СЕП България АД
София, 1784, бул. „Цариградско шосе” № 135
тел.: +359 700 18283
www.sepbulgaria.com

СЕП
Система за електронни плащания

„СЕП България” АД

София, 1784, бул. „Цариградско шосе” № 135
тел.: +359 700 18283, e-mail: esign@mobisafe.bg

Наръчник на потребителя

Политика по предоставяне на удостоверителни услуги

Версия: 3.2

Дата на публикуване: 30.03.2009 г.

Съдържание

Вие можете да изпращате Вашите коментари по тази „Политика по 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

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

1 Обхват

Този документ прави общ преглед на политиката по предоставяне на удостоверителни услуги на „СЕП България” АД в качеството му на регистриран доставчик на удостоверителни услуги(ДУУ). Представя общата концепция на „СЕП България” АД, относно предоставяне на удостоверителни услуги. Документа дефинира страните участници в процеса по предоставяне на удостоверителни услуги, техните задължения, типовете удостоверения за електронен подпис, процеса по проверка на самоличността съответно идентичността и областта на приложени на издадените удостоверения за електронен подпис(УЕП).

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

2 Ползвани източници

При разработката на „Политика по 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.

2.1 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".

2.2 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".

3 Определения и съкращения

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

3.1 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.

3.2 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
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
КИК	Код за идентификация на клиента

4 Общ преглед

„СЕП България" АД е доставчик на удостоверителни услуги, който работи в съответствие със Закона за електронния документ и електронния подпис (ЗЕДЕП) и подзаконовите нормативни актове, издадени по неговото прилагане.

„СЕП България" АД е регистриран, като ДУУ от Комисията за регулиране на съобщенията по реда определен от ЗЕДЕП и НАРЕДБА за реда за регистрация на доставчиците на удостоверителни услуги.

Регистрацията е под № 1170 от 17.07.2008 г .

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

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

„СЕП България" АД предоставя удостоверителни услуги посредством ***удостоверяващ орган*** и упълномощени ***регистриращи органи***.

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

Удостоверителните услуги на „СЕП България" АД се предоставят под търговската марка ***MobiSafe***.

4.1 Удостоверяващ орган

Доставчика на удостоверителни услуги „СЕП България" АД се идентифицира със своя удостоверяващ орган.

Удостоверяващия орган (УО) е трета доверена страна, която издава, публикува и управлява удостоверения за електронен подпис и предоставя достъп до тях на доверяващите се страни.

Удостоверяващият орган на „СЕП България" АД е отделна обособена организационна структура в рамките на „СЕП България" АД. Удостоверяващия орган носи цялата отговорност за предоставяне на удостоверителните услуги, като издава удостоверения за електронен подпис (УЕП) на физически, юридически лица и лица упражняващи свободни професии. Удостоверяващият орган извършва още дейности и по подновяване, спиране и възобновяване, прекратяване на УЕП, водене на регистър и осигуряване на достъп до него и удостоверяване на време.

Удостоверяващия орган се идентифицира в УЕП, като техен издател и използва частния си ключ за подписване на издаваните УЕП.

Удостоверяващия орган използва подизпълнители за предоставяне на част от дейностите по предоставяне на удостоверителните си услуги, като винаги носи

цялата отговорност и осигурява прилагането на всички изисквания посочени в настоящия документ.

4.2 Регистриращи органи

Удостоверяващият орган 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 идентичността.

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

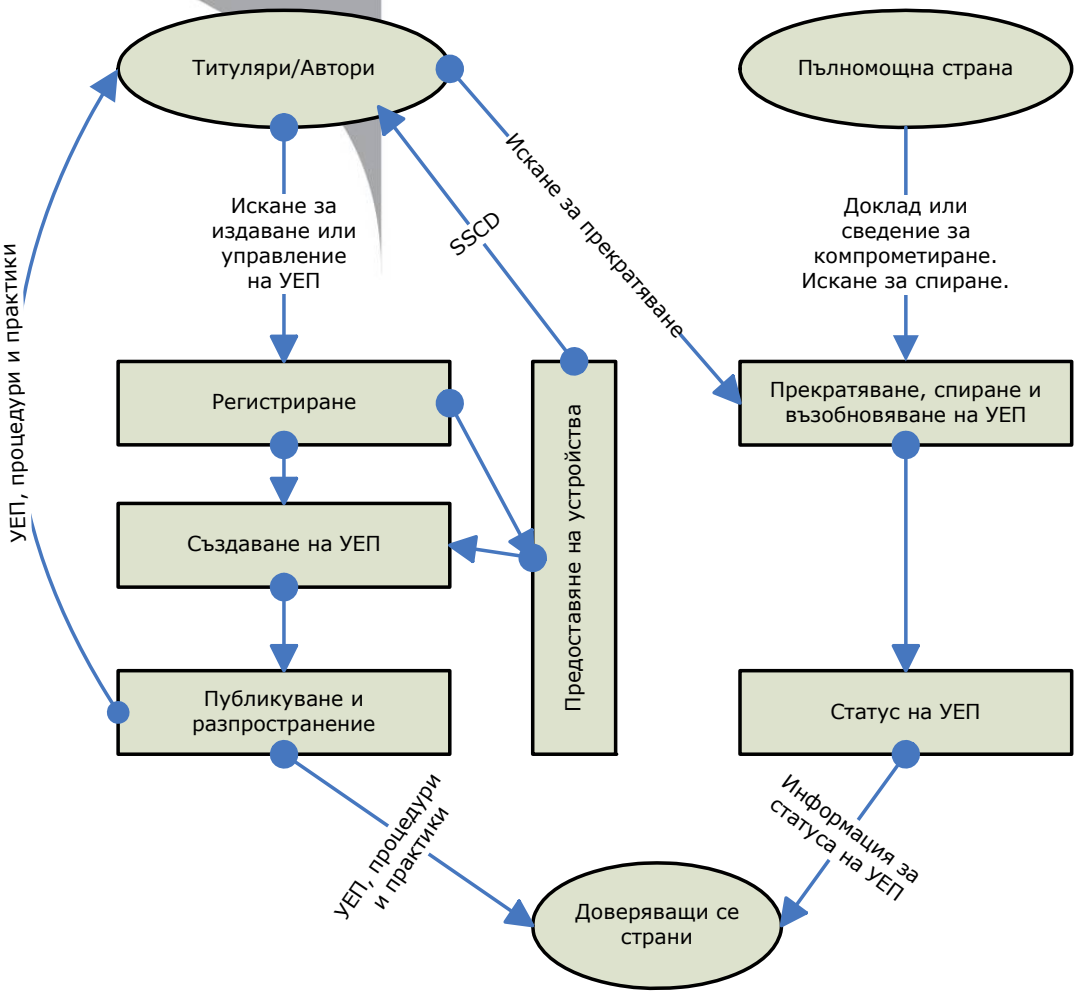
4.3 Модел на удостоверителни услуги

„СЕП България" АД следва следния технологичен модел за предоставяне на удостоверителни услуги.

