БОРИКА
БАНКОВИ УСЛУГИ

ПОЛИТИКА И ПРАКТИКА

ЗА ПРЕДОСТАВЯНАТА ОТ „БОРИКА“ АД УСЛУГА ЗА ДЪЛГОСРОЧНО КВАЛИФИЦИРАНО СЪХРАНЯВАНЕ НА КВАЛИФИЦИРАНИ ЕЛЕКТРОННИ ПОДПИСИ и ПЕЧАТИ (B-Trust Qualified Long-Terms Preservation Service of QES/QESeal (B-Trust Qualified LTPS)

Версия 3.0

В сила от:

1 Март 2020 г.

Хронология на измененията на документа				
Версия	**Автор (и)**	**Дата**	**Състояние**	**Коментар**
1.0	Димитър Николов	13.01.2019	Утвърден	Създаване на документа.
2.0	Димитър Николов	01.04.2019	Утвърден	Създаване на документа.
3.0	Димитър Николов	01.03.2020	Утвърден	Технически корекции

СЪДЪРЖАНИЕ

1 ОБХВАТ И УПОТРЕБА 4
2 СЪОТВЕТСТВИЕ И РЕФЕРЕНЦИИ 5
3 ОПРЕДЕЛЕНИЯ И СЪКРАЩЕНИЯ 7
3.1 Определения 7
3.2 Съкращения 8
4 ВЪВЕДЕНИЕ 8
5 КОНЦЕПЦИЯ 9
5.1 Общи изисквания 9
5.2 Цели на дългосрочно съхраняване 9
5.3 Е-документ и контейнер на съхраняване 9
5.4 Формати и профили на подписи/печати 10
В Приложение 1 на документа са представени форматите на контейнери на подписи/печати с посочените профили и нива на подписване. 11
5.5 Модел, механизъм и схеми на съхранение 11
5.6 Валидиране 13
5.7 Архив/Хранилище 13
5.8 Политика и практика 14
5.9 Управление на Политиката и Практиката 15
5.10 Други приложими документи 15
6 УСЛУГА (ПРОЦЕС НА ДЪЛГОСРОЧНО СЪХРАНВАНЕ) 15
6.1 Участващи страни 15
6.2 Модел на дългосрочно съхраняване 16
6.3 Цели на дългосрочно съхраняване 16
6.4 Доказателства относно целите на дългосрочно съхраняване 16
6.5 Функционален модел 17
6.6 Базови процеси и процедури 18
6.6.1 Приемане/Зареждане (Upload) на е-документ 18
6.6.2 Доставяне (Download) на съхраняван е-документ 19
6.6.3 Издаване на Потвърждение (ACK) за съхраняван е-документ 19
6.6.4 Визуализиране (Display) на съхраняван е-документ 19
6.6.5 Изтриване (Delete) на съхраняван е-документ 20
6.7 Прекратяване на Договора за УСЛУГАТА 20
6.8 Интерфейси и протоколи 20
6.8.1 OASIS DSS интерфейс 20
6.8.2 GUI интерфейс 20
6.9 Външни източници на доказателствен материал за съхраняване 20

7 ТЕХНИЧЕСКИ МЕРКИ ЗА СИГУРНОСТ 21
7.1 Гаранции за сигурност 21
7.2 Предпазни мерки за компютърна сигурност 21
7.3 Технически предпазни мерки, свързани с жизнения цикъл 21
7.4 Регулярен Одит/Сертифициране 21
7.5 Повторно криптиране (Прекриптиране) на Архива 21
7.6 (Непрекъснат) мониторинг на технологиите 21
7.7 Избор на външни доставчици 21
7.8 Поддръжка на оперативна съвместимост на подпис/печати 21
8 ОЦЕНКА НА РИСКА 22
9 ПРАКТИКА 22
9.1 Служебни удостоверения на УСЛУГАТА 22
9.2 Средства, управление и оперативен контрол на УСЛУГАТА 24
9.2.1 Вътрешна организация при Доставчика 25
9.2.2 Персонал 25
9.2.3 Управление на активи 25
9.2.4 Управление на достъпа 25
9.2.5 Криптографска сигурност – управление на ключове 25
9.2.5.1 Генериране на двойката ключове 25
9.2.5.2 Защита на частен ключ 25
9.2.5.3 Разпространение на публичния ключ 25
9.2.5.4 Продължаване на срока и/или преиздаване на удостоверението 26
9.2.6 Физическа и околна среда 26
9.2.7 Операционна сигурност 26
9.2.8 Мрежова сигурност 26
9.2.9 Управление на журнали 26
9.2.10 Непрекъсваемост 26
9.2.11 Прекратяване на услугата 26
9.3 Информационна сигурност 26
10 ДРУГИ БИЗНЕС УСЛОВИЯ И ПРАВНИ АСПЕКТИ 27
Приложение 1. Профили на е-подпис/печат и нива на подписване (е-документ), допустими за УСЛУГАТА 27

1 ОБХВАТ И УПОТРЕБА

Този документ:

- е разработен от „БОРИКА“ АД, юридическото лице, регистрирано в Търговския регистър към Агенцията по вписванията с ЕИК 201230426;
- влиза в сила на 01.04.2019 г.;

- съдържа политиката и изискванията за сигурност на оперираната от Доставчик на квалифицирани удостоверителни услуги (ДКУУ) „БОРИКА“ АД (Доставчик) услуга за квалифицирано дългосрочно съхраняване на квалифицирани електронни подписи и печати за дълго време (означавана в документа с УСЛУГА) в съответствие с Регламент 910/2014 на ЕП и Съвета;
- има характер на общи условия по смисъла на чл. 16 от Закона за задълженията и договорите (ЗЗД);
- включва описание на политиката и практиката при предоставяне на УСЛУГАТА от Доставчика и е публичен документ с цел установяване на съответствие на дейността на Доставчика с нормативната уредба;
- определя практиката при опериране и управление на УСЛУГАТА, за да позволи на потребители и доверяващи се страни, които имат сключен Договор за използване на квалифицираните удостоверителни услуги на B-Trust и/или подписано Споразумение за ниво на обслужване към такъв договор, да получат описание и оценка на сигурността на тази квалифицирана услуга
- служи за оценка на оценка на дейността на ДКУУ „БОРИКА“ АД да предоставя квалифицирано съхранение на квалифицирани е-подписи/печати в съответствие с Регламент 910/2014;
- определя основните формати на подписи/печати, към които е приложима УСЛУГАТА;
- определя механизмите и схемата на съхранение на квалифицирани подписи и печати УСЛУГАТА;
- определя релациите/връзките с „външни“ доверени/квалифицирани услуги (например CRL, OCSP, TSA), предоставящи информация на УСЛУГАТА;
- адресира само техническите аспекти на дългосрочно съхраняване на валидността на е-подписи/печати, но не и тяхната приложимост (т.е., правната приложимост) за различни бизнес-цели;
- може да бъде променян от ДКУУ и всяка нова редакция на тази Политика и Практика се публикува на интернет-страницата на Доставчика като отменя предишната версия на този документ.

Извън обхвата на документа са:

- Правната приложимост (правила за приложимост) на дългосрочно съхраняваните квалифицирани е-подписи/печати за различни бизнес-цели;
- Техническите аспекти на формати, синтаксисът, кодировката на е-подписа/печата, конкретните формати, профили и кодировка на документите за подпис/печат;
- Процесите на подписване/подпечатване, т.е. генерирането на квалифицираните е-подписи/печати, които са обект на тази УСЛУГА.

2 СЪОТВЕТСТВИЕ И РЕФЕРЕНЦИИ

Настоящият документ е изготвен в съответствие с:

- Регламент 910/2014 на Европейския парламент и Съвет относно удостоверителните услуги и се позовава на информация, относно подготвяните в съответствие с този Регламент международни препоръки, спецификации и стандарти;
- Закон за електронния документ и електронните удостоверителни услуги (ЗЕДЕУУ);
- Наредба за отговорността и за прекратяването на дейността на доставчиците на удостоверителни услуги (НОПДДУУ);
- Следва да се използва съвместно с основните документи B-Trust CPS-eIDAS (Практика на Доставчика) и B-Trust CP-eIDAS (Политика на Доставчика) при одит на УСЛУГАТА с цел установяване на съответствие на дейността на Доставчика с нормативната уредба;

Съдържанието и структурата на документа се базира на следните утвърдени международни спецификации:

- ETSI TS 119 511 v.1.1.1: “Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques”;
- ETSI TS 101 533-1: "Electronic Signatures and Infrastructures (ESI) Data Preservation Systems Security; Part 1: Requirements for Implementation and Management";
- ETSI TR 101 533-2: "Electronic Signatures and Infrastructures (ESI) Data Preservation Systems Security; Part 2: Guidelines for Assessors";
- ETSI SR 019 510 V1.1.1 (2017-05) Electronic Signatures and Infrastructures (ESI) Scoping study and framework for standardization of long-term data preservation services, including preservation of/with digital signatures.

Следните документи (технически спецификации) нямат пряко отношение към настоящия документ, но могат да бъдат в помощ тези, които го използват:

- ETSI EN 319 102-1: Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures, Part1: Creation and Validation;
- ETSI TS 119 102-2: Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures, Part 2: Signature Validation Report;
- ETSI TS 119 101: Electronic Signatures and Infrastructures (ESI); Policy and Security requirements for applications for signature creation and signature validation;
- ETSI TS 119 442: "Electronic Signatures and Infrastructures (ESI); Protocol for TSPs providing signature validation services";
- ETSI EN 319 122-1: "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures";
- ETSI EN 319 122-2: "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 2: Extended CAdES signatures";
- ETSI EN 319 132-1: "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures;
- ETSI EN 319 132-2: "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 2: Extended XAdES signatures;
- ETSI EN 319 142-1: "Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures;
- ETSI EN 319 142-2: "Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 2: Additional PAdES signatures profiles;
- ETSI EN 319 421: Policy and Security Requirements for Trust Service Providers issuing Electronic Time-Stamps;
- ETSI EN 319 422: "Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles;
- ETSI EN 319 162-1 Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 1: Building blocks and ASiC baseline containers;
- ETSI EN 319 162-2 Electronic Signatures and Infrastructures (ESI);
- Associated Signature Containers (ASiC); Part 2: Additional ASiC containers;
- RFC 6970 X.509 Internet Public Key Infrastructure: Online Certificate Status Protocol – OCSP.

