанието на удостоверението може да се потвърди чрез електронен подпис.

Ако титуляра не притежава удостоверение за електронен подпис, приемането на съдържанието на удостоверението се потвърждава чрез саморъчен подпис под хартиен формуляр.

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

След издаване, удостоверението се получава от титуляра/автора. Автора 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 титуляра/автора да приеме издаденото удостоверение.

Удостоверението се смята за прието ако в рамките на 7 седем дни след получаването на удостоверението не е постъпило искане за прекратяване.

**Ако удостоверението не е ясно отхвърлено в 7 дневен срок от представянето или получаването му, то удостоверението се смята за прието.**

Всяко прието удостоверение е публикувано в електронния публичен регистър на „СЕП България“ АД.

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

**С приемането на удостоверението титуляра/автора 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.**

#### 4.5 Използване на удостоверението и ключовата двойка

Титуляра/автора, 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 УЕП (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 УЕП 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 УЕП. (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.

#### 4.6 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 титуляр, който има издадено преди това валидно удостоверение за електронен подпис. Новото удостоверение съдържа: данните от подновяваното 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 УЕП и го представя On-line или чрез РО, на титуляра/автора за одобрение;
- Удостоверението не се публикува в публичния регистър, докато не се получи потвърждение от титуляра/автора за приемане на удостоверението.

„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 УЕП;
- Изпращане на поща или електронна поща до титуляра/автора, на предоставен от него адрес, информация, позволяваща на титуляра/автора да получи УЕП.

„СЕП България“ АД публикува удостоверението в публичната си директория след приемането му от страна на титуляра/автора.

Публикуването на УЕП 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 УЕП.

**„СЕП България“ АД винаги информира титуляра/автора, минимум 30 дни предварително, относно предстоящото изтичане на периода на валидност на УЕП.**

## 4.7 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 титуляра съдържаща се в удостоверението не е променена.

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

Издава се ново удостоверение, съдържащо данните за титуляра 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.

Всички удостоверения могат да се модифицират on-line. 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 УЕП и го представя On-line или чрез РО, на титуляра/автора за одобрение;
- Удостоверението не се публикува в публичния регистър, докато не се получи потвърждение от титуляра/автора за приемане на удостоверението.

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

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

„СЕП България“ АД публикува удостоверението в публичната си директория след приемането му от страна на титуляра/автора.

Публикуването на УЕП 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 УЕП.

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.

## 4.8 Прекратяване на удостоверение

Прекратяване е действие при което удостоверението за електронен подпис се включва в Списъка със спрени и прекратени удостоверения. 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.

### 4.8.1 Обстоятелства, при които се допуска прекратяване

Основната причина за прекратяване на УЕП 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 УЕП;
- Прекратяване на юридическото лице на титуляра;
- Смърт или поставяне под запрещение на физическото лице – автор;
- Установяване, че УЕП 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 Автора не е върнал предоставената му за ползване от титуляра криптографска карта при отпадане на основанието за овластяване. В този случай УЕП 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. Подаващия 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 трябва да съдържа информация, която позволява по категоричен начин да се идентифицира титуляра/автора според 3.4 Идентификация и автентификация при прекратяване, от РО или от УО.

#### **4.8.2 Кой може да иска прекратяване на удостоверение**

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

- Титуляра или негов представител, ако титулярът е юридическо лице собственик на УЕП;
- Оператор РО, който може да иска прекратяване на УЕП от името на титуляра/автора или от свое име, ако информацията, с която разполага удовлетворява изискванията за прекратяване на УЕП;
- По искане на посочени в нормативен акт органи;
- Упълномощен представител на УО.

Операторите РО трябва да обработват с повишено внимание искания за прекратяване, които не са подадени от титуляра/автора и във всички случаи, от които титуляра/автора може да претърпи загуби в следствие на прекратяването.

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.

### 4.8.3 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. Титуляра 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 УЕП;
- **Трети метод** – основава се на подаване на искане, което не е в електронна форма, като хартиен документ, факс, телефонно обаждане. Идентификацията и автентификацията на лицата в този случай е описана в *„Правилата за издаване на удостоверения, включително правилата за установяване идентичността на титуляра на универсалния електронен подпис“* и на интернет адрес <http://e-sign.mobisafe.bg>

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.

**Всяко искане на прекратяване трябва да идентифицира по безспорен начин удостоверението, което ще се прекрати, да съдържа причина за прекратяване и трябва да е автентифицирано (подписано с електронен или саморъчен подпис).**

Процедурата за прекратяване на удостоверение за електронен подпис 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 СПУ 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 иницирането на процес по прекратяване.

**Необходимо е, ако искането за прекратяване е подадено от пълномощен представител на УО – РО, то да се провери и потвърди от оператор на РО.**

Ако удостоверението е прекратено или частния ключ, съответстващ на публичния от удостоверението е съхранен на електронно криптографско устройство, при прекратяване на удостоверението, устройството може да се унищожи физически или да бъде изтрито по сигурен начин. Тази операция трябва да се извърши от собственика на криптографското устройство физическо или юридическо лице или негов представител. Картата трябва да се съхранява по сигурен начин, докато се изтрие или унищожи.

#### **4.8.4 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 СПУ. Доверяващата се страна е длъжна да направи проверката в актуалния текущ СПУ.

Проверката на статуса на издадените удостоверения може да се базира само на СПУ, ако периода на публикуване на СПУ, посочен от „СЕП България“ АД, не носи сериозен риск от загуби за доверяващите се страни. Иначе доверяващите се страни трябва да се свържат с ДУУ (телефон, факс) или да използват On-line проверка на статуса на издадените удостоверения (точка 4.8.6).

Ако проверяваното удостоверение за електронен подпис се намира в СПУ, 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 СПУ;

<b>keyCompromise</b>	-	нарушена е сигурността на частния ключ;
<b>caCompromised</b>	-	нарушена е сигурността на ключа на УО;
<b>cessationOfOperation</b>	-	причината, поради която е издадено удостоверението вече не съществува;
<b>certificateHold</b>	-	удостоверението е спряно.

Ако удостоверението е прекратено поради следните причини:

<b>affiliationChanged</b>	-	модифицирани са данни на удостоверението;
<b>superseded</b>	-	удостоверението включено в СПУ е заменено с друго удостоверение;

Крайното решение относно валидността на удостоверението се взема от доверяващата се страна. Когато взема решение доверяващата се страна трябва да вземе предвид, че няма основание да се довери на автор, чийто частен ключ е бил компрометиран.

#### 4.8.5 Периодичност на публикуване на СПУ

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. Списъка с прекратените удостоверения на базовия УО, се обновява най-малко 1 (един) път годишно.

Списък със спрени и прекратените удостоверения се публикува в публичния регистър на ДУУ.

#### 4.8.6 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 СПУ, за статуса на издадените удостоверения.

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

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

**OCSP услугата е достъпна за всички титуляри/автори и доверяващи се страни, които приемат начина на предоставяне на услугата описан в тази практика.**

Статуса на удостоверението е достъпен в реално време, незабавно след прекратяване на удостоверението, като се прави справка в базата данни на доставчика. Информацията е по-актуална от тази, съдържаща се в СПУ.

#### 4.8.7 Необходимост от проверка валидността On-line

Доверяващите се страни не са задължени да проверяват статуса на удостоверенията on-line, като ползват механизма описан в 4.8.6. Препоръчително е да се използва OCSP услугата в ситуации, в които има голям

риск от фалшификация на електронни документи подписани с електронен подпис или се изисква от спецификата на приложение или регулаторна рамка.

## **4.9 Спиране и възобновяване на удостоверение**

### **4.9.1 Обстоятелства при спиране на удостоверение**

Спиране е действие, при което удостоверението за електронен подпис се включва временно в Списъка със спрени и прекратени удостоверения. За времето на престой на удостоверението в СПУ, с него не може да се потвърждават електронни подписи. След изваждане на удостоверението от СПУ 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.

### **4.9.2 Обстоятелства при възобновяване на удостоверение**

Възобновяване е действие, при което титуляра/автора, след като е бил уведомен, че удостоверението му е било включено в СПУ, 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.

### **4.9.3 Кой може да иска спиране и възобновяване на удостоверение**

#### **4.9.3.1 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, без да е длъжен да се увери в самоличността или в представителната му власт;
- 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.

#### **4.9.3.2 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 е узнал причината за спирането, както и че искането за възобновяване е направено вследствие на узнаването;
- Отпадане на основанията за спиране.