Дефинирани са следните услуги от технологична гледна точка:

- **Регистриране** – приемане на искането за издаване на УЕП, проверка чрез допустимите средства самоличността, съответно идентичността, на автора и на титуляра и ако е необходимо - други данни за тези лица, включени в удостоверението. Обработване на подадените искания за управление за отразяване на промените, спиране, възобновяване, прекратяване на издадени УЕП. Проверява самоличност съответно идентичност и специфични данни за заявителите на УЕП. Резултата от тази услуга се изпраща към услугата по създаване на УЕП.
- **Създаване на УЕП** – създаване и подписване УЕП, базирано на данните проверени от услугите по регистриране. Публикуване в списък с издадените УЕП.
- **Публикуване и разпространение** – предоставяне на УЕП на титулярите/авторите и при съгласие на автора предоставя на информация за УЕП на доверяващите се страни. Тази услуга публикува политиките и практиките на доставчика по отношение на удостоверителните услуги и списъка с прекратените удостоверения.
- **Прекратяване на УЕП** – управляване исканията и реагиране при докладване на сведения свързани със спиране и/или прекратяване на УЕП. В резултат се предприемат действия по прекратяване или спиране/възобновяване на УЕП.
- **Статус на УЕП** – предоставяне на информация за статуса на УЕП на доверяващите се страни. Използват се списъци с прекратени УЕП или услуги предоставящи информация за статуса на УЕП в реално време. Информацията за статуса на УЕП се обновява на зададен период.

- **Предоставяне на устройства** – това може да бъдат смарт карти или други устройства за сигурно създаване на електронен подпис. Устройствата се подготвят и предоставят на авторите пряко или по сигурен начин чрез титуляра. Това може да бъдат услуги по създаване и предоставяне на ключова двойка на авторите или по подготовка, генериране и предоставяне на титулярите/авторите на устройства и необходимите данни за активиране.
- **Удостоверяване на време** – предоставяне на услуги по удостоверяване на време за целите на проверка на електронния подпис.



4.4 Удостоверителна политика и практика

В качеството си на ДУУ „СЕП България” АД опериращ на територията на република България, разработва за тази цел „Наръчник на потребителя”, който включва:

- „Политика по предоставяне на удостоверителни услуги”;
- „Практика при предоставяне на удостоверителни услуги”.

„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.

„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.

4.4.1 Предназначение

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.

4.4.2 Ниво на детайлност

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

Практика при предоставяне на удостоверителни услуги, детайлно описва следваните практики от ДУУ при предоставяне на удостоверителни услуги и посочва как се реализират общите изисквания към ДУУ.

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

4.4.3 Подход

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

Практика при предоставяне на удостоверителни услуги е свързана с организационната структура, операционните процедури, помещенията, компютърното и комуникационно обкръжение на УО на ДУУ.

4.4.4 Документи по отношение на трети страни

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

- „Правилата за издаване на удостоверения, включително правилата за установяване идентичността на титуляра на универсалния електронен подпис";
- „Условията и редът за използване на универсалния електронен подпис, включително изискванията за съхраняване на частния ключ";
- „Договор за предоставяне на удостоверителни услуги".

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

4.4.5 Процедури за сигурност

СЕП България" АД разработва и поддържа в съответствие с тази политика и в съответствие със ЗЕДЕП и подзаконовите нормативни актове, издадени по неговото прилагане:

- „Процедури за сигурност, прилагани при издаването и ползването на универсалния електронен подпис".

Документа не е публичен и достъп до него имат само служители на КРС и упълномощени от тях лица.

4.5 Титуляр и Автор

4.5.1 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.

4.5.2 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.

4.5.3 Разграничаване на титуляр/автор

Когато УЕП е издадено на физическо лице за лично ползване то се явява титуляр и автор т.е. 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 т.е. титуляра и автора се различават.

4.6 Типове издавани удостоверения

Според тази политика се издават удостоверения за електронен подпис. Всеки тип удостоверение издадено според тази политика се идентифицира с уникален идентификатор.

4.6.1 Удостоверения за универсален електронен подпис

4.6.1.1 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 транзакции 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.

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

4.6.1.3 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.

4.6.2 Специализирани удостоверения за електронен подпис

4.6.2.1 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 представител/ли да следят за правилно и надеждно функциониране на информационната система.

5 Политика по предоставяне на удостоверителни услуги

5.1 Общи сведения

Политиката по предоставяне на удостоверителни услуги представлява определен набор от правила, които показват приложимостта на удостоверенията за електронен подпис за конкретна общност и/или клас от приложения с общи изисквания за сигурност.

В тази удостоверителна политика са представени:

- Общия подход по предоставяне на удостоверителни услуги от „СЕП България” АД;
- Общите характеристики на политиката по предоставяне на удостоверителни услуги от „СЕП България” АД;
- Задължения, отговорност и необходима информация за страните участващи в удостоверителния процес;
- Изискванията към дейността на доставчика на удостоверителни услуги и използваните от него подходи и технология.

Тази удостоверителна политика е за удостоверения за универсален електронен подпис в съответствие със ЗЕДЕП и за специализирани удостоверения както е посочено в 4.6.

УЕП издадени в съответствие с тази политика, включват идентификатор, който може да се използва от доверяващите се страни, за да определят приложимостта и доверието за приложение.

В този документи се дефинира следната удостоверителна политика:

„Удостоверителна политика за удостоверения за универсален електронен подпис, изискваща използването на устройства за сигурно създаване на подпис и за специализирани удостоверения за целите на идентификация”

5.2 Идентификация

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

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

5.2.1 Идентификатор на политиката

Идентификатора на удостоверителна политика е:

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

OID: 0.4.0.1456.1.1

OID: 1.3.6.1.4.1.30299.1.1

5.2.2 Идентификатори на политика за типовете удостоверения

Отделните типове УЕП се идентифицират чрез допълнителен идентификатор на типа УЕП издаван от „СЕП България” АД. Идентификаторите са както следва:

MobiSafe Private

OID: 1.3.6.1.4.1.30299.1.1.1

MobiSafe Organization

OID: 1.3.6.1.4.1. 30299.1.1.2

MobiSafe Profession

OID: 1.3.6.1.4.1. 30299.1.1.3

MobiSafe Server

OID: 1.3.6.1.4.1. 30299.1.1.4

Идентификаторите на политиката, според която се издават различните типове удостоверения се включват в съдържанието на всяко издадено удостоверение в съответствие с тази политика и конкретен тип удостоверение.

5.3 Потребителска общност и приложение на УЕП

УЕП от типа посочен в **4.6.1**, издадени в съответствие с тази Политика имат смисъла на удостоверения за универсален електронен подпис съгласно ЗЕДЕП.

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

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

5.4 Спазване на политиката

5.4.1 Общи сведения

ДУУ използва идентификатора, дефиниран в 5.2.1, само за доказване на съответствие с тази удостоверителна политика.

5.4.1.1 Доказателства за спазване на политиката

ДУУ при поискване от участниците в удостоверителния процес, предоставя доказателства за спазване на тази политика. Това може да бъдат както регистрация на ДУУ в Комисията за регулиране на съобщенията така и резултати от вътрешни одити и проверки.