Всякаква информация, свързана с този документ, може да се получи от Доставчика на адрес:

бул. „Цар Борис III" № 41

София 1612

„БОРИКА“ АД

телефон: 0700 199 10

имейл адрес: info@b-trust.org

Официална страница на доставчика: www.b-trust.bg

3 ОПРЕДЕЛЕНИЯ И СЪКРАЩЕНИЯ

3.1 Определения

УСЛУГА (Preservation Service) – квалифицирана услуга за дългосрочно съхраняване на квалифицирани подписи/печати в съответствие с Регламент 910/2014 ЕС

Съхраняване (Preservation) – функция, която поддържа даннов обект, в правилна и независимо разбираема форма, евентуално в дългосрочен план

Дългосрочен план (Long time) – достатъчно дълго време за съхраняване, отнесено към времето на евентуални технически промени (в крипто алгоритми, размер на ключове, хеш функции) или на технологията за съхраняване

Цел на съхранение (Preservation goal) – една от следните цели, поддържани през време на срока за съхранение: доказателство за интегритет, доказателство за съществуване, за наличност, за на валидност на подпис/печат или утвърдено време, за конфиденциалност, за автентичност на Потребител/заявител, за идентификация на DPS

Е- документ (E-document) – електронен документ, който съдържа поне един електронен подпис или печат, съответстващ на eIDAS; в зависимост от типа, електронният документ може да съдържа допълнителни електронни документи и съответни метаданни, подписи, контра-подписи и времеви печати

Контейнер (Container) за съхраняване – даннова структура (даннов обект), която съдържа е-подпис(и)/печат(и), т.е. подписан е-документ и други метаданни, специфични за дългосрочно съхраняване на обекта

Идентификатор на контейнер - уникална данна, идентифицираща контейнера за съхранение; генерира се от УСЛУГАТА, както и се изпраща на УСЛУГАТА

Архив – база данни за съхранение на данновите обекти в контейнери за съхранение с определена(и) цел(и) и свързаните с нея компоненти (компютърни системи, комуникационни връзки, електрозахранване, физическа и противопожарна защита и системи за сигурност и тяхната резервация)

Абонат (Client) – Лице или организация, подписали договор с Доставчика, за да се използва УСЛУГАТА

Подател (Submitter) – Лице, което изпраща е-документи на УСЛУГАТА; може да бъде различно от Абоната, но с предоставени му права (на достъп) да ползва УСЛУГАТА

Доказателствен запис (Evidence record) – даннов елемент, който служи за доказателство за съществуване на даннов обект или група даннови елементи в даден момент

Доказателство за съхряняване (Preservation evidence) – данни, които служат да покажат, че цел(и) за съхраняване на подпис(и)/печат(и) (например, интегритет, съществуване или валидност) са спазени

Механизъм на съхраняване (Preservation mechanism) – механизъм, използван за съхраняване на е-документ(и)

Схема на съхраняване (Preservation scheme) – механизъм(и) за съхраняване, които се използват за постигане на конкретна/и цел(и) на съхраняване на подписи/печати

Политика на съхраняване (Long-time Preservation Policy/LTPP) – набор от правила, приложими към УСЛУГАТА, определящи механизми (схема на съхраняване) и вътрешните процеси, чрез които се постигат целите на съхраняване на подписи/печати

Време на съхраняване (Preservation time frame) – време, определено в договора за ползване на УСЛУГАТА

Доказателство за съществуване (Proof of existence) – съществуване на даден е-документ (подпис/печат) в (преди) определен момент (например, квалифициран времеви печат)

Доказателство за интегритет (Proof of integrity) – поддържане на ненарушимост цялостност(например, хеш, подпис/печат)

Доказателство за валидност (Proof of validation) – поддържане на валидност на подпис/печат.

3.2 Съкращения

QES/QESeal (КЕП/КЕПечат) – Квалифициран Електронен Подпис/Печат

QC (КУ) – Квалифицирано удостоверение

КУКЕП - Квалифицирано удостоверение за КЕП

КУКЕПечат –Квалифицирано удостоверение за КЕПечат

AdES/AdESeal (УЕП/УЕПечат) – Усъвършенстван Електронен Подпис/Печат

AdES_QC (УЕП_КУ) - Усъвършенстван Електронен Подпис с Квалифицирано удостоверение

AdESeal (УЕПечат) – Усъвършенстван Електронен Печат с Квалифицирано удостоверение

OCSP (status) – Онлайн статус на удостоверение

PKI – Инфраструктура на публични ключове

LTPP – Политика на съхраняване (за дълго време)

УСЛУГА – B-Trust Qualified LTPS

СА/УО – Удостоверяващ Орган

TSA/УОВ – Удостоверяващ Орган на Време

4 ВЪВЕДЕНИЕ

Силата и пригодността на криптографските механизми е функция на времето. Необходимо е да се прилагат подходящи механизми за съхранение, които са в състояние да поддържат валидността на подписания обект за дълги периоди от време чрез прилагането на различни технологии и схеми за съхранение и криптографски алгоритми.

Тази необходимост се признава и визира в Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета, както може да се види в т. (61) на преамбюла:

(61) Настоящият регламент следва да осигури дългосрочното съхраняване на информация, за да се осигури правната валидност на електронните подписи и електронните печати за продължителен период от време и да се гарантира, че те могат да бъдат валидирани независимо от бъдещи промени в технологиите.

Освен това чл. 34, ал.1 от Регламента гласи, че:

Услугата по квалифицирано съхраняване на квалифицирани електронни подписи може да се предоставя единствено от доставчик на квалифицирани удостоверителни услуги, който използва процедури и технологии, позволяващи надеждността на квалифицирания електронен подпис да се разшири извън срока на технологична валидност.

Настоящият документ представя Политиката и Практиката за УСЛУГАТА на ДКУУ „БОРИКА“ АД, както и схемата (механиъм и цели) за съхраняване, която се използва за съхраняване на валидността на КЕП и КЕПечати и на даннови обекти, асоциирани с подписи/печати.

5 КОНЦЕПЦИЯ

5.1 Общи изисквания

Тази Политика и Практика на Доставчика за УСЛУГАТА адресира:

- дългосрочното съхраняване на е-документи (даннови обекти);
- статусът (доказателство) на валидност на дългосрочно съхранявани подписи/печати.

Съхраняването (на интегритета) на цифрови обекти, които не са подписани/подпечатени, е извън обхвата на настоящия документ. Извън този обхват е и правната валидност на дългосрочно съхраняваните подписи/печати.

5.2 Цели на дългосрочно съхраняване

Представената в настоящия документ схема за дългосрочно съхраняване адресира следните цели:

- интегритет на е-документ;
- съществуване (преди/в даден момент) на подписан/подпечатен е-документ;
- валиден статус на подписи/печати в дългосрочен план.

Интегритетът на данните се проверя по време на срока за съхранение чрез доказателство за интегритет (хеша, подпис/печат).

Съществуването на данновия обект (е-документа) в определен момент се поддържа се чрез комбиниране на доказателство за интегритет (ненарушимост) и квалифициран времеви печат.

Валиден статус на подписи/печати в дългосрочен план се поддържа чрез доказателство за валидност на подписа/печата.

Съгласно настоящия документ, УСЛУГАТА е приложима за два основни типа даннови обекти:

- подписан/подпечатен е-документ (опаковащ и опакован подпис/печат), за който трябва да се съхранява дълготрайно валиден статус;
- обособен подпис/печат и асоциираданнов обект (документ/файл).

За да се съхрани валидността на електронния подпис/печат трябва да бъдат запазени всички данни за тяхната валидация, валидността на които изтича (не може да бъде гарантирана) в бъдеще (удостоверения, информация за отмяна/прекратяване - CRL, OCSP отговори, доверителни списъци и т.н.).

Допълнителни цели за дългосрочното съхраняване са идентифициране на Доставчика на УСЛУГАТА, неотменимост на подаване на данновите обекти към УСЛУГАТА и поверителност на данните в обмена.

УСЛУГАТА създава доказателства за съхраняване, с които потвърждава, че изпълнява съответните цели на съхранение за посочените даннови обекти (е-документи).

5.3 Е-документ и контейнер на съхраняване

Е-документът (подписан/подпечатен даннов обект) е данни, които се обработват от УСЛУГАТА с цел дългосрочно съхраняване на подписите/печатите. Може да бъде основен даннов обект (опакован/опаковащ подпис/печат), който трябва да бъде съхранен или метаданни, които предоставя Заявител/Подател или самата УСЛУГА събира и добавя. Понастоящем, тази версия на УСЛУГАТА използва контейнер, съдържащ само един е-документ и добавяните метаданни за дългосрочно съхраняване.

Услугата (може да) добавя метаданни като например, удостоверения на УО (CA), CRL/OCSP- отговори, подписи/печати, времеви печати, доказателства, отчети на валидиране.

Не всички е-документи следва да бъдат подадени за съхраняване едновременно.

Подателят е субектът, който изпраща е-документ (и) до УСЛУГАТА. Той може да е различен от Абоната-собственик на изпратените за съхраняване е-документи. УСЛУГАТА създава идентификатор на контейнер, който връща на Подателя (когато УСЛУГАТА поддържа архив). Идентификаторът на контейнера за съхраняване е уникален.. Генерира се на базата на хеш-функция, тоест представлява хеш-код, с указан идентификатор на хеш-алгоритъма.

5.4 Формати и профили на подписи/печати

РЕШЕНИЕ ЗА ИЗПЪЛНЕНИЕ (ЕС) 2015/1506 на Комисията определя техническите спецификации и стандарти на формати и профили на квалифицирани и на усъвършенствани е-подписи/печати, които всяка страна-членка на Съюза следва да поддържа (подписва и валидира) и които се приемат от органите на публичния сектор на страните-членки с оглед на тяхната трансгранична оперативна съвместимост и изискуемото ниво на сигурност (профил) за конкретни бизнес-цели:

- XAdES Базов профил - ETSI TS 103 171 v.2.1.1 (2012) (или draft ETSI EN 319 132-1, 2015);
- CAdES Базов профил - ETSI TS 103 173 v.2.1.1 (20012) (или draft ETSI EN 319 122-1, 2015);
- PAdES Базов профил - ETSI TS 103 172 v. 2.1.1 (2012) (или draft ETSI EN 319 142-1, 2015).