#### **4.9.4 Процедура по спиране и възобновяване на удостоверение**

##### **4.9.4.1 Процедура по спиране на действието на удостоверение**

„СЕП България“ АД спира удостоверение за електронен подпис след настъпване на някое от основанията посочени в 4.9.3.1 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 подателя на искането. Проверката може да се извърши по телефона, чрез факс, или при посещение на РО от пълномощен представител или обратно;

**Предварителна идентификацията и автентификацията на лицата подали искане за спиране на удостоверение не се изисква от ЗЕДЕП.**

- 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 за спирането на действието на удостоверението.

##### **4.9.4.2 Процедура за възобновяване на действието на удостоверение**

„СЕП България“ АД възобновява удостоверение за електронен подпис след настъпване на някое от основанията посочени в 4.9.3.2, 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 възобновява 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 – след като „СЕП България“ АД, съответно КРС се увери, че титулярът 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 и негов пълномощник, ако титулярът е юридическо лице;
- Подалия искането за възобновяване се автентифицира според определеното в точка 3.5;
- 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. 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 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 УЕП в съответствие с тази практика.

#### **4.9.5 Ограничения на периода на спиране**

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

### **4.10 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.

#### **4.10.1 Експлоатационни характеристики**

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

- При СПУ – да се изтегли СПУ за съответния УО и да се инсталира в приложението на крайния потребител. Мястото, от където може да се изтегли СПУ 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.

#### **4.10.2 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.

## 4.11 Удостоверяване на време

„СЕП България“ АД предоставя услуги по удостоверяване на дата и час на представяне на електронен документ, подписан с частен ключ, съответстващ на публичния ключ, включен в удостоверение, издадено от него.

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

### 4.11.1 Процедура по предоставяне на услугата удостоверяване на 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 Доставчика на адрес: <http://tsa.mobisafe.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 GMT;
- Идентификация на доставчика на удостоверено време – „СЕП България“ АД.

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

### 4.11.2 Уверение за трети страни

Ползвайки услугата по удостоверяване на време, потребителите и трети страни получават уверение за това, че този електронен документ е съществувал в този вид към удостовереното от „СЕП България“ АД време.

## 4.12 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.

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

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

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

## **5 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.

### **5.1 Съоръжения на доставчика**

#### **5.1.1 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.

##### **5.1.1.1 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.

##### **5.1.1.2 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.

Физическия 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.

### **5.1.1.3 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.

### **5.1.1.4 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.

### **5.1.1.5 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 с съответствие с нормативната регулация. В защитените помещения и архивите е изградена автоматична система за гасене, която се включва автоматично при откриване на огън.

### **5.1.1.6 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.

### **5.1.1.7 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.

### **5.1.1.8 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.

## **5.1.2 Съоръжения на РО**

### **5.1.2.1 Местоположение и конструкция**

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.mobisafe.bg> или в офиса на „СЕП България“ АД.

### **5.1.2.2 Физически достъп**

Достъпа до базовия РО е в съответствие с 5.1.1.2.

Достъпа до другите РО няма допълнителни изисквания по отношение на физическия достъп. Препоръчва се офиса на РО да е отделен и да разполага с оборудване което да позволи сигурно съхранение на данни и документи. Достъпа да се следи и да е ограничен до служители на РО и техни клиенти.

#### **5.1.2.3 Електрозахранване и климатизация**

Базовия РО се захранва от основния и резервен източник на „СЕП България“ АД.

При другите РО няма специални изисквания по отношение на електрозахранването и климатизацията.

#### **5.1.2.4 Наводнение**

Няма определени изисквания.

#### **5.1.2.5 Противопожарни мерки**

Няма определени изисквания.

#### **5.1.2.6 Съхраняване на носители**

Носителите използвани за архивиране на текущата информация и резервни копия, и хартиените документи се съхраняват в сейфове разположени в базовия РО.

#### **5.1.2.7 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.

#### **5.1.2.8 Съхранение на резервните копия**

Копията се съхраняват в сейфове изискващи двуфакторен достъп.

Препоръчва се архивите и резервните копия от текущите данни и информация да се съхраняват извън РО.

### **5.1.3 Сигурност на титуляра/автора**

Титуляра/авторът е отговорен за съхранението на паролите за достъп, идентификационни кодове, ПИН и деблокиращ ПИН. В случай, че титуляра/автора поддържа регистър на пароли, кодове и ПИН, то той трябва да се съхранява по надежден и сигурен начин, и да е достъпен само за упълномощени от него лица.

Пароли за криптиране на съдържание на носители да не се съхраняват заедно с носителите.

## **5.2 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.

### **5.2.1 Доверени длъжности**

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

Длъжностите от персонала на доставчика на удостоверителни услуги включват:

- **администратор по сигурността**, който отговаря за определянето и администрирането на системите и правилата за сигурност за цялата система, включително одобряване създаването и прекратяването на действието на удостоверенията;
- **системен администратор**, който отговаря за инсталирането, конфигурирането и управлението на инфраструктурата на публични ключове, за регистрацията и създаването на удостоверенията;
- **системен оператор**, който отговаря за ежедневната работа на системата, като извършва редовно процедури по архивиране, резервиране и възстановяване;
- **системни контрольори**, които отговарят за управлението на архивите и файловете с данни за регистрираните действия и функции, извършвани в системата на доставчика.

## 5.2.2 Разделяне на задълженията

Дължностите по 5.2.1 се изпълняват от различни лица.

## 5.2.3 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. Персонала няма достъп до доверени дейности докато не приключат необходимите проверки.

## 5.3 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;
- Не изпълняват задачи, които може да доведат до конфликт на интереси.

### 5.3.1 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.

### 5.3.2 Проверка на знанията

„СЕП България“ АД преди да назначи лице на съответните длъжности проверява познанията и квалификацията му в съответствие с 5.3.1.

### 5.3.3 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 по 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;
- Процедури за действие при извънредни ситуации, повреди, аварии и природни бедствия.

### 5.3.4 Непрекъснатост на обучението

Обучението на персонала посочено в 5.3.3 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.

### 5.3.5 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.

### 5.3.6 Договори с външни лица

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

### 5.3.7 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 по 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.

## 5.4 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.

### 5.4.1 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 журналите предварително е определен и е предвиден достатъчен капацитет за нормална работа на системите. При достигане на определен размер се създават нови журнали. Старите се архивират и изтриват от оперативните системи.

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

- Тип на събитието;

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

Записите могат да бъдат:

- Аларми от защитни стени и мрежови сензори;
- Операции съответстващи на регистрация, удостоверяване/издаване, смяна на ключове и подновяване, прекратяване, спиране/възобновяване и други услуги предоставяни от УО;
- Всяка промяна на хардуера или софтуера;
- Физическо посещение на защитените периметри и нарушаване на 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 журналите, системите и бази данни.

Достъп до журналите имат само системния контролър и лица осъществяващи проверка на дейността на ДУУ.

#### **5.4.2 Преглед на журналите**

Поне веднъж месечно се прави детайлен преглед на журналите. При проверката журнала се преглежда и за цялостност и автентичност. Веднъж седмично подробно се преглеждат журналите от произволно избрана операция. При инцидент или съмнение за инцидент по сигурността се преглеждат всички журнални файлове.

#### **5.4.3 Период на съхранение**

Журналите 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 5 години.

#### **5.4.4 Защита на журналните файлове**

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

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

- Само упълномощени лица – проверяващи и служители на ДУУ, имат право да преглеждат файловете;
- Само системния контролър 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 да достъп важат и за архивирани и предадени за съхранение записи.

#### **5.4.5 Архивиране на журналните файлове**

„СЕП България“ АД ежесечно 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.

#### **5.4.6 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.

#### **5.4.7 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.

Системният контролор е отговорен за провеждането на вътрешни одити за съответствие на записаните събития в журналите, тяхната коректност и съхраняване и предприетите последващи действия, с тази практика при предоставяне на удостоверителни услуги.

### **5.5 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 СПУ, ключовете използвани от РО 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).

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

Хартиените оригинали се съхраняват за срок най- малко от 5 години след изтичане на ангажиментите на „СЕП България“ АД по отношение събитието, за което се отнасят. След това се съхранява само електронния вариант на документа.

### 5.5.1 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 СПУ;
- 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.

### 5.5.2 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 5 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 5 години;
- Списъка с прекратени удостоверения, кореспонденцията и подадените искания, както и взетите решения се съхраняват според по-горе описаната схема.