5.4.1.2 Одит от трета страна

В случай че са налични одити от трета страна, ДУУ при поискване от участниците в удостоверителния процес, предоставя доказателства за спазване на тази политика. Това могат да бъдат резултати от одити и проверки на оторизирани органи.

5.4.1.3 Несъответствия

В случай, че ДУУ не отговаря на изискванията посочени в тази политика и ако това е предписано от проверяващия орган, се спира издаването на УЕП с включен идентификатор, като е посочено в 5.2.1.

Предприемат се незабавни мерки по отстраняване на несъответствието, като се спазва предписаното от проверяващия орган.

5.4.1.4 Проверка на съответствието

Съответствието на ДУУ с тази политика се проверява периодично или при настъпване на важни промени в дейността му.

5.4.2 Съответствие с политиката

Спазването на тази политика от ДУУ означава, че:

- ДУУ спазва всички задължения като са дефинирани в точка **6.1** Задължения на ДУУ
- ДУУ е реализирал контроли, които удовлетворяват всички изисквания дефинирани в точка **7.** Изисквания към дейността на ДУУ.

6 Задължения и отговорности

6.1 Задължения на ДУУ

„СЕП България” АД осигурява спазването на всички изисквания за дейността, детайлизирани в точка **7. ”**Изисквания към дейността на ДУУ**”**, за да реализира спазването на тази удостоверителна политика.

„СЕП България” АД носи цялата отговорност за спазването на процедурите разработени в съответствие с тази политика, включително и при използване на подизпълнители.

„СЕП България” АД осигурява всички удостоверителни услуги съгласно своята „Практика при предоставяне на удостоверителни услуги”.

6.2 Задължения на титуляра/автора

„СЕП България” АД урежда отношенията си с потребителите на своите услуги чрез договор.

„СЕП България” АД сключва договор с титуляра, в който отразява неговите задължения. Ако титуляра и автора се различават, то титуляра трябва да доведе до знанието на автора задълженията, които се отнасят и за него от посочени по-долу:

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

б) Да използва ключовата двойка само за електронен подпис и в съответствие с всяко друго ограничение, за което титулярът е информиран (виж точка 7.3.4);

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

г) Ако титуляра/автора генерират сами двойката ключове:

a. Да използват алгоритми одобрени като подходящи за целите на универсалния електронен подпис;
b. Да използват дължина на ключовете одобрена като подходяща за целите на универсалния подпис за времето на валидност на УЕП;
c. Частният ключ на автора да бъде използван единствено под контрола на автора;
d. Ако политиката по предоставяне на удостоверителни услуги изисква използването на SSCD, да използва УЕП само с електронни подписи създадени с използването на такова устройство;

д) Да уведоми ДУУ незабавно, ако настъпи някое от следните събития преди края на периода на валидност посочен в удостоверението:

a. Загуба на частния ключ на автора, кражба, съмнение за компрометиране;
b. Загубен контрол върху частния ключ на автора поради компрометиране на данните за активиране (т.е. ПИН) или по друга причина;
c. Невярно, непълно или променено съдържание на удостоверението.

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

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

6.3 Информация за доверяващите се страни

Доверяващите се страни са лица 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.

Реда и условията на удостоверителните услуги предоставяни на доверяващите се страни трябва ясно да посочват, че разумното доверяване на УЕП, означава:

- Да се провери валидността, спирането или прекратяването на УЕП, като се използва актуална информация за статуса предоставена от ДУУ (виж точка 7.3.4);
- Да се вземат предвид както всички ограничения на използването на УЕП предоставени на доверяващите се страни в УЕП, така и реда и условията предоставени на доверяващите се страни в публикуваните документи на доставчика (виж точка 7.3.4);
- Да вземе всички предпазни мерки посочени в регламентиращите документи на ДУУ (виж точка 4.4.4).

6.4 Законово съответствие

Дейността на „СЕП България” АД по издаване на удостоверения за универсален електронен подпис е в съответствие със ЗЕДЕП и подзаконовите актове по неговото прилагане.

7 Изисквания към дейността на ДУУ

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

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

7.1 Практика при предоставяне на удостоверителни услуги

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

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

В съответствие с тази политика, „СЕП България” АД в своята „Практика при предоставяне на удостоверителни услуги” декларира, че:

а) Спазва ЗЕДЕП и подзаконовата нормативна уредба, както и всички практики и процедури, разработени въз основа на изискванията посочени в тази политика;

б) Посочва всички задължения на трети лица имащи отношение към предоставяне на удостоверителните услуги, включително приложимите политики и практики;

в) Публикува и осигурява достъп както до своята Практика при предоставяне на удостоверителни услуги на всички потребители на удостоверителни услуги, така и до други документи необходими за определяне на съответствието с удостоверителната политика;

г) Публикува и осигурява достъп до условията и реда за ползване на УЕП, както е посочено в 7.3.4;

д) Определя висш ръководен орган, който управлява и одобрява практики при предоставяне на удостоверителни услуги, съгласно тази политика и ги представя пред КРС за одобрение;

е) Ангажира висшето ръководство и неговата отговорност по отношение на установяване и спазване на практиките при предоставяне на удостоверителни услуги;

ж) Дефинира процес по преглед на практиките при предоставяне на удостоверителни услуги, включително отговорности по поддръжката им;

з) Информира незабавно за настъпили промени в своята „Практика при предоставяне на удостоверителни услуги”, одобрението съгласно **(д)** по горе, и публикува ревизираната ППУУ като се изисква във **(в)**;

и) Документира използваните алгоритми и техните параметри.

7.2 Инфраструктура за доставка на удостоверителни услуги – Управление на ключовете

7.2.1 Генериране на ключовете на ДУУ

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

7.2.1.1 Защитена среда

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

7.2.1.2 Упълномощен персонал

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

7.2.1.3 Поделяне на секретни части

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

7.2.1.4 Надеждни системи

„СЕП България" АД използва надеждни системи при предоставяне на своите удостоверителни услуги и генерация на ключовите си двойки. Надеждната система представлява компютърен хардуер, софтуер и процедури, които осигуряват приемливо ниво на защита срещу рискове, свързани със сигурността, предоставя разумно ниво на работоспособност, надеждност, правилно опериране и изпълнение на изискванията за сигурност.

7.2.1.5 Генериране на ключовете на „СЕП България" АД

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

7.2.1.6 Стартова процедура

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

7.2.1.7 Криптографски хардуер

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

7.2.1.8 Ползвани алгоритми

Ключовете на „СЕП България” АД се генерират, като се използват алгоритми признати за подходящи за целите на издаване на удостоверения за универсален електронен подпис и отговарят на изискванията на „Наредба за изискванията към алгоритмите за усъвършенстван електронен подпис”.

7.2.1.9 Дължина на ключа

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

7.2.1.10 Гарантиране непрекъснатост на операциите

Достатъчно време преди края на периода на валидност на ключовете, подписващи издаваните УЕП, „СЕП България” АД генерира нова ключова двойка за подписване на удостоверения и прилага всички необходими мерки, за да избегне прекъсване на операциите на всяка страна, която може да разчита на ключовете на УО. Новите ключове се генерират и разпространяват в съответствие с тази политика.