РЕШЕНИЕТО (чл. 1 и 3), в съответствие с Регламент 910/2014, утвърждават следните усъвършенствани подписи/печати във формати CMS, XML и PDF на нива на съответствие (профили) B, T и LT, които следва да се признават между страните-членки.

РЕШЕНИЕТО (чл. 2 и 4) утвърждава условията, при които се потвърждава валидността на даден усъвършенстван електронен подпис/печат, а именно:

(1) удостоверението в подкрепа на усъвършенстваният електронен подпис/печат е било валидно към момента на подписването/подпечатването, а когато усъвършенстваният електронен печат е подкрепен от квалифицирано удостоверение, това квалифицирано удостоверение е отговаряло към момента на подписването/подпечатването на изискванията съгласно приложение III към Регламент (ЕС) № 910/2014 и е било издадено от доставчик на квалифицирани удостоверителни услуги;

(2) данните от валидирането на подписа/печата съответстват на данните, предоставени на доверяващата се страна;

(3) уникалният набор от данни, представляващ Титуляря/създателя на печата, е надлежно предаден на доверяващата се страна;

(4) ако към момента на подписването/подпечатването е бил използван псевдоним, то това е ясно указано на доверяващата се страна;

(5) когато усъвършенстваният електронен подпис/печат е създаден от устройство за създаване на квалифициран електронен подпис/печат, използването на такова устройство е ясно указано на доверяващата се страна;

(6) цялостността на подписаните/подпечатаните данни не е застрашена;

(7) изискванията по член 36 от Регламент (ЕС) № 910/2014 са били изпълнени към момента на подписването/подпечатването;

(8) системата, използвана за валидиране на усъвършенстваният електронен подпис/печат, предоставя на доверяващата се страна правилния резултат от процеса на валидиране и ѝ позволява да открие евентуални проблеми, свързани със сигурността.

ДКУУ „БОРИКА“ АД оперира и предоставя квалифицирана удостоверителна услуга за валидиране на квалифициран/усъвършенстван подпис/печат с квалифицирано удостоверение, която съответства на Регламент 910/2014 ЕС и отговаря на изискванията (чл. 1 – 4) на горепосоченото Решение. Виж документ B-Trust QSVS-eIDAS.

В допълнение, B-Trust QSVS-eIDAS валидира посочени формати на подписи/печати и с профил _LTA, както и подписи/печати с профил ASiC-S/E. Поддържането на тези AdES-формати на подписи/печати с профил _LTA, определя избора на формата на контейнера за дългосрочно съхранение на подписани/подпечатени на настоящата УСЛУГА.

В Приложение 1 на документа са представени форматите на контейнери на подписи/печати с посочените профили и нива на подписване.

5.5 Модел, механизъм и схеми на съхранение

5.5.1 Модел

Настоящата версия на УСЛУГАТА е изпълнена и се предоставя с асоциирано собствено Хранилище/Архив, т.е. следва Модел WST (preservation service with storage) съгласно спецификацията ETSI TS 119 511 v.1.1.1.

5.5.2 Механизми

Съгласно същата спецификация, основните механизми за съхраняване, които могат да се приложат за дългосрочно съхраняване са:

- Времеви печат (Time stamp);
- Усъвършенстван подпис/печат с разширен формат/профил (AdES);
- Доказателствен запис (Evidence Record/ER);
- Отчет на валидиране (от услуга за квалифицирано валидиране на подпис/печат/QSVS)

Усъвършенстваният подпис/печат с разширен формат/профил (AdES) осигурява вътрешен механизъм, чрез който остава проверим в след дългосрочен план. Виж документ „Политика и Практика на ДКУУ „БОРИКА“ АД за услугата за квалифицирано валидиране на подписи/печати (B-Trust QSVS – CP and CPS).

Всички AdES формати с профил-разширение на базовия (BASELINE/B) – т.е., B_T, B_LT и B_LTA се явяват разширение на предшестващото ниво с допълнителен доказателствен материал за дългосрочно съхраняване на подписа/печата:

- Ниво _T – към базовия формат на подписа/печата се добавя времеви печат; подписът/печатът е създаден преди удостоверяването време с времевия печат – важно доказателство в случай, че удостоверението на подписа/печата стане невалидно в бъдеще (след срока на валидност или прекратяване на удостоверението);
- Ниво _LT - този формат разширява предишния с допълнителен доказателствен материал за валидността на удостоверението на подписа/печата (OCSP-статус, CRL-код); подпис/печат с това ниво позволява валидиране, при условие, че няма технологични промени (например, използвани алгоритми да станат слаби);
- Ниво _LTA - специфичен хеш алгоритъм преизчислява хешът на първоначално подписания/подпечатен документ с подписаните атрибути и заедно с преди добавен материал за валидиране и времеви печат се защитават с нов времеви печат; подпис/печат с това ниво позволява да се валидира оригиналния подпис при условие, че последния добавен времеви печат да бъде валидиран и последният използван хеш-алгоритъм да е още надежден.

Формат AdES на подпис/печат с профил _LTA е най-подходящ за контейнер за дългосрочно съхраняване. Механизмите на този профил са сходни за различните формати посочени в РЕШЕНИЕТО. Базира се на стандартизирани формати и има висока степен на оперативна съвместимост - този контейнера за дългосрочно съхраняване може лесно да бъде изнасян от УСЛУГАТА в друга такава услуга (на друг ДКУУ). Целият липсващ материал за валидиране се добавя, изчислява се хеш върху съществуващия подпис, включително

първоначално подписания/подпечатен документ и времевия печат се генерира/изчислява върху последния изчислен хеш.

Настоящата версия на УСЛУГАТА използва като контейнер за съхранение на подписан/подпечатен даннов обект (е-документ) с формат AdES с профил LTA на подпис/печат.

5.5.3 Схема

Схемата за дългосрочно съхранение се определя от механизма за (дългосрочно) съхраняване и предоставяните доказателство за това, които се прилагат за да се постигне определена цел или набор цели за съхраняване на е-документи (виж т. 5.2).

Съгласно спецификация ETSI TS 119 511, допустими са различни схеми, базирани на AdES механизма за съхранение.

5.5.3.1 Чрез ER

Ако няма ER (Evidence Record) за е-документа, AdES подписът се валидира, събира се и се добавя липсващия доказателствен материал за валидност в контейнера; УСЛУГАТА създава ER, който защитава всички елементи на контейнера и го съхранява в Архива.

Ако за е-документа има ER, УСЛУГАТА само усилва ER (посредством подновяване на времевия печат (Time-stamp Renewal).

5.5.3.2 Чрез усилване, (разширяване) на AdES

Е-документ с AdES формат и профил_LTA на подписа/печата се подава на УСЛУГАТА. При обособен (detached) подпис е необходим и първоначалния документ или поне неговия хеш за съответния хеш-алгоритъм. При базов подпис/печат (ниво B), УСЛУГАТА добавя времеви печат към подписа/печата. След това УСЛУГАТА валидира е-документа (чрез вътрешен или външен процес) като попълва липсващия доказателствен материал за валидност (ниво _LT).

Забележка: В случай на усилен вече подпис/печат (ниво _LTA), УСЛУГАТА валидира и усилва само последния времеви печат.

Вътрешен процес-мониторинг следи за следващо усилване на подписа/печата (е-документа) – например, изтичане периода на валидност на удостоверението на последния времеви печат и/или при вече обявен за слаб криптографски/хеш алгоритъм.

5.5.3.3 Чрез времеви печати с дълъг период на валидност

Тази схема е специален случай на предишната.

Периодът на валидност на времевия печат, вместо да бъде ограничен от периода на валидност на базовото удостоверение на TSA (УО за времеви печати), се удължава достатъчно много криптографските алгоритми да останат сигурни с цел рядко усилване на подписите/печатите на е-документите.

5.5.3.4 Чрез отчет на валидност

Когато УСЛУГАТА получи за съхранение подписан/подпечатан е-документ във формат AdES, при валидиране на подпис/печата тя ще заяви отчет на валидност от услугата за валидиране на подписи/печати. Вместо да подсилва оригиналния подпис/печат на е-документ, УСЛУГАТА ще подсилва само подписа/печата на отчета за валидност, за да го поддържа проверяем дългосрочно. Допълнително, с цел гарантиране на интегритета на първоначалния е-документ (дори при вече слаб начален хеш-алгоритъм), негова хеш-стойност с последно използван хеш-алгоритъм ще се добавя към подписа/печата на отчета на валидиране преди неговото усилване. Схемата съхранява е-документа заедно с усилвания отчет за валидиране. Оригинално подадения подпис/печат (е-документ) не се променя.

Настоящата версия на предоставяната от ДКУУ „БОРИКА“ АД УСЛУГА имплементира дългосрочно съхраняване на е-подпис/печат съгласно схемата от т. 5.5.3.2.

5.6 Валидиране

Валидирането в обхвата на УСЛУГАТА е процес, който проверява валидността на подписи/печати на е-документи и на времеви печати. Процесът на квалифицирано валидиране на подпис/печати е извън обхвата на този документ.

УСЛУГАТА трябва да използва вътрешен процес за валидиране или външна квалифицирана услуга за валидиране за да провери статуса на валидност на подпис/печат, преди да съхрани е-документ (и) в контейнера за съхраняване.

ДКУУ „БОРИКА“ АД предоставя и поддържа квалифицирана услуга за валидиране на КЕП/КЕПечат, която е в съответствие с Регламент 910/2014 ЕС. Виж документ „B-Trust Политика и Практика на услугата за квалифицирано валидиране на електронни подписи и печати“ (B-Trust QSVS-eIDAS).

За да провери валидността на времеви печати към е-документи (подписи и печати), подлежащи на съхранение, УСЛУГАТА трябва да използва вътрешен и/или външен процес (квалифицирана услуга за времеви печати). Проверката за валидност на времеви печати е директна и не изисква задължително използване на квалифицираната услуга за времеви печати. Квалифицираната услуга за времеви печати B-Trust QTSA-eIDAS на Доставчика също може да се използва за проверката на валидност на времевите печати.

