Общодостъпен документ

ПОЛИТИКА И ПРАКТИКА

ЗА ПРЕДОСТАВЯНАТА ОТ „БОРИКА“ АД УСЛУГА ЗА КВАЛИФИЦИРАНО ВАЛИДИРАНЕ НА КВАЛИФИЦИРАНИ ЕЛЕКТРОННИ ПОДПИСИ и ПЕЧАТИ

(B-Trust Qualified Signature Validation Service (B-Trust QSVS))

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	20.05.2018	Утвърден	Първо издание.
2.0	Димитър Николов	01.04.2019	Утвърден	Технически корекции.
3.0	Димитър Николов	01.03.2020	Утвърден	Технически корекции

СЪДЪРЖАНИЕ

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 услугата за квалифицирано валидиране на квалифициран електронен подпис и печат (означавана в документа с УСЛУГА) в съответствие с техническите спецификации ETSI EN 319 102-1, ETSI TS 119 101, ETSI TS 119 441 и ETSI TS 119 442 за тази услуга, оперирана от Доставчик на квалифицирани удостоверителни услуги (ДКУУ) „БОРИКА“ АД;
- 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;
- дефинира 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 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 валидиране на квалифицирани е-подпис/печати в съответствие с Регламент 910/2014;
- определя основните формати на е-подписи/печати, към които е приложима УСЛУГАТА;
- определя протоколите и интерфейсите на УСЛУГАТА;
- определя връзките с „външни“ квалифицирани услуги (например CRL, OCSP, TSA), предоставящи информация на УСЛУГАТА;
- адресира само техническите аспекти на валидност на е-подписа/печата, но не и проверката за 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.

Извън обхвата на документа са:

- Правната приложимост (правила за приложимост) към различни бизнес-цели на квалифицирания е-подпис/печат; спецификацията ETSI TS 119 172-1 може да послужи за тази цел;
- Техническите аспекти на формати, синтаксисът, кодировката на е-подписа/печата, конкретните формати, профили и кодировка на документите за подпис/печат;
- Процесите на подписване, т.е. генериране на квалифициран е-подпис/печат;

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 119 441 Policy Requirement for TSP providing signature validation services.
- ETSI TS 119 442: "Electronic Signatures and Infrastructures (ESI); Protocol for TSPs providing signature validation services"
- ETSI EN 319 401: "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers".
- ETSI TS 119 101: "Electronic Signatures and Infrastructures (ESI); Policy and security
- requirements for applications for signature creation and signature validation".
- 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;

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

- 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

Валидиране (Validation) – цялостен процес на верифициране и потвърждаване на валидността на е-подпис/печат.

Приложимост на е-подпис/печат (Signature applicability) – определяне на правната приложимост на е-подписа/печата към определени бизнес-цели.

„Външно” приложение (Driving application) – приложение/компонента, което използва процеса на валидиране на подписа/печата за да го валидира.

Правила за приложимост на е-подпис/печат (Signature applicability rules) – правила, които определят (правната) приложимост на подписа/печата за конкретни бизнес-цели (например, за квалифицирано време на подписа/печата, за идентификация на Титулярят/Създател, за квалификация на подписа/печата, за доклад от валидиране, др.).

Квалифициран е-подпис/печат (Qualified e-signature/e-seal/QES) – съгласно Регламент 910/2014.

Усъвършенстван електрон подпис/печат с квалифицирано удостоверение (Advanced e-signature/e-seal with Qualified certificate/AES_QC) – съгласно Регламент 910/2014

Усилен квалифициран е-подпис/печат (Augmentation of e-signature) – квалифициран е-подпис/печат с базов профил и включени към него данни, позволяващи валидността на е-подписа/печата да се поддържа извън периода на валидност на ассоциираното с подписа/печата удостоверение) (например, профили BASELINE_T, BASELINE_LT, BASELINE_LTA).

Формат на е-подпис (Signature class) – даннова структура (XLM, CMS, PDF) за подписи/печати за постигане на определена функционалност (CAdES, XAdES, PAdES, ASiC).

Профил на е-подпис (Signature Level) – специфичен формат, определящ набор от включени към подписа данни (BASELINE_B, BASELINE_T, BASELINE_LT, BASELINE_LTA), позволяващи постигане на определена бизнес-цел.