### 5.5.3 Период на съхраняване в архив

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

### 5.5.4 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, архива периодично се прехвърля на нови

носителите, 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 при 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.

### 5.5.5 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.

### 5.5.6 Изискване за удостоверено време за записите

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

### 5.5.7 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.

## 5.6 Смяна на ключовете

Прилага се процедура за случаите, когато УО на „СЕП България“ АД подменя ключовете, с които подписва издаваните удостоверения и списък със спрени и 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 титуляри/автори. Публикува се информация в печатните издания.

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 и списък с прекратени удостоверения.**

## 5.7 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.

### 5.7.1 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.

Доставчикът назначава служител/и, които периодично анализират нарушенията на сигурността, с цел да се посочат потенциалните рискове и разходите за покриването им.

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“.

### 5.7.2 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:

- **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. Плана 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, в съответствие с 5.5.5, се правят резервни копия на базите данни. Копията съдържат всички подадени искания, издадените, подновени и прекратени удостоверения. Копията се съхраняват на двете места;
  - Периодично, в съответствие с 5.5.5, 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.
- **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;
- **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.
- **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.
  - **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.

### 5.7.3 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.

### 5.7.4 Продължаване на дейностите след възстановяване от бедствия и авария

След всяко възстановяване на системата от авария, системния контролърор 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.

## **5.8 Прекратяване или прехвърляне на дейността**

### **5.8.1 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 Регистриран доставчик на удостоверителни услуги. Също така му предава и цялата документация, свързана с дейността му.

При невъзможност „СЕП България“ АД да прехвърлил 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.

### **5.8.2 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 на потребителя;
- По искане на РО.

**Регистриращ орган на „СЕП България“ АД не може да прехвърля своята дейност.**

## 6 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.

### 6.1 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 – MobiSafe CA;

Частния ключ на SEP Root CA се използва изключително и само за подписване на публичните ключове на: MobiSafe CA; MobiSafe TSA и подписване на издавания от него СПУ.

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

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;

#### 6.1.1 Генериране на ключови двойки

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

Ключовете 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.

„СЕП 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.

#### **6.1.1.1 Генериране на ключовете на SEP Root CA**

Процедурата се изпълнява всеки път при инициализация на системата за доставка на удостоверителни услуги на „СЕП 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.

#### **6.1.1.2 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 „СЕП България“ АД. „СЕП България“ АД издава ново УЕП на SEP Root CA и за период от една година „СЕП България“ АД поддържа новото и старото УЕП, след което старото изтича и остава валидно новото УЕП на SEP Root CA.

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

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

#### **6.1.1.3 Смяна на ключовете на оперативния УО на ДУУ**

Следва се процедурата описана в 6.1.1.2 като новото оперативное удостоверение се издава от SEP Root CA и се подписва с новия частен ключ.

#### **6.1.2 Предоставяне на частния ключ на автора**

Титуляра/автора сам генерира своята ключова двойка, като използва криптографско устройство например смарт/сим карта.

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.

#### **6.1.3 Предоставяне на публичния ключ до УО**

Когато титуляра/автора генерира сам ключова двойка, то те трябва да предоставят публичния ключ от двойката 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 одобрят от оператор на РО.

#### 6.1.4 Предоставяне на публичния ключ на УО до доверяващите се страни

Публичния ключ на УО на „СЕП България“ АД се разпространяват 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.mobisafe.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 резултат от процедурата описана в 6.1.1.1.

#### 6.1.5 Дължина на ключовете

Дължината на използваните ключове е в съответствие с „Наредба за изискванията към алгоритмите за усъвършенстван електронен подпис“ и е както следва:

СОБСТВЕНИК НА КЛЮЧА	ПАРАМЕТРИ НА КЛЮЧА	
	RSA	ВАЛИДНОСТ
SEP Root CA	4096 bit	20 години
MobiSafe CA	2048 bit	10 години

#### 6.1.6 Параметри на генерация на публичния ключ и проверка за качество

Параметрите на генерираните ключове от „СЕП България“ АД са в съответствие с „Наредба за изискванията към алгоритмите за усъвършенстван електронен подпис“.

### 6.2 Защита на частния ключ

Частните ключове на ДУУ и крайните потребители се генерират, съхраняват и използват посредством криптографски хардуерни модули. Хардуерните криптографски модули, които използва „СЕП България“ АД са в съответствие на чл. 26. от „Наредбата за дейността на доставчиците на удостоверителни услуги, реда за нейното прекратяване и за изискванията при предоставяне на удостоверителни услуги“, като създаването, съхраняването и използването на частния ключ на доставчика на удостоверителни услуги се извършват в система със защитен профил, определен в съответствие с общите изисквания (CC), ниво на сигурност EAL 3 или по-високо съгласно стандарта ISO 15408 или друга спецификация, определяща еквивалентни нива на сигурността.

### 6.2.1 Криптографски модули – стандарти и контроли

„СЕП България“ АД използва следните криптографски модули за базовия и оперативните УО:

СОБСТВЕНИК НА КЛЮЧА	ИЗПОЛЗВАН КРИПТОГРАФСКИ МОДУЛ
SEP Root CA	хардуерен модул с EAL 3 или по-висока
MobiSafe CA	хардуерен модул с EAL 3 или по-висока

„СЕП България“ АД издава удостоверения и удостоверява предоставени от титуляра/автора публични ключове, ако ключовата двойка е генерирана на смарт карта с ниво на сигурност EAL 3 или по-високо.

### 6.2.2 Достъп до частния ключ на доставчика

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

### 6.2.3 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 УЕП, се архивират, съхраняват и възстановяват съвместно най-малко от двама служители на доверени позиции във физически защитена среда.

### 6.2.4 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.

### 6.2.5 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 ключа 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.

### 6.2.6 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.

### 6.2.7 Активиране на частния ключ

Частния 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.

### **6.2.8 Деактивиране на частния ключ**

Частния 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.

### **6.2.9 Унищожаване на частния ключ**

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

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

### **6.2.10 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.

## **6.3 Други аспекти от управлението на ключовете**

### **6.3.1 Архивиране на публичния ключ**

Публичните ключове на „СЕП България“ АД се съхраняват като част от удостоверение за електронен подпис и се архивират 10 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.

### **6.3.2 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
<b>SEP Root CA</b>	20 години	19 години
<b>MobiSafe CA</b>	10 години	9 години
<b>MobiSafe TSA</b>	10 години	10 години
<b>MobiSafe OCSP</b>	10 години	10 години
<b>MobiSafe Private</b>	3 години	3 години
<b>MobiSafe Organization</b>	3 години	3 години
<b>MobiSafe Professional</b>	3 години	3 години
<b>MobiSafe Server</b>	3 години	3 години

## 6.4 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 не оторизирано 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 то 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, когато титулярът е юридическо лице. Във всички случаи се изисква титуляра/автора да сменят ПИН веднага след като го получат.

## 6.5 Управление на компютърната сигурност

### 6.5.1 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.

### 6.5.2 Оценка на сигурността

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

## 6.6 Технически контроли

### 6.6.1 Разработка на информационна система

„СЕП България“ АД разработва и внедрява приложенията и системния софтуер за предоставяне на удостоверителни услуги.

### 6.6.2 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.

## 6.7 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.

## 7 Профили на удостоверения, списък със спрени и прекратени удостоверения и OCSF

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

### 7.1 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.

#### 7.1.1 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.

##### 7.1.1.1 Базови полета

„СЕП България“ АД поддържа следните полета в издаваните удостоверения:

- **Основно поле** – съдържа основните полета на УЕП:
  - **Version:** трета версия (X.509 v.3);
  - **SerialNumber:** уникален сериен номер на удостоверението в рамките на издаващия удостоверяващия орган;
  - **Signature:** идентификатора 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