5.7 Архив/Хранилище

Архивът е специализирана база данни за съхраняване и управление/поддръжка на контейнерите за дългосрочно съхраняване на цифровите обекти (е-документи, доказателства).

УСЛУГАТА поддържа интегриран Архив/хранилище и изпълнява следните операции/процедури:

- Upload (DEPOSIT) - проверява електронните подписи/печати в е-документа или файла чрез услугата B-Trust QSVS (квалифицирано валидиране), доставя дългосрочния материал (отчета/доказателство) за валидност подпечатен с квалифициран времеви печат на тази услуга, създава контейнера и го запазва с приетия е-документ в Архива; връща на Подателя уникален идентификатор на съхранения контейнер;
- Download (RETRIEVE) – Потребителят/Абонат може да изтегля свои е-документи съхранявани в контейнери в Архива и съответния дългосрочен материал за валидност (доказателство за валидност);
- ACK (RETRIEVE PROOF) - По искане на Потребителя/Абоната Доставчикът издава потвърждение (доказателство за съхраняване) във връзка с архивиран е-документ; УСЛУГАТА връща исканите доказателства за съхранение. Тази процедура може да се изпълни съвместно в рамките на процедурата RETRIEVE/DOWNLOAD
- DISPLAY – В определени дата и място Потребителят/Абонат има възможност да разглежда своите е-документи, съхранявани в Архива;
- UPDATE STORED ELEMENTS (опция) – Потребител/Абонат изпраща идентификатора на контейнера и "Delta е-документ" за да се актуализира е-документ в контейнер на Архива, създавайки нова версия на контейнера; УСЛУГАТА връща новата версия на актуализирания контейнер и (опция), актуализираните доказателства за съхранение. Оригиналната версия на контейнера се запазва;
- DELETE - По искане на Абоната/Потребителя, УСЛУГАТА предоставя селективно изтриване на е-документ(и) за съхраняване (и всички съответни доказателства за дългосрочно валидиране), съхранявани в Архива. Заличаването означава физическото изтриване на PDO (документ) по такъв начин, че да не може да бъде възстановен по-късно (или само с нереалистично високи финансови разходи) от Архива;
- AUGMENTATION – Тази процедура/операция не е част от интерфейса на Потребителя и се задейства автоматично (вътрешно), за да осигури дългосрочното съхраняване на валидността на подпис (и)/печат (и) на е-документи, т.е. да удължи периодът, през който се поддържа доказателството на тази цел (валидност на подпис (и)/печат(и);

- MONITORING – Тази процедура не е част от интерфейса на Потребителя и се активира автоматично (вътрешно), в съответствие с Политиката на УСЛУГАТА. Операцията следи различни събития, които биха застрашили възможността за потвърждаване на доказателствата за съхранение. Може да активира (вътрешно) процедурата AUGMENTATION.

ДКУУ „БОРИКА“ АД предоставя на Абонатите УСЛУГАТА с интегриран към нея Архив за съхранение на е-документи и доказателствата за съхраняване.

5.8 Политика и практика

Този документ дефинира общите елементи на Политиката и на Практиката на Доставчика на УСЛУГАТА и има характер на общи условия по смисъла на чл. 16 от Закона за задълженията и договорите (ЗЗД). Тези условия са част от писмен Договор за удостоверителни услуги, който се сключва между Доставчика и Потребителите.

Политиката определя условията и правилата, към които се придържа Доставчика за да имплементира Практиката при предоставяне на УСЛУГАТА.

Практиката описва как Доставчикът прилага описаната Политика и процедурите, които той следва за да предоставя УСЛУГАТА.

Доставчикът, чрез тази УСЛУГА дългосрочно съхранява квалифициран е-подпис/печат и/или усъвършенстван подпис/печат придружен от квалифицирано удостоверение на всяка заинтересована страна, като съблюдава обща Политика на дългосрочно съхраняване.

Правило в Практиката на Доставчика на УСЛУГАТА е да съхранява дългосрочно валидира подписи/печати с формати/профили съгласно Политиката му като следва условията и процедурите включени в настоящия документ.

Практиката на Доставчика при предоставяне на УСЛУГАТА се осъществява от обекта B-Trust Qualified Long Terms Preservation Service (B-Trust QLTPS) обозначен с идентификатор 1.3.6.1.4.1.15862.1.6.7 съгласно документа B-Trust CPS-eIDAS:

УСЛУГА за дългосрочно съхраняване на КЕП/КЕПечати (B-Trust Qualified LTPS)	Идентификатор на обект
Практика на Доставчика на УСЛУГАТА	**1.3.6.1.4.1.15862.1.6.7**

В съответствие с настоящия документ, Практиката на Доставчика изпълнява Политика относно УСЛУГАТА с идентификатори както следва:

УСЛУГАТА (B-Trust QSVS)	Идентификатор(и)
Политика на УСЛУГАТА	**1.3.6.1.4.1.15862.1.6.7.1** **0.4.0.19511.1.2**

Идентификаторът 0.4.0.19511.1.2 утвърждава, че УСЛУГАТА е приложима само към подписани/подпечатени е-документи, а не към даннови обекти изобщо (т.е., без подпис/печат).

УСЛУГАТА не утвърждава пред Потребителя/Доверяваща се страна приложимостта на дългосрочно съхранявани валидни подписи/печати, тя само утвърждава дългосрочната техническа валидност на подписа/печата.

Когато дългосрочно съхраняван успешно валидиран подпис/печат съдържа идентификатор на Политика на подписване, Доверяващата се страна може да оцени приложимостта на този подпис/печат към конкретната бизнес-цел, след като се е запознал с тази обща политика и Политиката на подписване.

Когато дългосрочно съхраняван валиден подпис/печат не включва (идентификатор на) Политика на подписване, Потребителят/Доверяващата се страна оценява приложимостта на

този подпис/печат, следвайки свои Правила/условия за приложимост или оценява приложимостта му спрямо означената Политика на удостоверението.

На практика, правната приложимост на дългосрочно съхранен валиден подпис/печат за конкретна бизнес-цел е изцяло в прерогативите на Потребителя/Доверяващата се страна. В доказателствата за съхраняване има необходимата информация (формат, профил, удостоверения, Доставчик, валидност, др.) с оглед на приложимостта, която се постига с този подпис/печат, а като следствие от това, и приложимостта му за конкретна бизнес-цел.

5.9 Управление на Политиката и Практиката

Практиката и Политиката на Доставчика за УСЛУГАТА подлежат на административно управление и контрол от страна на Съвета на директорите на „БОРИКА“ АД.

Допускат се промени, редакции и допълнения, които не засягат правата и задължения, произтичащи от този документ и стандартния договор за удостоверителни услуги между Доставчика и Потребителите/Доверяващи се страни. Те се отразяват в новата версия или редакция на документа след съгласуване и утвърждаване от Съвета на директорите.

Настоящата Политика и Практика трябва да бъдат преразглеждани най-малко веднъж годишно с цел да се отразяват потенциали изисквания и предпоставки относно промени в нивата за сигурност на алгоритми, формати и профили за подписи/печати. Всяка представена и одобрена нова версия или редакция на този документ незабавно се публикува на сайта на Доставчика.

Коментари, запитвания и разяснения по този документ могат да се отправят на:

- електронен адрес на Удостоверяващ орган: info@b-trust.org;
- електронен адрес на Доставчика: info@borica.bg;
- тел.: 0700 199 10 и факс: (02) 981 45 18 .

5.10 Други приложими документи

Този документ следва да се използва съвместно със следните документи за квалифицирани услуги на ДКУУ „БОРИКА“ АД:

- B-Trust CPS-eIDAS;
- B-Trust CP-eIDAS;
- B-Trust QSVS-eIDAS;
- B-Trust QSVS-eIDAS;
- B-Trust QTSA.

6 УСЛУГА (ПРОЦЕС НА ДЪЛГОСРОЧНО СЪХРАНВАНЕ)

6.1 Участващи страни

Страните, участващи в процеса на валидиране не е-подпис/печат са:

- Доставчик (ДКУУ), който оперира процеса на дългосрочно съхраняване;
- Абонати (Доверяващи се страни);
- Заявител/Потребител – упълномощено от Абоната лице, което ползва УСЛУГАТА;
- Косвени/външни страни/участници за процеса на дългосрочно съхраняване:
    - Страни, които са подписали/подпечатели документ(и);
    - Външни ДКУУ (техни удостоверяващи органи – CA, TSA, CRL/OCSP, QSVS);
    - Национален Доверителен списък (BG Trusted List);
    - Европейски списък на националните Доверителни списъци (List of Trusted Lists).

УСЛУГАТА има национален обхват само за клиентите на B-Trust. Доставчикът може да разшири клиентския обхват на УСЛУГАТА върху територията на страната и за клиенти на други ДКУУ, регистрирани от националния Регулатор (КРС) и опериращи в страната на базата на

двустранни споразумения. В този случай УСЛУГАТА ще прилага същите строги изисквания, които са приложими в B-Trust домейна.

.

6.2 Модел на дългосрочно съхраняване

УСЛУГАТА на ДКУУ „БОРИКА“ АД, следвайки общите нормативно утвърдени технически спецификации (RFC’s и/или TS) на IETF и на ETSI за дългосрочно съхраняване и в съответствие с представената Концепция в този документ за дългосрочно съхраняване на подписи/печати (т.е., е-документи), имплементира модела WST (УСЛУГА с Архив) и схема съгласно т. 5.5.3.3 на този документ (чрез усилване на AdES).

Съображения за избора на схемата:

- УСЛУГАТА може да се разглежда като разширение към функционалността на квалифицираната услуга за валидиране на подписи/печати B-Trust QSVS-eIDAS, която валидира стандартни формати на е-подпис/печат (XAdEX, CAdES, PAdES) с профил _LTA и е в съответствие с изискванията на Регламент 910/2014 ЕС;
- Допустимите формати на подписи/печати за дългосрочно съхраняване са еквивалентни на тези, поддържани от B-Trust QSVS-eIDAS;
- B-Trust QSVS-eIDAS валидира формати/профили на подпис/печати (е-документи) в строго съответствие с РЕШЕНИЕ ЗА ИЗПЪЛНЕНИЕ (ЕС) 2015/1506 относно Регламента, включително и ниво B_LTA; допълнително, услугата валидира подпис/печат във формат ASiC-S/E (контейнер на документи за подпис/печат) с нива на подписване (B, B_T, B_LT и B_LTA);
- B-Trust QSVS-eIDAS е част от обща платформа на ДКУУ „БОРИКА“ АД за квалифицирано подписване/подпечатване на документи и файлове, следвайки форматите/профилите посочени в РЕШЕНИЕТО (B, B_T, B_LT и B_LTA);
- Схемата с AdES (с профил _LTA) е еднотипна и лесно приложима за различните формати/профили на подпис/печати (е-документи);
- Оперативна съвместимост (в бъдеще) с друга подобна услуга (например, в национален мащаб).