Опакован е-подпис (Enveloping signature) - подписаният документ съдържа подписа, т.е. подписът е поделемент в подписания документ.

Опаковащ е-подпис (Enveloped signature) – подписът съдържа подписания документ, т.е. документът е поделемент на подписа.

Обособен е-подпис (Detached signature) - подписът и документът се намират в отделени файлове.

Схема на е-подпис/печат (Signature scheme) – тройка от: алгоритъм за създаване, алгоритъм за проверка и алгоритъм за генериране на двойка криптоключове.

Приложение/Сървис за валидиране на е-подпис (Signature Validation Application/Service – SVA/SVS) – приложение/сървис за валидиране е-подписа/печата в съответствие с Политиката на валидиране, включваща набор от ограничения и доставка на статус-индикатор и доклад от валидирането.

Услуга за валидиране на е-подпис/печат (Service Validation Service/SVS) – система, достъпна през мрежа, която валидира е-подпис/печат.

Квалифицирано валидиране на квалифициран е-подпис/печат (Qualified Validation Service of Qualified e-signature/e-seal/QSVS) – квалифицирано валидиране, в съответствие с Регламент 910/2014 (чл. 32, 33 и 40) – услуга за валидиране в съответствие с този документ.

Клиент за услугата за валидиране на е-подпис/печат (Signature Validation Service Client/SVS Client) –софтуер, който имплементира протокола за валидиране от страна на потребителя на услугата за валидиране.

Сървър на услугата за валидиране на е-подпис/печат (Signature Validation Service Server/SVS Server) – софтуер на УСЛУГАТА от страна на ДКУУ, който имплементира протокола за валидиране и изпълнява процеса на валидиране.

Политика на услугата за валидиране на е-подпис/печат (Signature Validation Service Policy/SVS Policy) – набор от ограничения за валидиране на е-подпис/печат, който управлява (се обработва от) модула за валидиране (SVA) – Политика на Доставчика за УСЛУГАТА; Политиката е техническа концепция и се лимитира от конкретен набор от ограничения.

Отчет на услугата за валидиране (Signature Validation Service Report/SVS Report) – доклад от процеса на валидиране на е-подписа/печата, който се представя на „външното“ приложение или на потребителя за техническа оценка на приложимостта му.

Практика на услугата за валидиране на е-подпис/печат (Signature Validation Service Practice Statement/SVS Practice Statement) – наборът от процедури за доставка/поддръжка на услугата за валидиране.

Ограничение (за валидиране на е-подпис) (Validation Constraint) – технически критерий (функционално изискване, стойност, диапазон и резултат), срещу който се валидира подписа/печата (съгласно EN 319 102-1).

Статус на валидиране на е-подпис/печат (Signature validation status) – един от следните стаус-индикатори на УСЛУГАТА – ВАЛИДАН (TOTAL-PASSED), НЕВАЛИДЕН (TOTAL-FAILLED) или НЕОПРЕДЕЛЕН (INDETERMINATE).

Доверителен списък (Trusted List/TL) – национален доверителен списък (или на страна-членка)

Списък на Доверителни списъци (List of Trusted Lists/LoTL) – Европейски списък на Доверителни списъци.

3.2 Съкращения

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

QC (КУ) – Квалифицирано удостоверение

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

AdES_QC (УЕП_КУ) - Усъвършенстван Електронен Подпис с Квалифицирано удостоверение

AdESeal (УЕПечат) – Усъвършенстван Електронен Печат с Квалифицирано удостоверение

DA – „Външно” приложение, свързано с процеса на валидиране

OCSP (status) – Онлайн статус на удостоверение

PKI – Инфраструктура на публични ключове

SD – Документ за подписване

SDO – Подписан документ

SVA – Валидиращо приложение

SVI – Валидиращ интерфейс

SVP – Валидиращ протокол

SVR – Заявка за валидиране

QSVS/SVS – Квалифицирана Услуга за Валидиране („УСЛУГА“)

SVS_Client – Клиент (софтуерен) на УСЛУГАТА

SVSP – Доставчик на услугата за Валидиране (ДКУУ „БОРИКА” АД)

SVS Policy – Политика на валидиране

SVS Practice – Практика на валидиране

SVS_Report – Доклад/Отчет от валидиране

SVS_Server – Сървър на УСЛУГАТА

TL – Доверителен списък (национален)

LoTL – Европейски списък на Доверителни списъци

КЗЛД – Комисия за Защита на Личните Данни

4 КОНЦЕПЦИЯ

4.1 Общи изисквания

Квалифицираната услуга за валидиране на квалифициран електронен подпис/печат (УСЛУГА) на ДКУУ „БОРИКА“ АД (Доставчик) е част от оперираната от него общата инфраструктура на публични ключове B-Trust®.