ИМЕ НА ПОЛЕ	СТОЙНОСТ ИЛИ ОГРАНИЧЕНИЕ НА СТОЙНОСТТА	
<b>serialNumber</b>	уникален сериен номер на удостоверението в рамките на издаващия удостоверяващия орган	
<b>signature</b>	sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5) id-ecdsa-with-sha1 (OID: 1.2.840.10045.4.1)	
<b>issuer (Distinguished Name)</b>	countryName	BG
	stateOrProvinceName	Sofia
	localityName	Sofia
	organizationName	System for Electronic Payments /SEP Bulgaria/ JSC
	organizationalUnitName	MobiSafe
	organizationalUnitName	EIK 131107204
	commonName	SEP Root CA, MobiSafe CA
	PostalAddress	bul.Tsarigradsko shose 135
	postalCode	1784
	Phone	00359 700 18283
	emailAddress	<a href="mailto:esign@mobisafe.bg">esign@mobisafe.bg</a>
<b>validity</b>	notBefore	UTCTime формат
	notAfter	UTCTime формат
<b>subject (Distinguished Name)</b>	<i>Distinguished Name на титуляра/автора в съответствие с изискванията на X.501. Стойностите на атрибутите са в зависимост от типа издавано УЕП.</i>	
	C, Country	определя контекста, в който се разглеждат останалите атрибути
	ST, State or Province	ако се ползват съдържа географска информация свързана с титуляра. Ако присъства organizationName то тази информация се отнася до организацията
	L, Location	
	O, Organization	ако се ползват съдържа името на организацията, с която е асоцииран титуляра и съответно свързана с организацията информация;
	OU, Organization Unit	съдържа типа на издаденото удостоверение
	UID, Unique Identifier	EGN/EIK на титуляра
	CN, Common Name	име на титуляра/автора
	T, Title	ако се използва съдържа позицията или функцията на автора в организацията на титуляра
	PostalAddress	адрес – ж. к., ул., ном., бл., ап. на титуляра
	PostalCode	пощенски код на титуляра
	Phone	телефон на титуляра
	EmailAddress	e-mail на автора за кореспонденция от името на титуляра
<b>Key Usage</b>	{digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment, keyCertSign, cRLSign}	
<b>Enhanced Key Usage</b>	{serverAuth, clientAuth, codeSigning, emailProtection, timeStamping, OCSPSigning}	
<b>Certificate Policies</b>	Policies: 1.3.6.1.4.1.30299.1.1 CPSuri: <a href="http://e-sign.mobisafe.bg/directory">http://e-sign.mobisafe.bg/directory</a>	
	Policies: 1.3.6.1.4.1.30299.1.1.{1,2,3} – в зависимост от типа УЕП. CPSuri: <a href="http://e-sign.mobisafe.bg/directory">http://e-sign.mobisafe.bg/directory</a> UserNotice: organization: SEP Bulgaria JSC explicitText: This certificate is issued as qualified certificate for qualified electronic signature using secure signature creation device	
<b>Certificate Policies</b>	Policies: 1.3.6.1.4.1.30299 CPSuri: <a href="http://www.crc.bg/">http://www.crc.bg/</a> UserNotice: organization: SEP Bulgaria JSC explicitText: SEP Bulgaria JSC – registered certification service provider	

ИМЕ НА ПОЛЕ	СТОЙНОСТ ИЛИ ОГРАНИЧЕНИЕ НА СТОЙНОСТТА
<b>CRL Distribution Points</b>	URL: <a href="http://crl.mobisafe.bg/">http://crl.mobisafe.bg/</a> { mobisafe_root_ca.crl,mobisafe_ca.crl} URL: ldap://ldap.mobisafe.bg/cn={"SEP Root CA", "MobiSafe CA"},ou=MobiSafe,dc=mobisafe,dc=bg
<b>Authority Information Access</b>	OCSP: <a href="http://ocsp.mobisafe.bg">http://ocsp.mobisafe.bg</a>
<b>Basic Constraints</b>	cA: yes/no, pathLenConstraint: 1
<b>Subject Alternative Name</b>	адрес на автора
<b>Authority Key Identifier</b>	
<b>Subject Key Identifier</b>	
<b>subjectPublicKeyInfo</b>	публичния ключ на титуляра/автора и алгоритъма, с който се използва
<b>Qualified Certificate Statements</b>	посочва, че удостоверението е издадено като удостоверение за универсален електронен подпис
<b>signatureAlgorithm</b>	sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5) id-ecdsa-with-sha1 (OID: 1.2.840.10045.4.1)
<b>signatureValue</b>	електронен подпис на ДУУ

### 7.1.1.2 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 СПУ;
 разширението **Key Usage** е критично.
- **Enhanced Key Usage:** дефинира приложенията, за които може да се използва ключа от удостоверението. Това разширение определя една или няколко области в добавка към **Key Usage** полето за допустимо използване на удостоверението. тези области следва да се тълкуват като ограничение по отношение на допустимото използване. Възможни са един или комбинация от няколко от следните елементи:
  - **serverAuth:** за TLS WWW автентификация на сървър. Съвместимост с **digitalSignature**, **keyEncipherment** или **keyAgreement**;

- **clientAuth:** за TLS WWW автентификация за клиент. Съвместимост с **digitalSignature** и/или **keyAgreement**;
- **codeSigning:** за подписване на изпълним код най често разпространяван през интернет Съвместимост с **digitalSignature**;
- **emailProtection:** за защита на E-mail. Съвместимост **digitalSignature**, **nonRepudiation**, и/или (**keyEncipherment** или **keyAgreement**);
- **timeStamping:** привързва хеш на обект към определено време. Съвместимост с **digitalSignature** и/или **nonRepudiation**;
- **OCSPSigning:** подписване на OCSP отговор Съвместимост с **digitalSignature** и/или **nonRepudiation**;

това разширение не е критично.

- При наличие на двете разширения **Key Usage** и **Enhanced Key Usage**, то двете разширения се обработват от приложението по отделно и удостоверението се използва за цели, които са съвместими и с двете разширения. В противен случай не се използва за никакви цели.
  - **Certificate Policies:** идентифицира една или няколко политики, чрез OID идентификатор на политиката и допълнителни квалификатори на политика;
- **CPSuri:** указател/препратка, под формата на URL, към мястото, където се намира „Практика при предоставяне на удостоверителни услуги“;
  - **UserNotice:** препратка към текст, който да се покаже на доверяващите се страни при проверка на УЕП. Текста 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 СПУ. Може да има повече от един механизъм за извличане на СПУ, 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 универсален електронен подпис.

### 7.1.1.3 Идентификаторите на обекти

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

**„СЕП България“ АД използва следната структура на идентификаторите на обекти, за идентифициране на политиката, според която се издават удостоверенията за електронен подпис:**

ИДЕНТИФИКАТОР НА ОБЕКТИ (OID)			
SEP Bulgaria JSC	SEP Root CA	MobiSafe CA	Типове удостоверения
1.3.6.1.4.1.30299	1	1	1   MobiSafe Private
			2   MobiSafe Organization
			3   MobiSafe Profession
			4   MobiSafe Server
			5   MobiSafe TSA
			6   MobiSafe OCSP

### 7.1.2 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. Частния ключ се използва за подписване на удостоверението на оперативния УО и удостоверението за валидация на удостоверение време.

**Периода 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 универсален подпис по смисъла на чл. 33. (1) т.2 от ЗЕДЕП.

**Профил на удостоверението на SEP Root CA е следния:**

ИМЕ НА ПОЛЕ	СТОЙНОСТ ИЛИ ОГРАНИЧЕНИЕ НА СТОЙНОСТТА		
<b>version</b>	Version 3		
<b>serialNumber</b>	уникален сериен номер на удостоверението в рамките на издаващия удостоверяващия орган		
<b>signature</b>	sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5)		
<b>issuer (Distinguished Name)</b>	C	BG	
	S	Sofia	
	L	Sofia	
	O	System for Electronic Payments /SEP Bulgaria/ JSC	
	OU	MobiSafe	
	OU	EIK 131107204	
	CN	SEP Root CA	
	PostalAddress(2.5.4.16)	bul.Tsarigradsko shose 135	
	PostalCode	1784	
	Phone	00359 700 18283	
	E	esign@mobisafe.bg	
<b>validity</b>	notBefore	UTCTime формат	
	notAfter	UTCTime формат	
<b>subject (Distinguished Name)</b>	C	BG	
	S	Sofia	
	L	Sofia	
	O	System for Electronic Payments /SEP Bulgaria/ JSC	

ИМЕ НА ПОЛЕ	СТОЙНОСТ ИЛИ ОГРАНИЧЕНИЕ НА СТОЙНОСТТА
	OU MobiSafe
	OU EIK 131107204
	CN SEP Root CA
	PostalAddress(2.5.4.16) bul.Tsarigradsko shose 135
	PostalCode 1784
	Phone 00359 700 18283
	E esign@mobisafe.bg
<b>Key Usage</b>	Certificate Signing, Off-line CRL Signing, CRL Signing (06)
<b>Certificate Policies</b>	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.30299 [1,1]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text=SEP Bulgaria JSC – registered certification service provider [1,2]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.crc.bg/ [2]Certificate Policy: Policy Identifier=1.3.6.1.4.1.30299.1 [2,1]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text=SEP Root CA [2,2]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://e-sign.mobisafe.bg/directory
<b>CRL Distribution Points</b>	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.mobisafe.bg/mobisafe_root_ca.crl [2]CRL Distribution Point Distribution Point Name: Full Name:  URL=ldap://ldap.mobisafe.bg/cn=SEP%20Root%20CA,ou=MobiSafe,dc=mobisafe,dc=bg
<b>Authority Information Access</b>	[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.mobisafe.bg
<b>Basic Constraints</b>	Subject Type=CA Path Length Constraint=None
<b>Issuer Alternative Names</b>	
<b>Subject Alternative Name</b>	
<b>Authority Key Identifier</b>	
<b>Subject Key Identifier</b>	
<b>subjectPublicKeyInfo</b>	публичния ключ на титуляра/автора и алгоритъта, с който се използва
<b>signatureAlgorithm</b>	sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5)
<b>signatureValue</b>	електронен подпис на ДУУ

### 7.1.3 Удостоверение на оперативния УО

Оперативния 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.