6.3 Цели на дългосрочно съхраняване

УСЛУГАТА поддържа следните цели за дългосрочно съхраняване:

- интегритет на е-документ (подпис/печат);
- съществуване (преди/в даден момент) на е-документ (подпис/печат);
- съхраняване на подписан/подпечатен е-документ и поддържане на статуса на валидност на подписи/печати (е-документи) в дългосрочен план;
- поддържане на доказателство за статуса на валидност на подписи/печати (е-документи) в дългосрочен план.

За допълнителна информация, виж т. 5.2 на настоящия документ.

6.4 Доказателства относно целите на дългосрочно съхраняване

УСЛУГАТА поддържа и предоставя следните доказателства на цели за дългосрочно съхраняване:

- Доказателство за интегритет на е-документ (подпис/печат);
- Доказателство за съществуване (преди/в даден момент) на е-документ (подпис/печат);
- Доказателство за статуса на валидност на подписи/печати (е-документи).

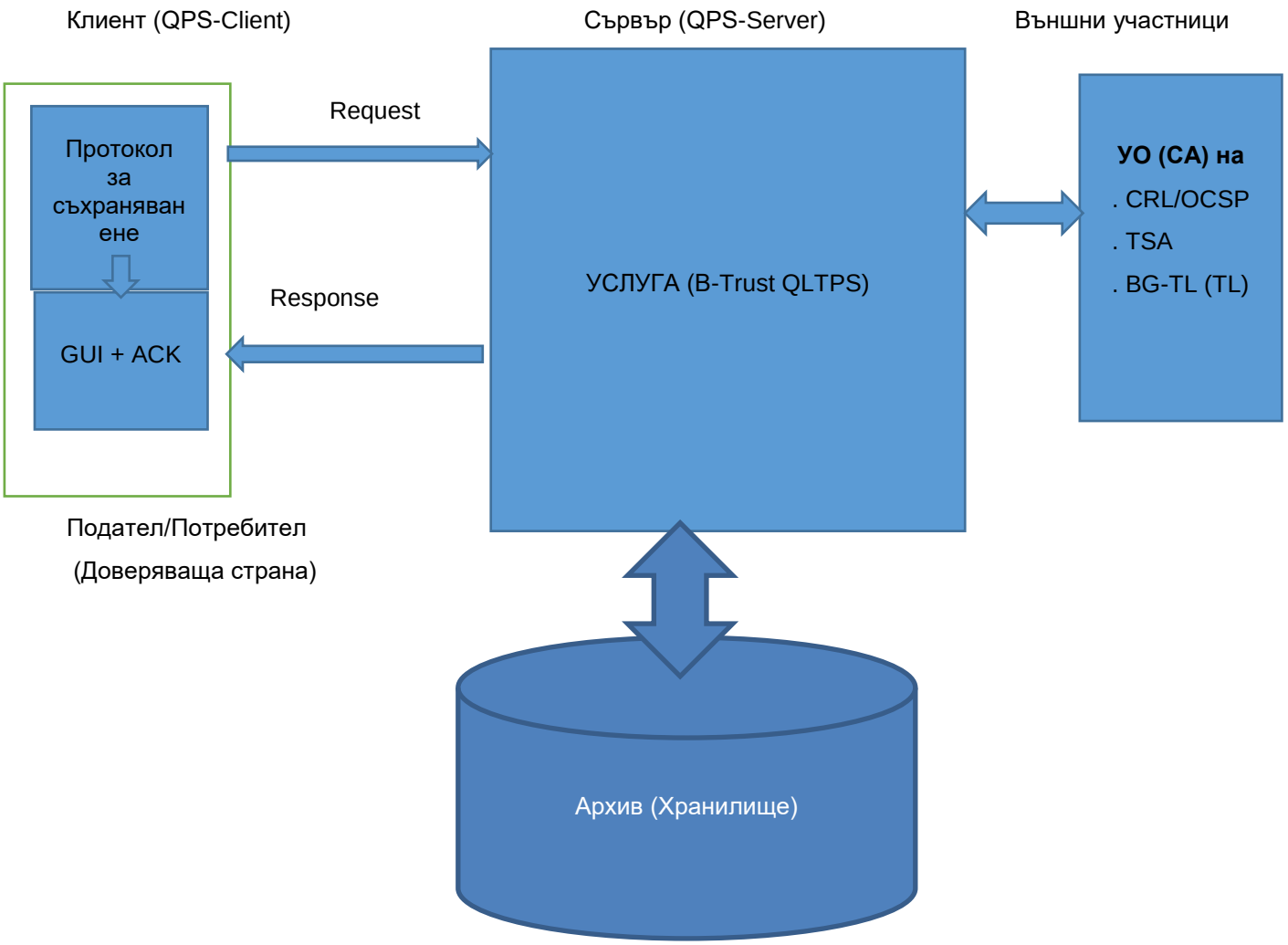
Посочените доказателства се базират на имплементираната схема на дългосрочно съхраняване, чрез която се събира, усилва и съхранява доказателствен материал заедно с първоначално подписани/подпечатени е-документи/файлове в Архива на УСЛУГАТА.

6.5 Функционален модел

УСЛУГАТА (B-Trust LTPS) на Доставчика „БОРИКА“ АД включва следните софтуерни компоненти:

- Клиент за съхраняване на подписа/печата (QPS_Client) – компонента е от страна на Заявител/Потребител. Може да бъде софтуерен клиент (в приложна система на Потребител) или уеб-браузър/уеб-клиент с графичен интерфейс (GUI) със следната функционалност:
  - заявки/функции
  - протокол за съхраняване
  - представяне доказателство на съхранение.
- Сървър за съхраняване (QPS_Sever) – уеб-сервиси (Signature/Seal Preservation Service/SPS) от страна на Доставчика със следната функционалност:
  - SPS-Upload – съгласно т. 5.6 на документа
  - SPS-Download – съгласно т. 5.6 на документа
  - SPS-ACK (Retrieve Proof) – съгласно т.5.6 на документа
  - SPS-Delete – съгласно т. 5.6 на документа
  - SPS-Monitor (вътрешна функция) – следи допустими силни криптографски и хеш алгоритмите
  - SPS-Augmentation (вътрешна функция) – съгласно т.5.6 на документа
  - протокола за съхраняване
  - интерфейси към вътрешни и външни/косвени участници/страни за УСЛУГАТА – CRL/OCSP на Удостоверяващ(и) Орган(и), TSA, BG-TL

На Фиг.1 е представен функционалния модел на УСЛУГАТА на Доставчика.



Фиг.1 Функционален модел на УСЛУГАТА

6.6 Базови процеси и процедури

Основната задача на УСЛУГАТА е дългосрочно съхраняване на валидността на електронния подпис или печат върху електронния документ/файла (е-документа). Във връзка с това и в съответствие с Политиката, УСЛУГАТА не допуска съхраняване на даннови обекти (документи и файлове) без подпис/печат.

6.6.1 Приемане/Зареждане (Upload) на е-документ

1. УСЛУГАТА приема е-документи, които трябва да бъдат архивирани само след идентифицирането на Абоната/Подателя в рамките на сигурна сесия/процедура. Защитената сесия (SSL/TLS) гарантира целостта и поверителността на заредените е-документи.

2. Политиката и Практиката информират Абоната/Подателя кои формати на подпис/печат (формат на контейнера) на е-документ приема УСЛУГАТА, как валидира електронните подписи и печати и при какви условия приема е-документи.

3. Валидността на електронния(ите) подпис(и) или печат(и) на получения от УСЛУГАТА е-документ се валидира(т) посредством пълния дългосрочен валидационен материал чрез B-QSVS. Валидирането може да се основава на частичен или пълния дългосрочен валидационен материал, приложен към електронен подпис или печат. Всяка все още необходима информация за валидирането и за дългосрочен доказателствен материал се събира от външни или вътрешни източници и се запазва към е-документа. След съставянето на дългосрочния материал за валидиране, УСЛУГАТА поставя квалифициран времеви печат на дългосрочния валидационен материал.

4. УСЛУГАТА съхранява приет е-документ криптиран. Криптирането гарантира, че неупълномощеният персонал не може да установи съдържанието на е-документа. Дешифрирането на кодирания е-документ става само в случаи, свързани с процедури като доставяне (Download), регулация (от страна на националния Регулатор) или повторно криптиране (при вече слаб криптоалгоритъм).

5. Доставчикът (УСЛУГАТА) проверява получените е-документи възможно най-скоро, но не по-късно от 3 дни от приемането и изпраща потвърждение на Абоната, че дългосрочният валидиращ материал (доказателството за валидност на подпис/печат) е съставен успешно и УСЛУГАТА е приела е-документа. Ако процесът по съставяне на доказателствен материал е неуспешен, Доставчикът (УСЛУГАТА) уведомява Абоната в съобщение за грешка. Въз основа на съобщението за грешка трябва ясно да се установи кой е-документ и каква е причината за отхвърлянето му.

6. Ако проверката за приемане на е-документ за съхранение не се потвърди пред Абоната в посочения срок, приема се, че Доставчикът/УСЛУГАТА не е приела електронния документ. Доставчикът е отговорен за съхраняването на е-документ и за осигуряването на дългосрочна валидност на включените подписи/печати след изпращане на положително потвърждение за приемане на е-документа за съхранение.

6.6.2 Доставяне (Download) на съхраняван е-документ

Доставчикът, чрез УСЛУГАТА гарантира, че Абонатът може да изтегли своите съхранявани в Архива документи и съответният материал за дългосрочно валидиране (доказателствен материал) през периода на договора за ползване на УСЛУГАТА.