7.2.2 Съхраняване, архивиране и възстановяване ключове на ДУУ

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

7.2.2.1 Държане и ползване на частния ключ

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

7.2.2.2 Защита на частния ключ

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

7.2.2.3 Архивиране на частния ключ

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.

7.2.2.4 Копия на частния ключ

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

7.2.2.5 Съхраняване на частните ключове на ДУУ

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

7.2.3 Разпространяване на публичните ключове на ДУУ

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

7.2.3.1 Източник и интегритет на публичния ключ

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

7.2.4 Защита частния ключ на доставчика

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

7.2.5 Използване на ключовете на ДУУ

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

7.2.5.1 Използване на частния ключ

Частните ключове на ДУУ, използвани при генерация на УЕП както е посочено в точка 7.3.3, може да се използва за подписване и на други типове УЕП, както и на информацията за статуса на издадените УЕП дотолкова, доколкото не са нарушени изискванията дефинирани в точки 7.2.1 до 7.2.3, 7.2.5 до 7.2.7 и 7.4.

7.2.5.2 Физическа защита

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

7.2.6 Прекратяване на жизнения цикъл на ключове на ДУУ

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

7.2.6.1 Унищожаване на подписващите ключове

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

7.2.7 Жизнен цикъл на криптографския хардуер ползван за подписване на УЕП

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

7.2.7.1 Доставка на криптографски хардуер

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

7.2.7.2 Съхранение на криптографски хардуер

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

7.2.7.3 Съвместен контрол

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

7.2.7.4 Функциониране на криптографския хардуер

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

7.2.7.5 Унищожаване на частните ключове в криптографския хардуер

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

7.2.8 Осигуряване на титуляра/автора услуги по управление на ключовете

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

7.2.8.1 Използвани алгоритми

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

7.2.8.2 Дължина на ключовете

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

7.2.8.3 Съхраняване на генерираните ключове

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

7.2.8.4 Предоставяне на ключовете

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

7.2.9 Подготовка на SSCD

ДУУ осигурява сигурно и надеждно издаване на УЕП чрез SSCD.

7.2.9.1 Контрол при подготовката на SSCD

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

7.2.9.2 Съхраняване и предоставяне на SSCD

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

7.2.9.3 Деактивация и реактивация на SSCD

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

7.2.9.4 Данни за активиране

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

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

7.3 Инфраструктура за доставка на удостоверителни услуги – Управление жизнения цикъл на УЕП

7.3.1 Регистрация на титуляра/автора

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

7.3.1.1 Предоставяне на информация за удостоверителните услуги

Преди да се подпише договор за удостоверителни услуги с титуляра, ДУУ информира титуляра за реда и условията относно използването на удостоверението, като е посочено в точка 7.3.4.

7.3.1.2 Канали за информиране

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

7.3.1.3 Проверка регистрация

ДУУ проверява по време на регистрацията чрез допустими средства, в съответствие с националното законодателство, самоличността съответно идентичността и ако е приложимо и други данни за лицето, на което се издава удостоверението за универсален електронен подпис. Проверката на доказателствата за идентичността на физическото лице, може да се извърши както пряко така и непряко като се използват средства осигуряващи сигурност еквивалентна на физическо присъствие. Представените доказателства може да са както в хартиена така и под форма на електронен документ.

7.3.1.4 Идентификация на физически лица

Физическите лица, трябва да представят доказателства за:

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

7.3.1.5 Идентификация на юридически лица

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

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

- Пълното име и юридическия статус на свързваното юридическо лице или организация – титуляр;
- Всякаква приложима регистрационна информация или информация от регистър;
- Доказателство, че физическото лице – автор представлява юридическото лице или организация – титуляр.

7.3.1.6 Съхранявана информация

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

7.3.1.7 Данни за представителство

Ако заявката за издаване на УЕП се подава от страна различна от автора (т.е. титуляра и авторът са различни – виж точка 4.5), тогава трябва да се представят доказателства, че подалия искането е упълномощен да действа от името на идентифицирания в УЕП автор.

7.3.1.8 Данни за обратна връзка

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

7.3.1.9 Договорни отношения

ДУУ пази подписан договор с абоната, който включва:

- Съгласие със задълженията на абоната (виж 6.2);
- Съгласие за ползване на SSCD;
- Съгласие ДУУ да съхранява записи от информация използвана за регистрация(виж 7.4.11.8, 7.4.11.9, 7.4.11.10), предоставяне на SSCD (виж 7.4.11.12, 7.4.11.13) и следващи действия по прекратяване (виж 7.4.11.14), идентичността и специфични атрибути на субекта поместени в удостоверението и предоставянето на тази информация на трета страна при същите условия, както се изисква в тази политика, в случай че ДУУ прекратява своята дейност;
- Дали и при какви условия титуляра изисква и автора дава съгласие за публикуване на удостоверението;
- Потвърждение, че информацията съдържаща се в удостоверението е вярна и точна.

7.3.1.10 Време за съхранение

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

7.3.1.11 Притежание на частния ключ

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

7.3.1.12 Притежание на SSCD

Ако ДУУ не е генерирал ключовата двойка и удостоверителната политика изисква използването на SSCD, процеса по заявяване издаване на

удостоверение гарантира, че публичния ключ предоставен за удостоверяване е генериран чрез SSCD.

7.3.2 Подновяване, смяна на ключове и актуализиране

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

7.3.2.1 Актуален УЕП

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

7.3.2.2 Променени условията на „СЕП България" АД

Ако някои от условията и реда на ДУУ са променени то те се съобщават на титуляра и той трябва да ги приеме в съответствие с точки 7.3.1.1, 7.3.1.2, 7.3.1.9.

7.3.2.3 Променено съдържание на УЕП

Ако някое от имената в удостоверението или данни са променени или предишното удостоверение е било прекратено то информацията за регистрация се проверява, записва и титуляра ги приема в съответствие с точки 7.3.1.3 до 7.3.1.7.

7.3.2.4 Запазване на ключовата двойка

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

7.3.3 Създаване на удостоверение

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

7.3.3.1 Профил на УЕП

Удостоверенията издавани в съответствие с тази удостоверителна политика съдържат:

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

- Усъвършенствания електронен подпис на ДУУ издал удостоверението;
- Ако е приложимо ограничение на обхвата на приложение на удостоверението;
- Ако е приложимо ограничение на размера на транзакциите, за които удостоверението може да се използва;

7.3.3.2 Мерки срещу фалшифициране на УЕП

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

7.3.3.3 Приемственост на процедурите

Процедурата по издаване на удостоверение се разглежда като едно цяло със свързаните с нея процедури по регистрация, подновяване или смяна на ключ, включително предоставяне на публичен ключ генериран от автора.

7.3.3.4 Сигурна генерация

Ако ДУУ генерира ключовете на автора то:

- Процедурата по издаване на удостоверение се разглежда заедно с процедурата по генериране на ключова двойка от ДУУ;
- Частния ключ (или SSCD – виж 7.2.9) по сигурен начин се предава на автора.

7.3.3.5 Уникалност на имената

ДУУ осигурява през цялото време уникалността на присвояваните от него имена на титуляри/автори **(Distinguished Name)**. По време на жизнения цикъл на ДУУ **Distinguished Name**, което е било използвано в издадено удостоверение никога не трябва да се използва отново.