**Периода 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 универсален подпис по смисъла на чл. 33. (1) т.2 от ЗЕДЕП.

Оперативния УО MobiSafe CA, издава удостоверения за електронен подпис в съответствие с политика с OID: 1.3.6.1.4.1.30299.1.1.

**Профила на удостоверението на MobiSafe CA е следният:**

ИМЕ НА ПОЛЕ	СТОЙНОСТ ИЛИ ОГРАНИЧЕНИЕ НА СТОЙНОСТТА	
<b>version</b>	Version 3	
<b>serialNumber</b>	уникален сериен номер на удостоверението в рамките на издаващия удостоверяващия орган	
<b>signature</b>	sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5)	
<b>issuer (Distinguished Name)</b>	C	BG
	S	Sofia
	L	Sofia
	O	System for Electronic Payments /SEP Bulgaria/ JSC
	OU	MobiSafe
	OU	EIK 131107204
	CN	MobiSafe Root CA
	PostalAddress(2.5.4.16)	bul.Tsarigradsko shose 135
	PostalCode	1784
	Phone	00359 700 18283
E	esign@mobisafe.bg	
<b>validity</b>	notBefore	UTCTime формат
	notAfter	UTCTime формат
<b>subject (Distinguished Name)</b>	C	BG
	S	Sofia
	L	Sofia
	O	System for Electronic Payments /SEP Bulgaria/ JSC
	OU	MobiSafe
	OU	EIK 131107204
	CN	MobiSafe CA
	PostalAddress(2.5.4.16)	bul.Tsarigradsko shose 135
	PostalCode	1784
	Phone	00359 700 18283
E	esign@mobisafe.bg	
<b>Key Usage</b>	Certificate Signing, Off-line CRL Signing, CRL Signing (06)	
<b>Enhanced Key Usage</b>		

ИМЕ НА ПОЛЕ	СТОЙНОСТ ИЛИ ОГРАНИЧЕНИЕ НА СТОЙНОСТТА
<b>Certificate Policies</b>	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.30299.1.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text=MobiSafe CA [1,2]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://e-sign.mobisafe.bg/directory [2]Certificate Policy: Policy Identifier=1.3.6.1.4.1.30299 [2,1]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text=SEP Bulgaria JSC – registered certification service provider [2,2]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.crc.bg/
<b>CRL Distribution Points</b>	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.mobisafe.bg/mobisafe_root_ca.crl [2]CRL Distribution Point Distribution Point Name: Full Name: URL=ldap://ldap.mobisafe.bg/cn=SEP%20Root%20CA,ou=MobiSafe,dc=mobisafe,dc=bg
<b>Authority Information Access</b>	[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.mobisafe.bg
<b>Basic Constraints</b>	Subject Type=CA Path Length Constraint=None
<b>Issuer Alternative Names</b>	
<b>Subject Alternative Name</b>	
<b>Authority Key Identifier</b>	
<b>Subject Key Identifier</b>	
<b>subjectPublicKeyInfo</b>	публичния ключ на титуляра/автора и алгоритъма, с който се използва
<b>signatureAlgorithm</b>	sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5)
<b>signatureValue</b>	електронен подпис на ДУУ

#### 7.1.4 Потребителски удостоверения

Потребителските удостоверения се издават от оперативния УО.

**Периода на валидност на издадените удостоверения е 3 (три) години. Дължината на ключа е 1024 бита за RSA алгоритъм или 163 бита за ECDSA алгоритъм.**

##### 7.1.4.1 Профил на MobiSafe Private

Удостоверението за електронен подпис, MobiSafe Private служи за доказване 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.

Удостоверението MobiSafe Private е удостоверение за универсален подпис.

**Профила на MobiSafe Private удостоверение е:**

ИМЕ НА ПОЛЕ	СТОЙНОСТ ИЛИ ОГРАНИЧЕНИЕ НА СТОЙНОСТТА	
<b>version</b>	Version 3	
<b>serialNumber</b>	уникален сериен номер на удостоверението в рамките на издаващия удостоверяващия орган	
<b>signature</b>	sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5) id-ecdsa-with-sha1 (OID: 1.2.840.10045.4.1)	
<b>issuer (Distinguished Name)</b>	C	BG
	S	Sofia
	L	Sofia
	O	System for Electronic Payments /SEP Bulgaria/ JSC
	OU	MobiSafe
	OU	EIK 131107204
	CN	MobiSafe CA
	PostalAddress(2.5.4.16)	bul.Tsarigradsko shose 135
	PostalCode	1784
	Phone	00359 700 18283
	E	esign@mobisafe.bg
<b>validity</b>	notBefore	UTCTime формат
	notAfter	UTCTime формат
<b>subject (Distinguished Name)</b>	C	BG
	S	област на титуляра
	L	населено място на титуляра
	OU	MobiSafe Private
	CN	име на титуляра
	UID (0.9.2342.19200300.100.1.1)	EGNxxxxxxxxxx[ЕГН/ЛНЧ/ггммдд на титуляра]
	PostalAddress (2.5.4.16)	адрес – ж. к., ул., ном., бл., ап. на титуляра
	PostalCode	пощенски код на титуляра
	Phone	телефон на титуляра
E	e-mail адрес на титуляра	
<b>Key Usage</b>	Digital Signature, Non-Repudiation, Key Encipherment, Data Encipherment (f0)	
<b>Enhanced Key Usage</b>	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
<b>Certificate Policies</b>	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.30299 [1,1]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text=SEP Bulgaria JSC – registered certification service provider [1,2]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: <a href="http://www.crc.bg/">http://www.crc.bg/</a> [2]Certificate Policy: Policy Identifier=1.3.6.1.4.1.30299.1.1.1 [2,1]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 [2,2]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: <a href="http://e-sign.mobisafe.bg/directory">http://e-sign.mobisafe.bg/directory</a>
<b>CRL Distribution Points</b>	[1]CRL Distribution Point Distribution Point Name: Full Name: URL= <a href="http://crl.mobisafe.bg/mobisafe_ca.crl">http://crl.mobisafe.bg/mobisafe_ca.crl</a> [2]CRL Distribution Point Distribution Point Name: Full Name: URL= <a href="ldap://ldap.mobisafe.bg/cn=MobiSafe%20CA,ou=MobiSafe,dc=mobisafe,dc=bg">ldap://ldap.mobisafe.bg/cn=MobiSafe%20CA,ou=MobiSafe,dc=mobisafe,dc=bg</a>
<b>Authority Information Access</b>	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL= <a href="http://ocsp.mobisafe.bg">http://ocsp.mobisafe.bg</a>
<b>Basic Constraints</b>	Subject Type=End Entity Path Length Constraint=None
<b>Authority Key Identifier</b>	
<b>Subject Key Identifier</b>	
<b>Qualified Certificate Statements</b>	посочва, че удостоверението е издадено като удостоверение за универсален електронен подпис
<b>subjectPublicKeyInfo</b>	публичния ключ на титуляра/автора и алгоритъма, с който се използва
<b>signatureAlgorithm</b>	sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5) id-ecdsa-with-sha1 (OID: 1.2.840.10045.4.1)
<b>signatureValue</b>	електронен подпис на ДУУ

#### 7.1.4.2 Профил на MobiSafe Organization

Удостоверението за електронен подпис MobiSafe Organization служи за доказване на самоличността, съответно на идентичността, на автора и на 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. Титуляра и автора се различават, като автора е физическо лице а титуляра юридическо. Автора върши изявленията от името и за сметка на титуляра.