1. Абонатът има достъп до е-документи и до материали (доказателства) за дългосрочно валидиране, запазени в Архива само чрез защитен канал.

2. УСЛУГАТА гарантира, че всеки Абонат има достъп само до е-документи и до материали за дългосрочно валидиране, за които той действително има право на достъп.

6.6.3 Издаване на Потвърждение (ACK) за съхраняван е-документ

По искане на Абоната, УСЛУГАТА издава Потвърждение във връзка със съхраняван е-документ. Потвърждението включва:

1. Изявление, че усъвършенстваните или квалифицирани електронни подписи, печати, времеви печати на съответните е-документи и съответните удостоверения са били валидни по време на удостоверяването с времеви печат на УСЛУГАТА и при валидиране след тяхното приемане в Архива.

2. Хешът на е-документ, името и идентификатора на Абоната.

3. Изявление, че даден е-документ има дадения хеш, така че той е идентичен на е-документ със същия хеш, представен от Абоната.

4. Времето на приемане на е-документа в архива.

УСЛУГАТА издава Потвърждението като подпечатен е-документ с квалифициран електронен печат на услугата за валидация на B-Trust QSVS или на хартиен носител.В случай на издаване на Потвърждението на хартиен носител го удостоверява длъжностно лице, отговарящо за Архива с неговия саморъчен подпис.

Издаването на Потвърждение може да бъде поискано от упълномощен представител на Абоната, ако предварително представи нотариално заверено пълномощно.

6.6.4 Визуализиране (Display) на съхраняван е-документ

УСЛУГАТА предоставя на Абоната възможност да визуализира свои е-документи съхранявани в архива на предварително определена дата и място.

6.6.5 Изтриване (Delete) на съхраняван е-документ

УСЛУГАТА предоставя по искане на абоната селективно изтриване на е-документи и всички съответстващи дългосрочни материали за валидиране (доказателства), съхранявани в Архива,. Заличаването означава физическото изтриване на съхраняван е-документ по такъв начин, че не може да бъде възстановен по-късно (или само с нереалистично високи финансови разходи). Заличаването се извършва върху цялата система на Доставчика като със заличаването се унищожава всяко запазено копие от е-документа.

6.7 Прекратяване на Договора за УСЛУГАТА

При прекратяване на Договора за УСЛУГАТА, Доставчикът предоставя е-документите и материалите за дългосрочно валидиране, които Абоната е поръчал да бъдат запазени за изтегляне (Download) от него или от друго оправомощено лице. След прекратяването на договора, Доставчикът трябва да заличи документите и дългосрочния валидационен материал на Абоната, чийто Договор е прекратен.

6.8 Интерфейси и протоколи

Доставчикът оперира и поддържа УСЛУГАТА като уеб-сервис, който се достъпва чрез:

- OASIS DSS интерфейс;
- GUI интерфейс.

И двата интерфейса използват защитен комуникационен канал, поддържащ автентификация на Заявителя/Потребител на УСЛУГАТА.

УСЛУГАТА се автентифицира пред Заявителя/Потребителя (Доверяващата се страна) чрез квалифицирано удостоверение за автентичност на уебсайт, издадено на нейната сървърна компонента (SPS_Server) от УО B-Trust Operational Advanced CA на B-Trust на ДКУУ„БОРИКА“ АД.

6.8.1 OASIS DSS интерфейс

QPS_Client приложение достъпва УСЛУГАТА чрез OASIS DSS Интерфейс, който дефинира набор от XML-команди (Requests/Responses) на протокола на УСЛУГАТА.

Протоколът на OASIS DSS интерфейса използват за транспорт SOAP-протокол, който пренася XML-командите (Requests/Responses) на УСЛУГАТА.

6.8.2 GUI интерфейс

УСЛУГАТА се достъпва от Заявителя/Потребителя (Доверяваща се страна) посредством уеб-приложение, което работи с неговия браузър и ползва графичен интерфейс. Посредством него Потребителя изпълнява процедурите/функциите от т. 6.7 на документа.

Този интерфейс използва HTTP(S) POST протокол за транспорт/обмен.

6.9 Външни източници на доказателствен материал за съхраняване

В определени случаи, например, събиране на доказателствен валидационен материал за съхраняване на подписи/печати, УСЛУГАТА изисква достъп до външни източници, свързани с процеса на валидиране на подписа/печата към подписан/подпечатен документ, който подлежи на дългосрочно съхраняване в Архива на Услугата. Такива външни участници във процес на дългосрочно съхраняване са:

- хранилища на удостоверения, поддържани от ДКУУ – Публични регистри, CRL/OCSP източници; TSA/удостоверяващи органи на време (времеви печати);
- национален Доверителен списък, външни (на страни-членки) Доверителни списъци (TL);

УСЛУГАТА използва стандартизирани програмни интерфейси за достъп до тези външни източници, за да достави доказателствен валидационен материал при съхраняване на подписи/печати в Архива.

7 ТЕХНИЧЕСКИ МЕРКИ ЗА СИГУРНОСТ

7.1 Гаранции за сигурност

Доставчикът на УСЛУГАТА използва надеждни системи и продукти, които са защитени срещу неправомерно модифициране. Доставчикът съхранява архивираните е-документи във физически защитена среда в съответствие с физическите и процедурните изисквания, описани в Раздел 5 на документа B-Trust CPS-eIDAS (общата Практика на ДКУУ „БОРИКА“ АД) и е гарантирана от политиките за вътрешна сигурност и редовните одити за вътрешна и външна сигурност.

Доставчикът криптира електронните документи винаги с алгоритъм, който се счита за сигурен/безопасен при дадено състояние на технологията и съхранява е-документите чрез криптирани.

7.2 Предпазни мерки за компютърна сигурност

Доставчикът използва надеждни ИТ системи и решения, технологии и резервираност в системите на УСЛУГАТА. Критичните компоненти на системата са резервирани. Използва не система от защитни стени (Firewalls) в ИТ-инфраструктурата на УСЛУГАТА.

7.3 Технически предпазни мерки, свързани с жизнения цикъл

Използват се системни елементи за УСЛУГАТА като се отчитат съображенията за сигурност, свързани с жизнения цикъл на компонентите.

7.4 Регулярен Одит/Сертифициране

Доставчикът на УСЛУГАТА е ДКУУ и дейността му подлежи на регулярен Одит в съответствие с Регламент 910/2014. Издаден и/или подновен сертификат на Доставчика на УСЛУГАТА удостоверяват съответствие на УСЛУГАТА с този документ. Виж т. 8 на документ „Практика при предоставяне на квалифицирани удостоверения и удостоверителни услуги за тях от „БОРИКА“ АД (B-Trust CPS-eIDAS)“.

7.5 Повторно криптиране (Прекриптиране) на Архива

Доставчикът гарантира, че архивираните е-документи са криптирани с алгоритъм за криптиране, който е сигурен/надежден по всяко време. Това изискване обуславя потребност от прекриптиране на Архива в бъдеще, когато използвания крипто-алгоритъм се приема за слаб/несигурен.

7.6 (Непрекъснат) мониторинг на технологиите

Доставчикът на УСЛУГАТА непрекъснато наблюдава развитието на технологиите, свързани с електронния подпис и криптографията. В случай, че техническа спецификация или нормативен документ обяви криптографски алгоритъм с даден параметър за рисков (недостатъчно сигурен), Доставчикът предприема съответни мерки да отстрани евентуален риск.

7.7 Избор на външни доставчици

Обхватът на УСЛУГАТА адресира (засега) само Потребителите на B-Trust. Настоящата версия на УСЛУГАТА не използва външни източници за събиране на доказателствен валидационен материал за подписи/печати.

7.8 Поддръжка на оперативна съвместимост на подпис/печати

Съгласно Политиката на УСЛУГАТА, Доставчикът съхранява само подписи/печати (е-документи) с международно утвърдени профили и нива на подписване, с оглед на бъдеща оперативна съвместимост с други подобни услуги за съхраняване.

8 ОЦЕНКА НА РИСКА

Отчитайки установени бизнес и технически проблеми при доставка, опериране и поддръжка на УСЛУГАТА, Доставчикът извършва оценка на риска за да идентифицира, анализира и оцени свързаните с това рискове.

Избират се подходящи мерки за избягване на идентифицирани рискове като се отчитат резултатите от оценката на риска. Приеманите мерки гарантират ниво на сигурност, съизмеримо със степента на идентифицираните рискове.

Доставчикът документира чрез Практиката и Политиката, включени като части от настоящия документ, изискванията към сигурността и оперативните процедури, необходими за избягване на идентифицирани рискове за УСЛУГАТА.

Периодично се изпълнява преглед и оценка на риска с цел преодоляване на идентифицирани рискови фактори.

Мениджмънтът на Доставчика одобрява резултатите от оценката на риска, предписаните мерки за преодоляване на идентифицирани рискови фактори и приема установения остатъчен риск относно УСЛУГАТА.

Виж документ „Практика при предоставяне на квалифицирани удостоверения и удостоверителни услуги за тях от „БОРИКА“ АД (B-Trust CPS-eIDAS).

9 ПРАКТИКА

Посочените в този документ процедури, механизми по контрол и технически характеристики на УСЛУГАТА са допълнение към съответните части в документа „Практика при предоставяне на квалифицирани удостоверения и удостоверителни услуги за тях от „БОРИКА“ АД (B-Trust CPS-eIDAS), които регламентират общите условия, дейности и процедури на „БОРИКА” АД като ДКУУ по предоставяне на квалифицирани удостоверителни услуги.

9.1 Служебни удостоверения на УСЛУГАТА

УСЛУГАТА има едно публично удостоверение:

-
- квалифицирано удостоверение за автентичност на уеб-сайт.

Доставчикът вътрешно използва квалифицираната услуга за валидация на подпис/печат B-Trust QSVS за да получи и достави на Потребител/Доверяваща се страна Потвърждение (доказателствен материал) за дългосрочно съхраняване на подписа/печата (е-документа). Потвърждението (отчета от валидация) е електронно подпечатен с квалифициран е-печат на услугата B-Trust QSVS. Виж документ “B-Trust QSVS” на ДКУУ „БОРИКА“ АД. Удостоверението на е-печата към Потвърждението (отчета) автентифицира Доставчика (B-Trust QSVS) като източник на генерираното Потвърждение за съхраняване на електронно подписан/подпечатен е-документ и утвърждава целостта на данните в Потвърждението.