7.3.3.6 Конфиденциалност и интегритет на данните за регистрация

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

7.3.3.7 Проверка на източника на регистрационните данни

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

7.3.4 Разпространяване на реда и условията

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

7.3.4.1 Публикувана информация

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

- Приложението на удостоверителна политика за издаване на удостоверения за универсален електронен подпис с използване на SSCD.
- Ограничения в използването;
- Задълженията на абоната както са дефинирани в точка 6.2 включително дали прилагането на политиката изисква използването на SSCD;

- Информация как да се провери удостоверението, включително изискването да се проверява списъка с прекратени удостоверения, така че доверяващите се страни имат предвид „разумно доверяване” на удостоверенията (виж точка 6.3);
- Ограниченията в отговорността включително целите/употребата за които ДУУ приема (или изключва) юридическа отговорност;
- Периода от време, през който информацията за регистрацията се съхранява(виж точка 7.3.1);
- Периода от време, през който ДУУ пази журналите със записите от събитията(виж точка 7.4.11);
- Процедурите за подаване на жалби, оплаквания и решаване на юридически спорове;
- Приложимото законодателство;
- Информация за регистрация на ДУУ от КРС или други сертификации за съответствие с тази политика, като се посочи и според коя схема.

7.3.4.2 Достъпност и разпространение на информацията

Информацията посочена в 7.3.4.1 по-горе е достъпна през цялото време за целите на комуникацията, може да бъде предавана електронно и използва ясен и разбираем език.

7.3.5 Публикуване на издадените УЕП

ДУУ предоставя на разположение, когато е необходимо на титуляра, автора и доверяващите се страни, издадените УЕП.

7.3.5.1 Достъп при генерация

След генерацията, цялото и вярно удостоверение е достъпно за титуляра или автора в зависимост от това за кой е бил издадено удостоверението.

7.3.5.2 Ограничаване на достъпа

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

7.3.5.3 Информация за доверяваща се страна

ДУУ предоставя на доверяващата се страна реда и условията за използване на удостоверенията (виж точка 7.3.4).

7.3.5.4 Идентифициране на приложимия ред и условия за УЕП

Приложимите ред и условия се идентифицират лесно за всеки отделен тип удостоверение.

7.3.5.5 Предоставяне на информация за УЕП

Информацията определена в 7.3.5.2 и 7.3.5.3 по горе е достъпна 24 часа на ден 7 дни в седмицата. След авария на системата, услуги или други поради други фактори, които не са под контрола на ДУУ, ДУУ ще положи максимални усилия, за да осигури престой на тези информационни услуги не повече, отколкото е максималният период от време посочен в практиката при предоставяне на удостоверителни услуги.

7.3.5.6 Публичност и достъпност на информацията за УЕП

Информацията определена в 7.3.5.2 и 7.3.5.3 е публична и достъпна за всички.

7.3.6 Прекратяване, спиране и възобновяване на УЕП

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

7.3.6.1 Документиране на процедурата

ДУУ документира като част от своята практика на доставчика при предоставяне на удостоверителни услуги (виж точка 7.1) процедурите по прекратяване на удостоверения, включително:

- Кой може да подава сведения и искане за прекратяване;
- Как се подават сведения и искания за прекратяване;
- Изисквания за допълнителни потвърждаване на сведенията и исканията за прекратяване;
- Дали и поради каква причина удостоверението може да бъде спряно;
- Механизмите използване за разпространяване на информация за прекратените удостоверения;
- Максималното закъснение, между приемане на искане за прекратяване или сведение за компрометиране и промяната в информацията за статуса на прекратените удостоверения, след което информацията става достъпна за доверяващите се страни.

7.3.6.2 Приемане на искания за прекратяване/спиране

Исканията и сведенията относно прекратяването се обработват веднага при постъпването.

7.3.6.3 Проверка на заявките

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

7.3.6.4 Спиране на УЕП преди прекратяване

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

7.3.6.5 Информиране за промяна на статуса

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

7.3.6.6 Необратимост на прекратяването

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

7.3.6.7 Списък със спрени и прекратени удостоверения

Списъка със спрени и прекратените удостоверения трябва да се публикува най-много през три часа и:

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

7.3.6.8 Достъпност на списъка с прекратени удостоверения

Услугите по управление на статуса на прекратените удостоверения са достъпни 24 часа на ден, 7 дни в седмицата. След авария на системата, услуги или поради други фактори, които не са под контрола на ДУУ, ДУУ ще положи максимални усилия, за да осигури престой на тези информационни услуги не повече, отколкото е максималният период от време посочен в практиката при предоставяне на удостоверителни услуги.

7.3.6.9 Статус на удостоверенията за електронен подпис

Информацията за статуса на удостоверения е достъпна 24 часа на ден, 7 дни в седмицата. След авария на системата, услуги или поради други фактори, които не са под контрола на ДУУ, ДУУ ще положи максимални усилия, за да осигури престой на тези информационни услуги не повече, отколкото е максималният период от време посочен в практиката при предоставяне на удостоверителни услуги.

7.3.6.10 Интегритет и автентичност на информацията за статуса на УЕП

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

7.3.6.11 Публикуване на информация за статуса на УЕП

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

7.3.6.12 Период на съхранение на прекратените УЕП в СПУ

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

7.4 Ръководство и управление на ДУУ

7.4.1 Управление на сигурността

ДУУ прилага административни и управленски процедури в съответствие с общоприети стандарти.

7.4.1.1 Анализ на риска

ДУУ извършва оценка на риска, за да оцени бизнес риска и да определи необходимите изисквания към сигурността и оперативни процедури. Анализа на риска периодично се преглежда и ревизира при нужда.

7.4.1.2 Използване на подизпълнители

ДУУ носи отговорност за всички аспекти от дейността по предоставяне на удостоверителни услуги дори ако някои функции се изпълняват от подизпълнители. Отговорностите на третите страни са ясно дефинирани от ДУУ и са предприети подходящи мерки, за да се гарантира, че третите страни са обвързани с реализирането на изискваните контроли от ДУУ.

7.4.1.3 Орган по информационна сигурност

Висшето ръководство на „СЕП България” АД осигурява ръководство на информационната сигурност чрез подходящ форум на високо ниво, който е отговорен за дефиниране на политиката за информационна сигурност на ДУУ и осигурява публикуването и запознаването с политиката на всички служители, за които тя се отнася.

7.4.1.4 Качество на услугите

ДУУ внедрява система за управление на качеството и информационната сигурност подходяща за услугите, които предлага.

7.4.1.5 Непрекъснатост на управлението

Инфраструктурата за информационна сигурност необходима за управление на информационната сигурност в рамките на ДУУ се поддържа постоянно. Всички промени които могат да имат влияние върху нивото на осигуряваната сигурност се одобряват от форума на ДУУ.

7.4.1.6 Реализация на контролите

Контролите и оперативните процедури за помещенията на ДУУ, системите и информационните активи осигуряващи удостоверителните услуги се документират, изпълняват и поддържат.