Удостоверението MobiSafe Organization е удостоверение за универсален подпис.

**Профила на MobiSafe Organization удостоверение е:**

ИМЕ НА ПОЛЕ	СТОЙНОСТ ИЛИ ОГРАНИЧЕНИЕ НА СТОЙНОСТТА	
<b>version</b>	Version 3	
<b>serialNumber</b>	уникален сериен номер на удостоверението в рамките на издаващия удостоверяващия орган	
<b>signature</b>	sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5) id-ecdsa-with-sha1 (OID: 1.2.840.10045.4.1)	
<b>issuer (Distinguished Name)</b>	C	BG
	S	Sofia
	L	Sofia
	O	System for Electronic Payments /SEP Bulgaria/ JSC
	OU	MobiSafe
	OU	EIK 131107204
	CN	MobiSafe CA
	PostalAddress(2.5.4.16)	bul.Tsarigradsko shose 135
	PostalCode	1784
	Phone	00359 700 18283
<b>validity</b>	E	esign@mobisafe.bg
	notBefore	UTCTime формат
	notAfter	UTCTime формат
<b>subject (Distinguished Name)</b>	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	MobiSafe Organization
	OU	организационна единица на титуляра
	UID (0.9.2342.19200300.100.1.1)	EGNxxxxxxxxxx[ЕГН/ЛНЧ/ггммдд на автора]
	CN	име на автора
	T	позиция на автора/ <b>овластяване</b>
	OU	EIKxxxxxxxxxx[ЕИК на титуляра]
	PostalAddress (2.5.4.16)	адрес по регистрация на титуляра – ж. к., ул., ном., бл., ап.
	PostalCode	пощенски код на титуляра по адрес за регистрация
	Phone	телефон на автора
E	служебен e-mail адрес на автора за водене на кореспонденция от името на титуляра	
<b>Key Usage</b>	Digital Signature, Non-Repudiation, Key Encipherment, Data Encipherment (f0)	
<b>Enhanced Key Usage</b>	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
<b>Certificate Policies</b>	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.30299 [1,1]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text=SEP Bulgaria JSC – registered certification service provider [1,2]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.crc.bg/ [2]Certificate Policy: Policy Identifier=1.3.6.1.4.1.30299.1.1.2 [2,1]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 [2,2]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://e-sign.mobisafe.bg/directory
<b>CRL Distribution Points</b>	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.mobisafe.bg/mobisafe_ca.crl [2]CRL Distribution Point Distribution Point Name: Full Name: URL=ldap://ldap.mobisafe.bg/cn=MobiSafe%20CA,ou=MobiSafe,dc=mobisafe,dc=bg
<b>Authority Information Access</b>	[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.mobisafe.bg
<b>Basic Constraints</b>	Subject Type=End Entity Path Length Constraint=None
<b>Authority Key Identifier</b>	
<b>Subject Key Identifier</b>	
<b>Qualified Certificate Statements</b>	посочва, че удостоверението е издадено като удостоверение за универсален електронен подпис
<b>subjectPublicKeyInfo</b>	публичния ключ на титуляра/автора и алгоритъма, с който се използва
<b>signatureAlgorithm</b>	sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5) id-ecdsa-with-sha1 (OID: 1.2.840.10045.4.1)
<b>signatureValue</b>	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 УЕП MobiSafe Organization. Предназначението на такива УЕП е само и единствено за провеждане на тестове.

#### 7.1.4.3 Профил на MobiSafe Profession

Удостоверението за електронен подпис, MobiSafe Profession служи за доказване 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.

Удостоверението MobiSafe Profession е удостоверение за универсален подпис.

**Профила на MobiSafe Profession удостоверение е:**

ИМЕ НА ПОЛЕ	СТОЙНОСТ ИЛИ ОГРАНИЧЕНИЕ НА СТОЙНОСТТА	
<b>version</b>	Version 3	
<b>serialNumber</b>	уникален сериен номер на удостоверението в рамките на издаващия удостоверяващия орган	
<b>signature</b>	sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5) id-ecdsa-with-sha1 (OID: 1.2.840.10045.4.1)	
<b>issuer (Distinguished Name)</b>	C	BG
	S	Sofia
	L	Sofia
	O	System for Electronic Payments /SEP Bulgaria/ JSC
	OU	MobiSafe
	OU	EIK 131107204
	CN	MobiSafe CA
	PostalAddress(2.5.4.16)	bul.Tsarigradsko shose 135
	PostalCode	1784
	Phone	00359 700 18283
	E	esign@mobisafe.bg
<b>validity</b>	notBefore	UTCTime формат
	notAfter	UTCTime формат
<b>subject (Distinguished Name)</b>	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	MobiSafe Profession
	OU	организационна единица на титуляра
	UID (0.9.2342.19200300.100.1.1)	EGNxxxxxxxxxx[ЕГН/ЛНЧ/ггммдд на автора]
	CN	име на автора
	T	позиция на автора/ <b>овластяване</b>
	OU	EIKxxxxxxxxxx[ЕИК на титуляра]
	PostalAddress(2.5.4.16)	адрес по регистрация на титуляра – ж. к., ул., ном., бл., ап.
	PostalCode	пощенски код на титуляра по адрес за регистрация
	Phone	телефон на автора
E	служебен e-mail адрес на автора за водене на кореспонденция от името на титуляра	
<b>Key Usage</b>	Digital Signature, Non-Repudiation, Key Encipherment, Data Encipherment (f0)	
<b>Enhanced Key Usage</b>	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
<b>Certificate Policies</b>	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.30299 [1,1]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text=SEP Bulgaria JSC – registered certification service provider [1,2]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.crc.bg/ [2]Certificate Policy: Policy Identifier=1.3.6.1.4.1.30299.1.1.3 [2,1]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 [2,2]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://e-sign.mobisafe.bg/directory
<b>CRL Distribution Points</b>	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.mobisafe.bg/mobisafe_ca.crl [2]CRL Distribution Point Distribution Point Name: Full Name: URL=ldap://ldap.mobisafe.bg/cn=MobiSafe%20CA,ou=MobiSafe,dc=mobisafe,dc=bg
<b>Authority Information Access</b>	[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.mobisafe.bg
<b>Basic Constraints</b>	Subject Type=End Entity Path Length Constraint=None
<b>Authority Key Identifier</b>	
<b>Subject Key Identifier</b>	
<b>Qualified Certificate Statements</b>	посочва, че удостоверението е издадено като удостоверение за универсален електронен подпис
<b>subjectPublicKeyInfo</b>	публичния ключ на титуляра/автора и алгоритъма, с който се използва
<b>signatureAlgorithm</b>	sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5) id-ecdsa-with-sha1 (OID: 1.2.840.10045.4.1)
<b>signatureValue</b>	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 УЕП MobiSafe Profession. Предназначението на такива УЕП е само и единствено за провеждане на тестове.

### 7.1.5 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)

### 7.1.6 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.

## 7.2 Профил на списъка със спрени и прекратени удостоверения

Списъка със спрени и прекратени удостоверения (CRL) съдържа следните полета:

- **tbCertList:** 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.

Смисъла на **signatureAlgorithm** и **signatureValue** е като при удостоверенията за електронен подпис.

Полето **tbCertList** съдържа поредица от задължителни и незадължителни полета. задължителните идентифицират издателя на СПУ а незадължителните съдържат информация за прекратените удостоверения и разширенията на СПУ.

Полетата са като следва:

- **version:** версия на формата на СПУ.
- **signature:** идентификатор на използвания алгоритъм от издалия СПУ УО;
- **issuer:** име на УО издал СПУ. Всеки УО от йерархията на „СЕП България“ АД, издава отделен СПУ;
- **thisUpdate:** дата на публикуване на СПУ кодирана в **UTCTime** формат;
- **nextUpdate:** известява за датата на която ще се публикува следващия СПУ. Ако полето е налично, стойността му посочва най-крайната дата на публикуване. Възможно е СПУ да се обнови преди тази дата.
- **revokedCertificates:** списък от прекратени удостоверения като полето е празно ако няма прекратени удостоверения. Информацията се съдържа в следните подплета:
  - **userCertificate:** сериен номер на прекратеното удостоверение;
  - **revocationDate:** дата на която е прекратено удостоверението;
  - **crlEntryExtensions:** допълнителна информация за прекратеното удостоверение.
    - **crlExtensions:** допълнителна информация относно СПУ;
  - **AuthorityKeyIdentifier:** позволява да се идентифицира публичния ключ съответстващ за частния ключ използван за подписване на СПУ;
  - **CRLNumber:** съдържа монотонно нарастваща последователност от числа. предоставя лесен начин да се определи кога един СПУ 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.