Удостоверението за уеб-сайт на B-Trust Qualified LTPS е квалифицирано удостоверение за уеб-сайт (организация) и е електронно подпечатано с частен ключ на Оперативния удостоверяващ орган B-Trust Operational Advanced CA на Доставчика. Това удостоверение онлайн автентифицира сайта на УСЛУГАТА пред Абоната/Потребителя и обслужва защитена SSL/TLS сесия с Потребителя.

Профилът на квалифицираното удостоверение за автентичност на уеб-сайт (организация) на УСЛУГАТА е съгласно документа „Политика при представяне на квалифицирани удостоверения за автентичност на уеб-сайт (B-Trust QCP-eIDAS Web SSL/TLS) на „БОРИКА“ АД и е посочен по-долу:

Поле	Атрибути	Значение/Стойност
Version	-	V3
Serial number	-	29 b9 2a 55
Signature algorithm	-	Sha256RSA
Signature hash algorithm	-	Sha256
Issuer	CN =	B-Trust Operational Advanced CA
	OU =	B-Trust
	O =	BORICA AD
	OrganizationIdentifier(2.5.4.97) =	NTRBG-201230426
	C =	BG
Validity from	-	2019-02-27T11:52:42Z
Validity to	-	2021-06-01T12:52:42Z
Subject	CN =	qltps.b-trust.org
	O =	BORICA AD
	2.5.4.97= (organizationIdentifier)	NTRBG-201230426
	OU	OV SSL
	C =	BG
Public key	-	RSA(2048 bits)
SubjectAlternativeName		https://qltps.b-trust.org
Subject Key Identifier	-	8b 07 4f 9d fc 60 23 1c da be 68 a2 dd 1d fe 90 c3 f0 cc 67

Authority Key Identifier	KeyID =	07 dc aa 30 76 98 b7 85 4b 6d 03 18 c8 e3 cd a7 7b 36 82 ef	
Issuer Alternative Name	URL =	http://www.b-trust.org	
Basic Constraints	Subject Type = Path length Constraint =	End Entity None	
Certificate Policy	-	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.15862.1.7.1.6 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.b-trust.org/documents/cps [2]Certificate Policy Policy Identifier=1.3.6.1.4.1.15862.1.6.7.1 [3] Certificate Policy Policy Identifier=0.4.0.19511.1.2 [4]Certificate Policy: Policy Identifier=2.23.140.1.2.2 [5]Certificate Policy: Policy Identifier=0.4.0.2042.1.7 [6]Certificate Policy: Policy Identifier=0.4.0.194112.1.4 (qcp-w)???	
Enhanced Key Usage	-	Server Authentication, Client Authentication	
CRL Distribution Points	-	[1] CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.b-trust.org/repository/B-TrustOperationalACA.crl	
Authority Information Access	-	[1] Authority Info Access Access Method=On-line Certificate Status Protocol Alternative Name: URL=http://ocsp.b-trust.org [2] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://ca.b-trust.org/repository/B-TrustOperationalACAOCSP.cer	
Key Usage (critical)	-	Digital Signature, Key Encipherment	
Qualified Statement	Qualified Certificate Statement:	id-qcs-pkixQCSyntax-v2 (oid=1.3.6.1.5.5.7.11.2)	id-etsi-qcs-SemanticsId-Legal (oid=0.4.0.194121.1.2)
		id-etsi-qcs-QcType (oid=0.4.0.1862.1.6)	id-etsi-qct-web (oid=0.4.0.1862.1.6.3)
		id-etsi-qcs-QcPDS (oid=0.4.0.1862.1.5)	PdsLocations PdsLocation=https://www.b-trust.org/documents/pds/qltps_pds_en.pdf language=en
Thumbprint (Sha1)		ed 14 85 aa c9 38 44 c0 11 7a 27 c2 01 d1 d1 b0 44 4e c0 6f	
Thumbprint (Sha256)		33 ea 95 fc f1 7f d2 bc fa c4 f3 af 06 25 bd 8f 8f d1 0e b0 c7 dd fb 7a c4 a1 0a 0b 24 31 b3 c6	

B-Trust използва следните алгоритми за електронен подпис/печат и защита на данните:

Наименование	**Алгоритъм**
Хеш-алгоритми:	SHA 256
Асиметрични алгоритми:	RSA
Симетричен алгоритъм	AES

9.2 Средства, управление и оперативен контрол на УСЛУГАТА

9.2.1 Вътрешна организация при Доставчика

„БОРИКА“ АД, регистриран ДКУУ по смисъла на Регламент 910/2014 и Закона за електронния документ и удостоверителните услуги (ЗЕДЕУУ) е Доставчик на УСЛУГАТА. Тази квалифицирана удостоверителна услуга работи и се поддържа чрез инфраструктурата на публични ключове B-Trust® , която е организационно звено на Доставчика. Документ „ Практика при предоставяне на квалифицирани удостоверения и удостоверителни услуги за тях от „БОРИКА“ АД (B-Trust CPS-eIDAS)“ относно вътрешната организация на тази инфраструктура и предоставяните чрез нея квалифицирани удостоверителни услуги, е приложим и към УСЛУГАТА.

9.2.2 Персонал

Характеристиката на персонала на ДКУУ, отговарящ за опериране и поддръжка на УСЛУГАТА и назначените длъжности са в съответствие с документа „ Практика при предоставяне на квалифицирани удостоверения и удостоверителни услуги за тях от „БОРИКА“ АД (B-Trust CPS-eIDAS)“.

9.2.3 Управление на активи

Управлението на активите на инфраструктурата B-Trust® на ДКУУ „БОРИКА“ АД съгласно документа „Практика при предоставяне на квалифицирани удостоверения и удостоверителни услуги за тях от „БОРИКА“ АД (B-Trust CPS- eIDAS)“ е приложимо за УСЛУГАТА.

9.2.4 Управление на достъпа

Всички компоненти, изискващи физическа и логическа защита относно критични данни и информация (сървъри, комуникационно оборудване, ключове, хранилища/архиви, др.) са обособени в помещения и зони с висока защита на достъпа. Физическият и логически контрол на достъпа до средата/инфраструктурата на B-Trust® на ДКУУ е в съответствие с документа „Практика при предоставяне на квалифицирани удостоверения и удостоверителни услуги за тях от „БОРИКА“ АД (B-Trust CPS-eIDAS)“ и е приложим към УСЛУГАТА.

9.2.5 Криптографска сигурност – управление на ключове

9.2.5.1 Генериране на двойката ключове

Двойката RSA ключове към квалифицираното удостоверение за усъвършенстван е-печат и за автентичност на уеб-сайт на УСЛУГАТА се генерира в софтуерна среда с висока степен на сигурност (PKCS#12) от персонал на Доставчика, който има право да изпълнява тази роля. Генерираните двойки RSA ключове са с дължина 2048 бита.

Описанието и ролята на този персонал са посочени в документа „Практика при предоставяне на квалифицирани удостоверения и удостоверителни услуги за тях от „БОРИКА“ АД (B-Trust CPS-eIDAS)“.

Средата за генериране на двойките ключове на УСЛУГАТА е описана в същия документ.

Процедурите по генериране на тези двойки ключове е в съответствие с документи „Политика при предоставяне на квалифицирани удостоверения за усъвършенстван електронен подпис/печат от „БОРИКА“ АД (B-Trust QCP-eIDAS AES/AESeal)“ и „Политика при предоставяне на квалифицирани удостоверения за автентичност на уеб-сайт от „БОРИКА“ АД (B-Trust QCP-eIDAS Web SSL/TLS)“.

9.2.5.2 Защита на частен ключ

Генерираните частни ключове на УСЛУГАТА се съхранява чрез криптографски файл със структура PKCS#12, защитен с надеждна парола. В специален сейф, се съхранява копие на криптографския файл за възстановителни цели.

9.2.5.3 Разпространение на публичния ключ

Публичните ключове на УСЛУГАТА са удостоверени чрез удостоверенията за усъвършенстван печат и автентичност на уебсайт, издадени от съответните Оперативни Удостоверяващи Органи в B-Trust-йерархията на Доставчика.

Доставчикът публикува удостоверението за автентичност на уеб-сайт на УСЛУГАТА на интернет страница на сайта си.

За да автентифицира УСЛУГАТА, Заявител/Потребител (Доверяваща се страна) следва да е заредил на своя система оперативното удостоверение на Удостоверяващ Орган B-Trust Operational Advanced CA (част от удостоверителните вериги на B-Trust, също публикувани на страница на сайта на Доставчика).

9.2.5.4 Продължаване на срока и/или преиздаване на удостоверението

Периодът на валидност на удостоверенията на УСЛУГАТА е 5 години. След изтичане на този период, срокът на валидност на удостоверението се продължава за период от 3 години. След този период се генерира нова двойка ключове за съответното удостоверение, частният ключ от която се съхранява в нов криптографски файл PKCS#12, а публичният ключ се удостоверява, чрез издаване на ново удостоверение на УСЛУГАТА. Двойката ключове с изтекъл период на валидност се съхранява, както следва:

- частен ключ – съхранява се за период от 10 години;
- публичен ключ – съхранява се за период от 10 години.

9.2.6 Физическа и околна среда

Приложените мерките и средствата относно физическата и околна среда към инфраструктурата B-Trust® на Доставчика съгласно документа „Практика при предоставяне на квалифицирани удостоверения и удостоверителни услуги за тях от „БОРИКА“ АД (B-Trust CPS-eIDAS)“ (т.5.1.) са в сила и се изпълняват за УСЛУГАТА.

9.2.7 Операционна сигурност

Операционната сигурност на платформата на УСЛУГАТА отговаря на изискванията за сигурността на компютърните системи в инфраструктурата на B-Trust съгласно документа „Практика при предоставяне на квалифицирани удостоверения и удостоверителни услуги за тях от „БОРИКА“ АД (B-Trust CPS-eIDAS)“ (т.т. 6.6, 6.7, 6.8).

9.2.8 Мрежова сигурност

Виж „Практика при предоставяне на квалифицирани удостоверения и удостоверителни услуги за тях от „БОРИКА“ АД (B-Trust CPS-eIDAS)“ (т. 6.9).