Изискванията и условията, съдържащи се в този документ адресират Политиката и Практиката на Доставчика относно УСЛУГАТА при работа с квалифициран електронен подпис/печат (КЕП/КЕПечат) и/или усъвършенстван електронен подпис/печат поддържан от квалифицирано удостоверение (УЕП_КУ/УЕПечат_КУ).

Относно общите изисквания към политиката и практиката на Доставчика, структурата и съдържанието на документа съответстват на ETSI EN 319 401 като включват специфичните изисквания за квалифицираното валидиране на КЕП/КЕПечат и УЕП/УЕПечат_КУ съгласно ETSI TS 119 441 и ETSI TS 119 442.

Потребители (Доверяващи се страни) трябва да използват настоящия документ, за да получат точно описание и оценка на сигурността на УСЛУГАТА и техническата валидност на валидираните КЕП/КЕПечати и УЕП_КУ/УЕПечати_КУ.

4.2 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 валидира квалифициран е-подпис/печат и/или усъвършенстван подпис/печат придружен от квалифицирано удостоверение на всяка заинтересована страна, като съблюдава обща Политика на валидиране.

Правило в Практиката на Доставчика на УСЛУГАТА е да валидира подпис/печат с формати съгласно Политиката му като следва условията и процедурите включени в настоящия документ.

Практиката на Доставчика при предоставяне на УСЛУГАТА се осъществява от обект B-Trust QSVS на B-Trust обозначен с идентификатор 1.3.6.1.4.1.15862.1.6.6:

УСЛУГА за квалифицирано валидиране на квалифицирани е-подписи и е-печати (B-Trust QSVS)	Идентификаторт
Практика на Доставчика на УСЛУГАТА	**1.3.6.1.4.1.15862.1.6.6**

В съответствие с ETSI EN 319 441 и този документ, Практиката на Доставчика изпълнява обща Политика относно УСЛУГАТА с идентификатори както следва:

УСЛУГА (B-Trust QSVS)	Идентификатор(и)
Политика на УСЛУГАТА	**1.3.6.1.4.1.15862.1.6.6.1** **0.4.0.19441.1.1** **0.4.0.19441.1.2**

Идентификаторът 0.4.0.19441.1.1 утвърждава съответствие Политиката за валидиране на Доставчика съгласно този документ с ETSI TS 119 441.

Идентификаторът 0.4.0.19441.1.2 утвърждава, че УСЛУГАТА е квалифицирана.

УСЛУГАТА не утвърждава пред Потребителя/Доверяваща се страна приложимостта на валидирания подпис/печат, тя само утвърждава техническата валидност на подписа/печата.

Когато успешно валидиран подпис/печат съдържа идентификатора на Политика на подписване, Доверяващата се страна може да оцени приложимостта на валидирания подпис/печат към конкретната бизнес-цел, след като се е запознал с тоози документ и съитветната Политика на подписване.

Когато подписът/печатът за валидиране не включва идентификатор на Политика на подписване, Потребителят/Доверяващата се страна оценява приложимостта на успешно валидиран подпис/печат, следвайки свои Правила за приложимост (Signature applicability rules) или оценява приложимостта спрямо означената Политика на удостоверението.

На практика, правната приложимост на валидиран подпис/печат за конкретна бизнес-цел е изцяло в прерогативите на Потребителя/Доверяващата се страна. В отчета на валидиране се указва формата и профила на валидирания подпис, тоест функционалността, която се постига с този подпис/печат, а като следствие от това, и приложимостта му за конкретна бизнес-цел.