7.4.2 Класификация и управление на активите

ДУУ защитава своята информация и активи по подходящ начин в зависимост от тяхната чувствителност.

7.4.2.1 Класификация на информационните активи

ДУУ описва всичките си информационни активи и ги класифицира в съответствие с резултата от анализа на риска.

7.4.3 Сигурност на персонала

„СЕП България" АД предприема мерки, за да гарантира, че персонала и практиките по наемане на персонал са в съответствие с необходимостта от изграждане на доверие в операциите на ДУУ.

7.4.3.1 Наемане на персонал

ДУУ разполага с достатъчно персонал притежаващ експертни знания, опит и необходимата квалификация за предлаганите услуги и назначени на подходящи длъжности.

7.4.3.2 Дисциплинарни мерки

Ако персонала наруши политиките и практиките на ДУУ се налагат подходящи дисциплинарни санкции.

7.4.3.3 Разработка на длъжностни характеристики

В длъжностните характеристики се документират свързаните със сигурността роли и отговорности по начин определен в политиката за информационна сигурност на ДУУ. Доверените роли, от които зависят сигурността на операциите на ДУУ се дефинират ясно.

7.4.3.4 Длъжностни характеристики

Постоянния и наетия персонал на ДУУ имат длъжностни характеристики дефинирани от гледна точка на разделение на отговорностите и минимум привилегии, определят отговорностите на позицията базирайки се на задълженията и нивото на достъп, образованието, проучване на кандидата, обучение. Където е възможно се прави разлика между общи и специфични функции на ДУУ.

7.4.3.5 Обучение на персонала

Персонала се запознава с административните и управленски процедури, които се прилагат заедно с процедурите по информационна сигурност на ДУУ.

7.4.3.6 Ръководен персонал

Ръководния персонал са лица притежаващи опит и обучени в областта на технологиите за електронен подпис и добре познаващи процедурите за сигурност с опит в областта на сигурността на информацията и оценка на риска до степен достатъчна, за да изпълняват управленски функции.

7.4.3.7 Избягване конфликт на интереси

Целия персонал на ДУУ на доверени роли е свободен от конфликти на интереси, които могат да доведат до съмнение в безпристрастното изпълнение на задълженията им.

7.4.3.8 Доверени роли

Доверените роли включват следните отговорности:

- Администратор по сигурността: цялата отговорност за администриране реализирането на практиките по сигурността. Допълнително одобрява генерацията/прекратяването/спирането на удостоверения;
- Системен администратор: упълномощен на инсталира, конфигурира и поддържа системата на ДУУ за регистриране, генерация на удостоверения, предоставяне на SSCD и управление на статуса на прекратените удостоверения;
- Системен оператор: отговорен за ежедневните операции на системата на ДУУ. Упълномощен да архивира и възстановява системата.
- Системен контрольор: упълномощен да преглежда архивите и журналите на системата на ДУУ.

7.4.3.9 Обвързване с доверена роля

Персонала на ДУУ се назначава на доверена роля след одобрение от висшето ръководство отговорно за информационната сигурност.

7.4.3.10 Проверка на персонала

ДУУ 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.

7.4.4 Физическа сигурност и сигурност на прилежащата среда

ДУУ контролира физическия достъп до критичните си приложения и минимизира рисковете свързани с физическата сигурност.

7.4.4.1 Достъп до защитените помещения

Физическия достъп до помещенията ангажирани с генерацията на удостоверения, подготовката на SSCD и услугите по предоставяне на информация за статуса на УЕП е ограничен до надлежно упълномощени лица.

7.4.4.2 Реализиране на контролите

Контролите се реализират по такъв начин, че да се избегнат загуби, повреди или компрометиране на активи и прекъсване на бизнес дейностите.

Контролите се реализират по такъв начин, че да се избегне компрометиране или кражба на информация и устройства за обработка на информацията.

7.4.4.3 Прилежаща среда на защитените помещения

Помещенията ангажирани с генерацията на удостоверения, подготовката на SSCD (7.2.9) и услугите по предоставяне на информация за статуса на прекратените УЕП, се намират във физически защитена среда, която да защитава услугите от компрометиране чрез неупълномощен достъп до системите и данните.

7.4.4.4 Постоянно наблюдение

Всяко лице намиращо се във физически защитения периметър не се оставя без наблюдение за значителен период от време, без да се наблюдава от друго упълномощено лице.

7.4.4.5 Дефиниране на защитени периметри

Физическата защита се постига чрез създаването на ясно дефинирани периметри за сигурност, физически бариери, около услугите по генерацията на удостоверения, подготовката на SSCD (7.2.9) и услугите по предоставяне на информация за статуса на УЕП. Всички части от помещенията, които се използват от други организационни единици са извън този периметър.

7.4.4.6 Множество защити

Контролите на физическата защита и защитата на прилежащото обкръжение са реализирани така, че да предпазват помещенията, в които се намират системните ресурси, самите системни ресурси и помещенията използвани за поддържане на тяхната работоспособност. Политиката за физическа сигурност на ДУУ и за защита на прилежащото обкръжение на услугите по генерацията на удостоверения, подготовката на SSCD (7.2.9) и услугите по предоставяне на информация за статуса на УЕП, включва физическия контрол на достъп, защита от природни бедствия, пожар, повреда с поддържащите системи - електрозахранване и комуникация, разрушаване на сградите, повреда във водопровода, защита срещу кражби, насилствено влизане, възстановяване след бедствие и др.

7.4.4.7 Изнасяне на активи

Контролите са реализирани така, че защитават срещу изнасяне на оборудване, информация, носители на информация и софтуер, свързани с ДУУ, без предварителна оторизация.

7.4.5 Управление на операциите

ДУУ осигурява сигурно и правилно функциониране на системите, при възможния минимален риск.

7.4.5.1 Защита от вируси

Интегритета на системите на ДУУ и информацията се защитава срещу вируси, зловреден и непроверен софтуер.

7.4.5.2 Реакция и докладване на инциденти

Пораженията следствие от инциденти и неправилно функциониране се минимизират, чрез въвеждането на процедури по докладване и реакция при инцидент.

7.4.5.3 Защита на носители на информация

Носителите на информация използвани от ДУУ, се съхраняват по сигурен начин и са защитени от повреда, кражба и не оторизиран достъп.

Процедурата по управление на носителите защитава срещу използване на носители, които ще отпаднат от употреба и ще влошат качествата си, за периода на съхранение на записите върху тях.

7.4.5.4 Установяване на процедурите

Процедурите са въведени и реализирани за всички доверени и административни длъжности, които имат отношение към предоставяне на удостоверителни услуги.

7.4.5.5 Работа с носители на информация

С всички носители на информация се борави по сигурен начин в съответствие с изискванията на схемата за класификация (виж точка 7.4.2). Носителите съдържащи чувствителни данни се унищожават по сигурен начин, ако повече не са необходими.

7.4.5.6 Планиране на капацитета

Наличните ресурса се наблюдават, за да се определи бъдещите допълнителни нужди от изчислителна мощност и обеми за съхраняване на данни.