9.2.9 Управление на журнали

Съгласно документа „Практика при предоставяне на квалифицирани удостоверения и удостоверителни услуги за тях от „БОРИКА“ АД (B-Trust CPS-eIDAS)“ (т. 5.4).

9.2.10 Непрекъсваемост

Съгласно прилаганите от Доставчика общи мерки, гарантиращи непрекъсваемост на функционирането на B-Trust инфраструктурата, в това число, на квалифицирани удостоверителни услуги, базиращи се на резервираност на критичните компоненти на инфраструктурата.

9.2.11 Прекратяване на услугата

В случай на прекратяване на УСЛУГАТА се изпълняват съответните процедури, съгласно документа „Практика при предоставяне на квалифицирани удостоверения и удостоверителни услуги за тях от „БОРИКА“ АД (B-Trust CPS-eIDAS)“ (т. 5.9).

9.3 Информационна сигурност

„БОРИКА“ АД не публикува отделна Политика на информационна сигурност за УСЛУГАТА.

Доставчикът оперира, поддържа и предоставя УСЛУГАТА като използва общата инфраструктура на публични ключове B-Trust®, чрез която предоставя квалифицирани удостоверителни услуги (квалифицирани удостоверения на подпис/печат и квалифицирани времеви печати) съгласно Регламент 910/2014.

Информационната сигурност на компонентите на B-Trust инфраструктурата е част от общата Политика на информационна сигурност на „БОРИКА“ АД, утвърдена от ръководството на фирмата. Тази политика установява организационните мерки и процедури по управление на сигурността на системите и информационните активи, чрез които се предоставят услугите. Персоналът, имащ пряко отношения към тези системи и активи е запознат с и изпълнява тази Политика. Виж документ „Практика при предоставяне на квалифицирани удостоверения и удостоверителни услуги за тях от „БОРИКА“ АД (B-Trust CPS-eIDAS).

Дългосрочно съхранявани в Архива подписи/печати (е-документи) могат да съдържат информация, която да се счита за лични данни. В съответствие с нормативната уредба относно такъв тип данни, „БОРИКА“ АД като ДКУУ, респективно като Доставчик на УСЛУГАТА, е регистрирана от КЗЛД като администратор на лични данни.

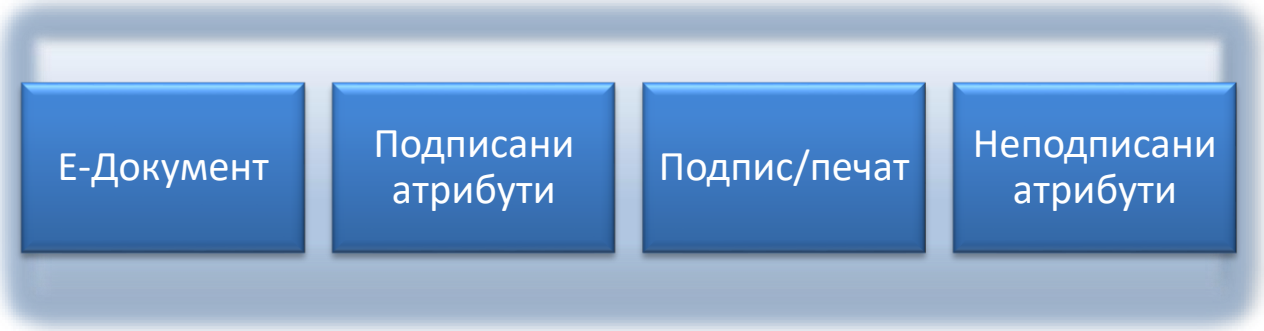
Дългосрочно съхраняваните е-документи в Архива са криптирани. Само оторизирани лица от персонала на Доставчика на УСЛУГАТА изпълняват функция по декриптиране, респективно повторно криптиране на съхраняваните подписи/печати (е-документи) в Архива.

10 ДРУГИ БИЗНЕС УСЛОВИЯ И ПРАВНИ АСПЕКТИ

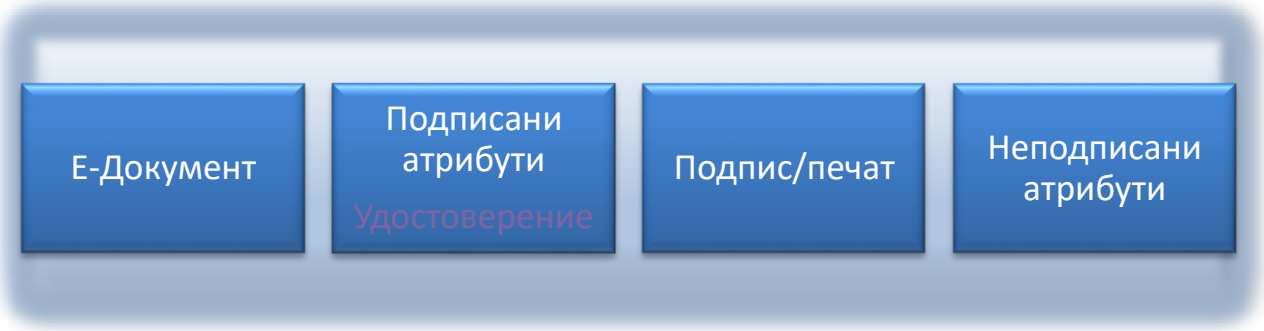
Съгласно т. 9 на документа „Практика при предоставяне на квалифицирани удостоверения и удостоверителни услуги за тях от „БОРИКА“ АД (B-Trust CPS-eIDAS)“.

Приложение 1. Профили на е-подпис/печат и нива на подписване (е-документ), допустими за УСЛУГАТА

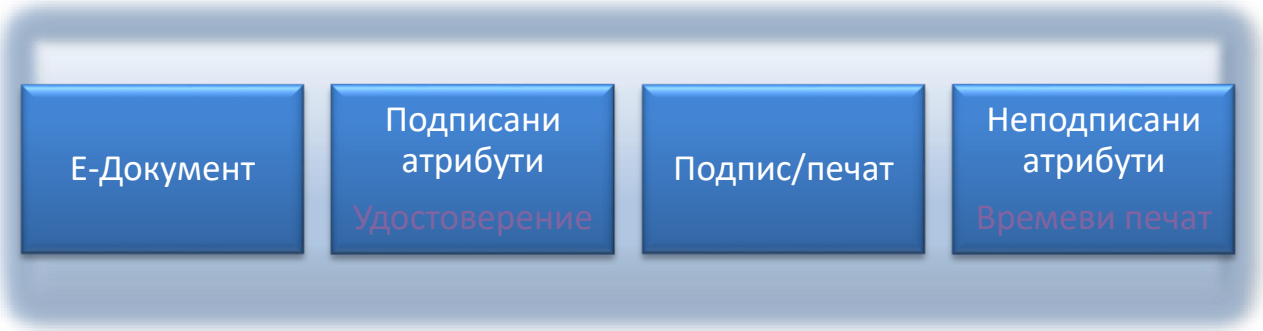
1. Обща структура на Е-подпис/печат



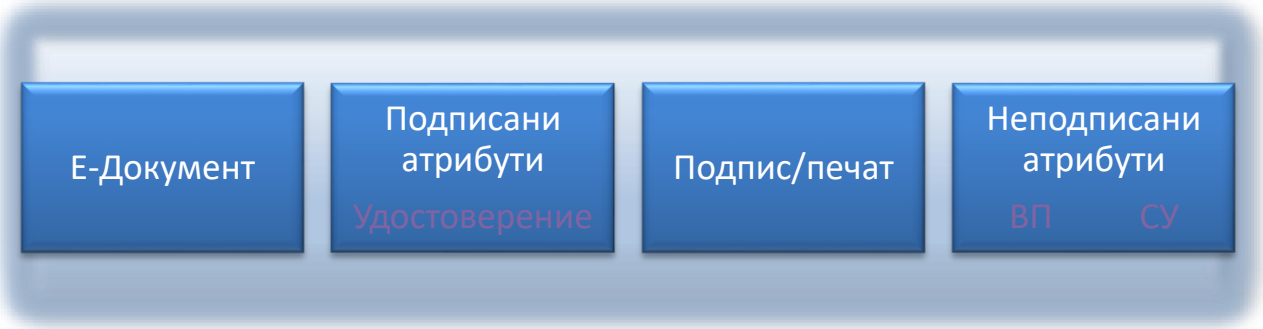
2. Базов е-подпис/печат (**BASELINE_B**)



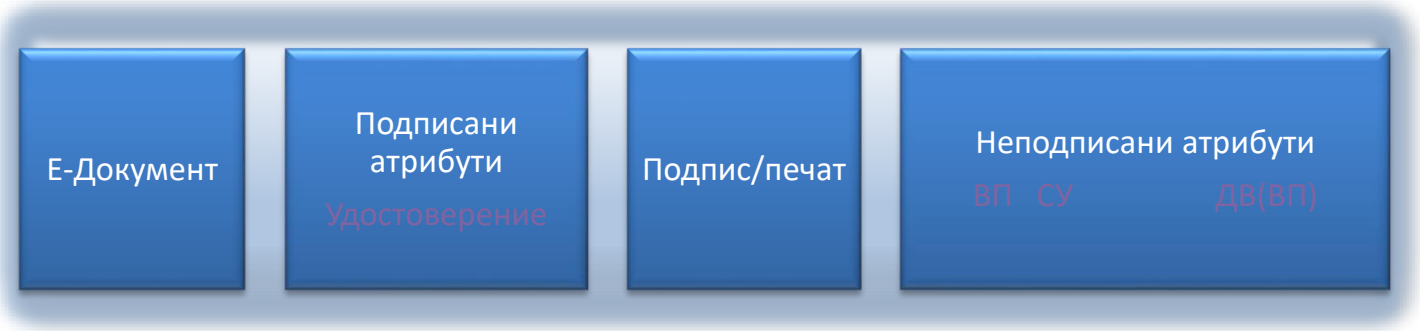
3. Профил **BASELINE_T** (с удостоверено време на подписа/печата)



4. Профил **BASELINE_LT** (с удостоверено време + статус на удостоверение)



5. Профил **BASELINE_LTA** (време + статус + допълнителни статус + време)



ВП – времеви печат

СУ – статус на удостоверение

ДВ – допълнителни данни за валидация