### Профилът на списъка с прекратени удостоверения е следният:

ПОЛЕ	СТОЙНОСТ, ПОДПОЛЕ СТОЙНОСТ	
<b>version</b>	Version 2	
<b>issuer (Distinguished Name)</b>	C	BG
	S	Sofia
	L	Sofia
	O	System for Electronic Payments /SEP Bulgaria/ JSC
	OU	MobiSafe
	OU	EIK 131107204
	CN	{SEP Root CA, MobiSafe CA}
	PostalAddress(2.5.4.16)	bul.Tsarigradsko shose 135
	PostalCode	1784
	Phone	00359 700 18283
	E	esign@mobisafe.bg
<b>thisUpdate</b>	дата на издаване на списъка с прекратени удостоверения	
<b>nextUpdate</b>	дата на издаване на следващ списък с прекратени удостоверения	
<b>signature</b>	електронен подпис на издателя на списъка с прекратени удостоверения	
<b>CRLNumber</b>	число от монотонно нарастваща редица	
<b>AuthorityKeyIdentifier</b>		
<b>revokedCertificates</b>	<b>userCertificate</b>	сериен номер
	<b>revocationDate</b>	дата на поставяне в списъка с прекратени удостоверения
	<b>crlEntryExtensions</b>	{unspecified, keyCompromise, cACompromise, affiliationChanged, superseded, cessationOfOperation, certificateHold, removeFromCRL, privilegeWithdrawn}

## 7.3 MobiSafe TSA профил

MobiSafe TSA удостоверението се използва за проверка на издадени обекти с удостоверение време. Удостоверението на MobiSafe TSA е според RFC 3280 а заявките и отговорите към MobiSafe TSA, за удостоверяване на време са съгласно RFC 3161.

### Профила на удостоверението на MobiSafe TSA е следния:

ИМЕ НА ПОЛЕ	СТОЙНОСТ ИЛИ ОГРАНИЧЕНИЕ НА СТОЙНОСТТА	
<b>version</b>	Version 3	
<b>serialNumber</b>	уникален сериен номер на удостоверението в рамките на издаващия удостоверяващия орган	
<b>signature</b>	sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5)	
<b>issuer (Distinguished Name)</b>	C	BG
	S	Sofia
	L	Sofia

ИМЕ НА ПОЛЕ	СТОЙНОСТ ИЛИ ОГРАНИЧЕНИЕ НА СТОЙНОСТТА	
	O	System for Electronic Payments /SEP Bulgaria/ JSC
	OU	MobiSafe
	OU	EIK 131107204
	CN	SEP Root CA
	PostalAddress(2.5.4.16)	bul.Tsarigradsko shose 135
	PostalCode	1784
	Phone	00359 700 18283
	E	esign@mobisafe.bg
<b>validity</b>	notBefore	UTCTime формат
	notAfter	UTCTime формат
<b>subject (Distinguished Name)</b>	C	BG
	S	Sofia
	L	Sofia
	O	System for Electronic Payments /SEP Bulgaria/ JSC
	OU	MobiSafe
	OU	EIK 131107204
	CN	MobiSafe TSA
	PostalAddress(2.5.4.16)	bul.Tsarigradsko shose 135
	PostalCode	1784
Phone	00359 700 18283	
E	esign@mobisafe.bg	
<b>Key Usage</b>	digitalSignature, nonRepudiation	
<b>Enhanced Key Usage</b>	timeStamping	
<b>Certificate Policies</b>	Policies: 1.3.6.1.4.1.30299.1.1.5 CPSuri: <a href="http://e-sign.mobisafe.bg">http://e-sign.mobisafe.bg</a> UserNotice: explicitText: MobiSafe TSA	
	Policies: 1.3.6.1.4.1.30299 CPSuri: <a href="http://www.crc.bg/">http://www.crc.bg/</a> UserNotice: organization: SEP Bulgaria JSC explicitText: SEP Bulgaria JSC – registered certification service provider	
<b>CRL Distribution Points</b>	URL: <a href="http://crl.mobisafe.bg/mobisafe_root_ca.crl">http://crl.mobisafe.bg/mobisafe_root_ca.crl</a> URL=ldap://ldap.mobisafe.bg/cn=MobiSafe%20CA,ou=MobiSafe,dc=mobisafe,dc=bg	
<b>Authority Information Access</b>	OCSP: <a href="http://ocsp.mobisafe.bg">http://ocsp.mobisafe.bg</a>	
<b>Basic Constraints</b>	cA: no pathLenConstraint: 0	
<b>Issuer Alternative Names</b>		
<b>Subject Alternative Name</b>	URL: <a href="http://tsa.mobisafe.bg">http://tsa.mobisafe.bg</a> client service location	
<b>Authority Key Identifier</b>		
<b>Subject Key Identifier</b>		
<b>subjectPublicKeyInfo</b>	публичния ключ на титуляра/автора и алгоритъма с който се използва	
<b>signatureAlgorithm</b>	sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5)	
<b>signatureValue</b>	електронен подпис на ДУУ	

## 7.4 OCSP профил

Услугата по проверка статуса на издадените удостоверения, „СЕП България“ АД предоставя освен чрез достъп по СПУ 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 MobiSafe CA. MobiSafe 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 MobiSafe CA, за удостоверяване на статуса на издадено от „СЕП България“ АД удостоверение, са съгласно RFC 2560.

**Профила на удостоверението на MobiSafe OCSP е следния:**

ИМЕ НА ПОЛЕ	СТОЙНОСТ ИЛИ ОГРАНИЧЕНИЕ НА СТОЙНОСТТА	
<b>version</b>	Version 3	
<b>serialNumber</b>	уникален сериен номер на удостоверението в рамките на издаващия удостоверяващия орган	
<b>signature</b>	sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5)	
<b>issuer (Distinguished Name)</b>	C	BG
	S	Sofia
	L	Sofia
	O	System for Electronic Payments /SEP Bulgaria/ JSC
	OU	MobiSafe
	OU	EIK 131107204
	CN	MobiSafe CA
	PostalAddress(2.5.4.16)	bul.Tsarigradsko shose 135
	PostalCode	1784
	Phone	00359 700 18283
	E	esign@mobisafe.bg
<b>validity</b>	notBefore	UTCTime формат
	notAfter	UTCTime формат
<b>subject (Distinguished Name)</b>	countryName	BG
	stateOrProvinceName	Sofia
	localityName	Sofia
	organizationName	System for Electronic Payments /SEP Bulgaria/ JSC
	organizationalUnitName	MobiSafe
	organizationalUnitName	EIK 131107204
	commonName	MobiSafe OCSP
	PostalAddress	bul.Tsarigradsko shose 135
	postalCode	1784
	TelephoneNumber	00359 700 18283
emailAddress	esign@mobisafe.bg	
<b>Key Usage</b>	digitalSignature, nonRepudiation	
<b>Enhanced Key Usage</b>	OCSPSigning	

ИМЕ НА ПОЛЕ	СТОЙНОСТ ИЛИ ОГРАНИЧЕНИЕ НА СТОЙНОСТТА
<b>Certificate Policies</b>	Policies: 1.3.6.1.4.1.30299.1.1.6 CPSuri: <a href="http://e-sign.mobisafe.bg">http://e-sign.mobisafe.bg</a> UserNotice: explicitText: MobiSafe OCSP  Policies: 1.3.6.1.4.1.30299 CPSuri: <a href="http://www.crc.bg/">http://www.crc.bg/</a> UserNotice: organization: SEP Bulgaria JSC explicitText: SEP Bulgaria JSC – registered certification service provider
<b>CRL Distribution Points</b>	URL: <a href="http://crl.mobisafe.bg/mobisafe_ca.crl">http://crl.mobisafe.bg/mobisafe_ca.crl</a> URL=ldap://ldap.mobisafe.bg/cn=MobiSafe%20CA,ou=MobiSafe,dc=mobisafe,dc=bg
<b>Authority Information Access</b>	OCSP: <a href="http://ocsp.mobisafe.bg">http://ocsp.mobisafe.bg</a>
<b>Basic Constraints</b>	cA: no pathLenConstraint: 0
<b>Issuer Alternative Names</b>	
<b>Subject Alternative Name</b>	
<b>Authority Key Identifier</b>	
<b>Subject Key Identifier</b>	
<b>subjectPublicKeyInfo</b>	публичния ключ на титуляра/автора и алгоритъма с който се използва
<b>signatureAlgorithm</b>	sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5)
<b>signatureValue</b>	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.