7.4.5.7 Докладване на инциденти и реакция

ДУУ действа по незабавен и координиран начин, за да отговори бързо на инцидент и минимизира пораженията от нарушаване на сигурността. Всички инциденти се докладват в максимално кратък срок.

7.4.5.8 Процес по наблюдение

Процеса по наблюдение, като е посочено в 7.4.11, стартира със старта на системата и се прекратява при спиране на системата.

7.4.5.9 Преглед на записите

Журналните файлове на системата се преглеждат периодично, за да се идентифицират доказателства за неправилни действия.

7.4.5.10 Оперативни процедури и отговорности

Операциите по информационна сигурност на ДУУ са отделени от останалите операции. Това могат да бъдат:

- Операционни процедури и отговорности;
- Защита от зловреден софтуер;
- Управление на мрежата;
- Активно наблюдение на журналите, анализ на събитията и последващи действия;
- Съхранение на носителите;

Тези дейности могат да се реализират от доверения персонал на ДУУ или от други специалисти при съответното наблюдение и контрол.

7.4.6 Управление на достъпа до системите

Достъпа до информационните системи на ДУУ е ограничен само до подходящо упълномощени лица.

7.4.6.1 Защита на външния периметър

ДУУ реализира контроли, за да защити вътрешния мрежов домейн от външния мрежов домейн достъпен за трети страни.

7.4.6.2 Защита на чувствителните данни

Чувствителните данни се защитават от не оторизиран достъп и модификация. Чувствителните данни се защитават допълнително, когато се обменят през незащитени мрежи.

7.4.6.3 Администриране на потребителите

ДУУ управлява и администрира потребителския достъп до информационните системи включително управление на потребителските имена и пароли, наблюдение на използването им, модифицирането им през определен период от време и отнемане на достъпа.

7.4.6.4 Достъп до информация и информационни системи

ДУУ ограничава достъп до информационните и приложни системи в съответствие с политиката за контрол на достъпа. Използваната от ДУУ система осигурява достатъчни контроли, за да се разделят доверените роли на ДУУ, включително разделянето на функциите на администратора по сигурността от тези на оператора. Използването на други програми освен основните се ограничава и контролира. Контрола на достъп позволява достъп само до ресурси необходими за реализиране на функциите присъщи на съответната длъжност.

7.4.6.5 Идентификация и автентификация

ДУУ идентифицира и автентифицира персонала, преди да се предостави достъп до критични приложения свързани с управлението на удостоверенията.

7.4.6.6 Запис на действията

ДУУ пази за определен период от време, журналите с действията (виж точка **7.4.11**).

7.4.6.7 Защита от повторна употреба

Чувствителните данни са защитени от повторно не оторизирано използване чрез достъп до техни съхранени копия.

7.4.6.8 Вътрешен периметър

ДУУ държи локалните мрежови компоненти във физически защитена среда и техните конфигурации периодично се проверяват за съответствие с изискванията на ДУУ.

7.4.6.9 Наблюдение на защитените зони

Осъществява се постоянно наблюдение на помещенията, за да може ДУУ да открие, регистрира и реагира незабавно на неупълномощен и/или неправилен опит за достъп до ресурсите.

7.4.6.10 Контрол при публикуване

Контролира се достъпа до системата за публикуване на издадените УЕП, при опитите да се добави или изтрие УЕП или да се модифицира информация отнасяща се до УЕП.

7.4.6.11 Контрол при статуса на издадените УЕП

Контролира се достъпа до системата за предоставяне на информация за статуса на УЕП, при опитите да се модифицира информация отнасяща се до статуса на УЕП.

7.4.7 Инсталиране и поддръжка на сигурните системи

ДУУ използва сигурни и надеждни системи, които са защитени срещу промени.

7.4.7.1 Анализ на изискванията за информационна сигурност

При проектиране на информационната система на ДУУ се взема предвид анализа на изискванията за информационна сигурност.

7.4.7.2 Контрол на промените

Реализира се процедура за контрол на промените при модификация и спешни корекции на операционния софтуер.

7.4.8 Управление непрекъснатостта на бизнес процесите и инцидентите

ДУУ възстановява операциите си в максимално кратък срок в случай на природно бедствие, аварии или компрометиране на частния си ключ.

7.4.8.1 План за гарантиране непрекъснатостта

ДУУ разработва, внедрява, периодично тества, преглежда и ревизира план за гарантиране непрекъснатостта на бизнес процесите.

7.4.8.2 Архивни копия на системите

За да може да се възстановят операциите на ДУУ, системите периодично се архивират и архивните копия се съхраняват на безопасно място.

7.4.8.3 Персонал отговорен за архива

Операциите по периодично архивиране се реализират от лица заемащи съответните доверени роли посочени в точка 7.4.3.

7.4.8.4 Компрометиране на частните ключове на ДУУ

Плана за гарантиране непрекъснатостта на бизнес процесите, се отнася и за в случай на компрометиране на частния ключ на ДУУ.

7.4.8.5 Дейности при компрометиране на частния ключ на ДУУ

В случай на компрометиране на частния ключ ДУУ предприема като минимум следните действия:

- Информира за компрометирането всички титуляри/автори и други страни, които имат отношение към удостоверителната дейност на ДУУ;
- Показва, че УЕП и информацията за статуса на УЕП издадени като е ползван компрометирания ключ може повече да не е валидна;
- При необходимост се прекратяват издадените УЕП.

7.4.8.6 Действия при компрометиране на използваните алгоритми

В случай, че всички алгоритми и техните параметри, използвани от ДУУ и неговите титуляри/автори осигуряван неадекватна сигурност за периода, за който е предвидено да се използват ДУУ ще:

- Информира всички титуляри/автори и други страни, които имат отношение към удостоверителната дейност на ДУУ;
- Прекратява всички засегнати УЕП.

7.4.9 Прекратяване дейността на ДУУ

ДУУ предприема мерки в резултат, от които се минимизира потенциалните загуби на титуляри/автори и доверяващите се страни при прекратяване своята дейността разгледана в тази политика и предприема мерки за поддръжка на записите изисквани като доказателство за удостоверяването, за целите на съдебен спор.

При прекратяване на дейността „СЕП България" АД информира Комисията за регулиране на съобщенията, по установения в ЗЕДЕП и подзаконовите актове по неговото прилагане, ред.

7.4.9.1 Дейности преди прекратяване

Преди да прекрати своята дейност, ДУУ изпълнява следния минимален набор от процедури:

- ДУУ информира за предстоящото прекратяване на дейността си всички титуляри/автори и други страни, които имат отношение към удостоверителната дейност на ДУУ;
- ДУУ прекратява всички договори с подизпълнители предоставящи удостоверителни услуги от името и за сметка на ДУУ, също така се прекратява достъпа на подизпълнителите до информационните системи на ДУУ;
- Предприема необходимите мерки за прехвърляне на задълженията по поддръжка на информацията за регистрация (виж точка 7.3.1) и архивите на журналите, включително информацията за статуса на прекратените УЕП (виж точка 7.4.11) за съответния период от време както е обявено на абонатите и доверяващите се страни (виж точка 7.3.4);
- ДУУ унищожава или изтегля от употреба своите частни ключове, както е определено в точка 7.2.6.

7.4.9.2 Ангажимент за покриване на разходите по прекратяване

ДУУ се ангажира да покрие цената платима при реализирането на дейностите по прекратяване.

7.4.9.3 Изявление при прекратяване на дейността

ДУУ посочва в своята практика при предоставяне на удостоверителни услуги следните клаузи:

- За уведомяване на засегнатите страни;
- За прехвърляне на отговорността на друга страна;
- За предприемане на мерки относно статуса за проверка на УЕП, които са издадени и все още валидни.

7.4.10 Съответствие със законовите изисквания

ДУУ се ръководи в своята дейност от ЗЕДЕП и подзаконовите актове по неговото прилагане. А за неуредените в тях случаи действащото българско законодателство.

7.4.10.1 Спазвани законови изисквания

Закон да електронния документ и електронния подпис и наредбите по неговото прилагане.

Закон за защита на личните данни.

Закон за защита на потребителите.

7.4.10.2 ***Защита на личните данни***

ДУУ защитава личните данни в съответствие глава шест от ЗЕДЕП и закона за защита на личните данни. За целите на защитата на личните данни, ДУУ разработва политика за защита на личните данни, в която задължително се разглеждат и следните моменти:

- Регистрацията и ако е приложимо използването на псевдоним (виж точка 7.3.1);
- Конфиденциалността на записите (виж точка 7.4.11 и 7.3.3.6);
- Защита на достъпа до персоналната информация (виж точка 7.4.6);
- Съгласие на потребителите (виж точка 7.3.1.9);

7.4.10.3 ***Технически и организационни мерки***

ДУУ предприема подходящи технически и организационни мерки срещу не оторизираната и незаконна обработка на персонални данни и срещу случайна загуба, унищожаване или повреда на лични данни.

7.4.10.4 ***Разкриване на лични данни***

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

7.4.11 Поддържане на записи относно УЕП

ДУУ поддържа записи за свързаната с удостоверенията за универсален електронен подпис, информация за определен период от време за целите на предоставяне на доказателства за удостоверяването при съдебен процес.

7.4.11.1 ***Конфиденциалност и интегритет***

ДУУ взема мерки относно конфиденциалността и интегритета на текущите и архивирани записи отнасящи се до удостоверенията за универсален електронен подпис.

7.4.11.2 ***Архивиране на записи***

ДУУ архивира напълно всички данни отнасящи се до удостоверенията за универсален електронен подпис и пази конфиденциалността на архива както е посочено в практиката по предоставяне на удостоверителни услуги.

7.4.11.3 ***Предоставяне на достъп до записите***

Записите отнасящи се до удостоверенията за универсален електронен подпис се предоставя при оторизирано искане, за да се предоставят доказателства за удостоверяването, при съдебен процес. Автора и при ограниченията на изискванията за защита на личните данни (виж точка 7.4.10) титуляра имат достъп до регистрационната и друга информация относно субекта.

7.4.11.4 ***Точно време***

За всички важни събития на ДУУ свързани с прилежащата среда, управлението на ключовете и управлението на УЕП се записва и точното време на събитието.

7.4.11.5 ***Съхраняване на записите***

Записите отнасящи се до удостоверенията за универсален електронен подпис се пазят за подходящ период от време, за да се осигурят правно валидни доказателства в подкрепа на електронните подписи в съответствие с приложимото законодателство.

7.4.11.6 Защита на записа на събития

Събитията се записват по такъв начин, че не може лесно да се изтрият или унищожат през определения периода от време за тяхното съхранение.

7.4.11.7 Документиране на събития

ДУУ документира за кои данни и събития се води журнал.

7.4.11.8 Записвани събития

ДУУ записва всички събития свързани с регистрацията включително исканията за смяна на ключа или подновяване.

7.4.11.9 Записвана информация

ДУУ поддържа записи за цялата регистрационна информация, която включва:

- Типа на представените документи от заявителя при регистрацията;
- Запис на уникалните идентифициращи данни, номера или ако е приложимо комбинация от данни на идентифициращи документи;
- Място на съхранение на копия от исканията и идентификационните документи, включително подписан договор с абоната (виж точка 7.3.1.9);
- Всички допълнителни уговорки в договора с абоната, като съгласие за публикуване на удостоверението (виж точка 7.3.1.9);
- Идентичността на лицето приело искането;
- Използвания метод за проверка на идентификационните документи;
- Името на приелия УО и/или изпратил искането РО;

7.4.11.10 Защита на личните данни

ДУУ полага дължимата грижа за личните данни на автора.

7.4.11.11 Записи за жизнения цикъл на ключовете

ДУУ води журнал за всички събития свързани с генерацията на неговите ключове включително и генерацията на потребителски ключове от ДУУ.

7.4.11.12 Записи за жизнения цикъл на УЕП

ДУУ води журнал за всички събития свързани с жизнения цикъл на удостоверенията, включително генерацията на ключова двойка за автора.

7.4.11.13 Записи при подготовка на SSCD

Ако е приложимо ДУУ води записи за събитията свързани с подготовката на SSCD.

7.4.11.14 Записи при заявки за прекратяване

ДУУ води записи за всички искания свързани с прекратяването на удостоверения както и предприетите в резултат на това мерки.

7.5 Организационни мерки

7.5.1 Не дискриминационни политики и практики

ДУУ следва политики и процедури, които нямат дискриминационен характер.

7.5.2 Достъпност на услугите

ДУУ предоставя удостоверителни услуги на всички желаещи, чиито дейности са в обявения обсег на операции.

7.5.3 Водещо законодателство

ДУУ се ръководи в своята дейност от ЗЕДЕП и подзаконовите актове по неговото прилагане.

7.5.4 Покриване на отговорността

ДУУ урежда по подходящ начин ангажиментите произтичащи от неговите операции и/или дейности.

7.5.5 Финансова стабилност и ресурси

ДУУ е финансово стабилен и разполага с всички ресурси, за да оперира в съответствие с тази политика.

7.5.6 Жалби, спорове и оплаквания

ДУУ прилага политика и процедури за разрешаване на оплаквания, жалби и спорове постъпващи от клиенти и други страни относно предоставянето на електронни сигурни услуги и други свързани въпроси.

7.5.7 Документиран ангажимент

ДУУ детайлно описва задълженията при сключване на договори, включително случаите, когато при предоставяне на услугите си въвличат подизпълнители и/или други трети страни.

7.5.8 Организационна независимост

Частта от ДУУ ангажирана с генерацията на УЕП и управление на информацията за статуса на издадените УЕП е организационно независима при вземане на решения свързани с установяването, предоставянето и поддръжката и преустановяването на услуги. Старшия изпълнителен персонал, старшия персонал и персонала на доверени позиции е свободен от всякакъв комерсиален, финансов и друг натиск, който може да доведе до злополучно въздействие върху услугите, които осигуряват.

7.5.9 Организационна структура и длъжностни характеристики

ДУУ има ясна документирана организационна структура с разписани задължения и отговорности на всички нива и разработва длъжностни характеристики за всички доверени длъжности като отчита задълженията и отговорностите произтичащи от тази политика по предоставяне на удостоверителни услуги.