Отговорите на запитванията за статуса на удостоверенията са според 4.8.6.

## **8 Проверка и контрол на дейността**

### **8.1 Честота и обстоятелства на проверките**

Контрол върху дейността на „СЕП България“ АД, като ДУУ съгласно ЗЕДЕП се осъществява от Комисията за регулиране на съобщенията.

„СЕП България“ АД осъществява постоянен вътрешен контрол, който се осъществява от упълномощени вътрешни одитори.

За целите на вътрешния контрол се извършват 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.

### **8.2 Идентификация и квалификация на проверяващите**

Лицата осъществяващи проверките са изрично упълномощени от Комисията за регулиране на съобщенията 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.

### **8.3 Избягване конфликт на интереси**

Проверяващите лица трябва да са независими в своята дейност от проверяваната организация или звено на „СЕП България“ АД.

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

### **8.4 Обхват и детайлност на проверките**

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

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

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

## **8.5 Предприемане на действия за отстраняване на недостатъците**

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

## **8.6 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.

## 9 Търговски и правни условия

### 9.1 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.mobisafe.bg>.

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

#### 9.1.1 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, то те не се възстановяват, ако услугата не се ползва.

#### 9.1.2 Възстановяване на суми

При приемане на удостоверението, ако Титуляра посочи грешки или непълноти, които не са по негова вина, „СЕП България“ АД прекратява удостоверението и издава ново безплатно без допълнително заплащане или възстановява направеното плащане.

## 9.2 Финансова отговорност

### 9.2.1 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 универсален 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.

### **9.2.2 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, както е посочено в точка 9.8.

Застраховката не покрива и Доставчикът не отговаря за случаите по точка 9.7 от Практика при предоставяне на удостоверителни услуги и в частност 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 дължима 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.

## **9.3 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.

### **9.3.1 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.

### **9.3.2 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.

### **9.3.3 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.

## **9.4 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. Събраната информация, включена в удостоверенията за електронен подпис и в списъка за прекратени удостоверения, може да съдържа лични данни по смисъла на Закона за защита на личните данни.

„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.

Информацията, която се събира, независимо дали ще се включи в съдържанието на УЕП или не, се събира само доколкото е необходима за нуждите на издаване и управление на удостоверенията и не може да бъде ползвана за други цели или предоставяна на трети лица, без изричното съгласие на предоставилите я лица или ако това е позволено със закон.

С подписване на Договора за удостоверителни услуги и приемането на разпоредбите на Наръчника за потребителя Титуляра и Автора се съгласяват личните им данни, събрани от ДУУ, да бъдат включени в удостоверението за универсален електронен подпис и да са общодостъпни за всички заинтересувани лица.

Информацията, която потребителите предоставят на ДУУ е защитена от разкриване освен в случаите посочени в споразумението с потребителя, съдебен акт или друго съобразено със законите искане.

## 9.5 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 възпроизведени 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.

## 9.6 Статут и гаранции

### 9.6.1 Статут и гаранции на „СЕП България“ АД

„СЕП България“ АД е ДУУ регистриран от Комисията за регулиране на съобщенията 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.

### 9.6.2 Статут и гаранции на регистриращите органи

РО действат от името и за сметка на „СЕП България“ АД, като „СЕП България“ АД носи цялата отговорност за тяхната дейност. 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 електронен подпис;
- Потвърдената от оператор РО информация и включена в издаденото удостоверение е точна и пълна и съответства на състоянието към момента на извършване на проверката.

### **9.6.3 Статут и гаранции на титуляра/автора**

Титуляра 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.

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.

### **9.6.4 Статут и гаранции 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 универсален 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.

## 9.7 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 УЕП и електронните подписи;
- Всякакви други вреди, освен тези, които са свързани с доверяване на информацията, посочена в дадения УЕП, базирана на потвърдената информация;
- Грешка в потвърдената информация, която е в следствие на измама или умишлено невярно изявление на поискалия издаването на удостоверението за електронен подпис;
- Използването на УЕП, 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.

## 9.8 Ограничение 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
<b>MobiSafe Private</b>	60 000 лева
<b>MobiSafe Organization</b>	60 000 лева
<b>MobiSafe Professional</b>	60 000 лева
<b>MobiSafe Server</b>	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 универсален електронен.

## **9.9 Обезщетения и компенсации**

Във всички случаи на неизпълнение на задълженията от страна на титуляра, произтичащи от Наръчника за потребителя или от Договора за удостоверителни услуги, „СЕП България“ АД ще предприеме мерки, за да бъде обезщетен за претърпени щети.

## **9.10 Срок на действие и прекратяване на действието**

### **9.10.1 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 не валидността 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.

### **9.10.2 Прекратяване действието на ППУУ**

Действието на практика при предоставяне на удостоверителни услуги се прекратява с прекратяване на дейността на „СЕП България“ АД като ДУУ.

В случай че някоя от клаузите на настоящата практика при предоставяне на удостоверителни услуги 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.

### **9.10.3 Последствия от прекратяване действието на ППУУ**

След прекратяване на действието на Практиката при предоставяне на удостоверителни услуги 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.

## **9.11 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.

„СЕП България“ АД приема съобщения в зависимост от техния тип по следния начин:

- Писмени съобщения – в регистриращите органи на „СЕП България“ АД от оператор РО, който регистрира подаденото съобщение;
- Писмени съобщения – по пощата, писмо с обратна разписка или по куриер на адрес:

Адрес: „СЕП България“ АД, гр. София, 1784,  
бул. „Цариградско шосе“ № 135  
Телефон: +359 700 18283  
Интернет сайт: <http://e-sign.mobisafe.bg>.

- Съобщения по електронна поща на: [esign@mobisafe.bg](mailto:esign@mobisafe.bg). Съобщението трябва да е подписано с универсален електронен подпис.

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 универсален електронен подпис.

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

## 9.12 Изменения и допълнения

„СЕП България“ АД, при необходимост променя и допълва тази практика. Практиката може да бъде променян по всяко време, като всяка промяна в него се отразява след одобрение от страна на 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 по предоставяне на удостоверителни услуги и Практика при предоставяне на удостоверителни услуги.

## 9.13 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, 1784,  
бул. „Цариградско шосе“ № 135.

В седемдневен срок от подаването на жалбата, Ръководител отдел „Бизнес операции“ 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 четиринадесет дневен срок от получаването, за което писмено уведомява жалбоподателя.

### **9.14 Приложимо законодателство**

За неуредените в настоящата Практика при предоставяне на удостоверителни услуги се прилага българското законодателство.

### **9.15 Съответствие със законовите изисквания**

„СЕП България“ АД се ръководи в своята дейност от ЗЕДЕП и подзаконовите актове по неговото прилагане. А за неуредените в тях случаи действащото българско законодателство. „СЕП България“ АД се ръководи при предоставяне на удостоверителните услуги от следните закони:

- Закон да електронния документ и електронния подпис и наредбите по неговото прилагане.
- Закон за защита на личните данни.
- Закон за защита на потребителите.

### **9.16 Допълнителни разпоредби**

#### **9.16.1 Правоприемство**

Правата и задълженията, посочени в тази практика 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 тази практика.

#### **9.16.2 Отделяне на условията**

Ако някоя от клаузите в тази практика или нейното прилагане се окаже недействителна или изпълнима изцяло или частично то клаузата ще бъдат тълкувани по такъв начин, че да отговарят на първоначалните намерения на страните.

#### **9.16.3 Тълкуване**

Тази Практика 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.

Заглавията и подзаглавията в тази практика са определени по този начин само за удобство и справки и не трябва да бъдат използвани при тълкуване или изпълнение на клаузите.

#### **9.16.4 Отказ от изпълнение**

Тази практика ще бъде изпълняван като цяло и ако някое от лицата не успее да изпълни някоя от клаузите, то това няма да бъде разглеждано като отказ от бъдещо изпълнение на тази или на други клаузи.

#### **9.16.5 Форсмажор**

Наличието на форсмажорни обстоятелства, води до отмяна на правата, произтичащи от тази Практика при предоставяне на удостоверителни услуги.

### **9.16.6 Юрисдикция**

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