УСЛУГАТА се заплаща от Потребителя/Доверяващата се страна съгласно договорни условия с Доставчика за нейната доставка и ползване.

4.3 Управление на Политиката и Практиката

Практиката и Политиката на Доставчика 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.

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

4.4 Други документи относно УСЛУГАТА

Политиката и Практиката на Доставчика на УСЛУГАТА са по-скоро технически документи и специфицират техническите аспекти и характеристики на валидирането на е-подписи/печати. Тези документи са собственост на Доставчика и определят:

- Практиката – как Доставчикът оперира УСЛУГАТА;
- Политиката – наборът от ограничения, срещу които УСЛУГАТА определя техническата валидност на подпис/печата.

УСЛУГАТА проверява техническата валидност на подписа/печата, но не и и приложимостта на подписа/печата за определена бизнес-цел. Това изисква да бъдат документирани критерии относно бизнес аспектите на приложимост на е-подписа/печата, включително правните аспекти на приложимостта им. Тези критерии формират Правила за приложимост (Signature applicability rules), които определят дали подписът/печатът съответства на параметрите на определени бизнес-цели (Business Scoping Parameters/BSP), а именно:

- Параметри, отнасящи се до бизнес-приложения, които изискват е-подписи/печати;
- Параметри, зависещи от законови/нормативни разпоредби, свързани в контекста на осъществяване на бизнес-целите;
- Параметри, свързани с участниците в процесите на създаване и валидиране на е-подпис/печат;
- Др.

УСЛУГАТА (съгласно този документ) и Правилата за приложимост са два независими процеса:

- УСЛУГАТА (процесът на валидиране на подписа/печата) може да завърши със статус-индикатор ВАЛИДЕН, но да не отговаря на определени правила за приложимост,

както и

- Подписът/печатът може да съответства на определени Правила, но УСЛУГАТА връща статус-индикатор НЕОПРЕДЕЛЕН или НЕВАЛИДЕН.

Това изисква да бъдат документирани критерии относно бизнес аспектите на приложимост на е-подписа/печата, включително правните аспекти на приложимостта им.

Следва да има документ за Правила за приложимост на е-подпис/печат, които определят изисквания, разработени в контекста на параметрите на бизнес-целите (Business Scoping Parameters/BSP), а именно:

- Параметри, отнасящи се до бизнес-приложения, които изискват е-подписи/печати;
- Параметри, зависещи от законови/нормативни разпоредби, свързани в контекста на осъществяване на бизнес-целите;
- Параметри, свързани с участниците в процесите на създаване и валидиране на е-подпис/печати;
- Др.

Правилата относно правна приложимост на е-подписа/печата за бизнес-цели са извън обхвата на настоящия документ, следва да бъдат изготвени от Потребители/Доверяващи се страни на е-подпис/печат и са тяхна собственост. Тези правила могат да бъдат документирани или подготвени за автоматизирана проверка (например, на база Отчета на валидиране) след използване на УСЛУГАТА, преди окончателното приемане на е-подписа/печата от Доверяващата се страна за определените бизнес-цели.

5 КОНЦЕПТУАЛЕН МОДЕЛ НА ПРОЦЕСА НА ВАЛИДИРАНЕ

5.1 Участващи страни

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

- Доставчик на УСЛУГАТА в качеството му на ДКУУ, който оперира процеса на валидиране;
- Потребители (Доверяващи се страни);
- Косвени участници за процеса на валидиране:
  - Страни, които са подписали/подпечатели документ(и);
  - Външни ДКУУ (техните удостоверяващи органи – CA, TSA, CRL/OCSP);
  - Национален доверителен списък на регулативния орган КРС;
  - Националните Доверителни списъци (Trusted Lists) на страните-членки;
  - Европейски списък на националните Доверителни списъци (List of Trusted Lists).

5.2 Формати и профили на съответствие на КЕП/КЕПечат

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 с издадени за тях квалифицирани удостоверения, 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 за конкретни бизнес-цели:

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

(1) удостоверението в подкрепа на усъвършенстваният електронен подпис/печат е било валидно към момента на подписването/подпечатването, а когато усъвършенстваният електронен подпис/печат е подкрепен от квалифицирано удостоверение, това квалифицирано удостоверение е отговаряло към момента на 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 създателя на подписа/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;

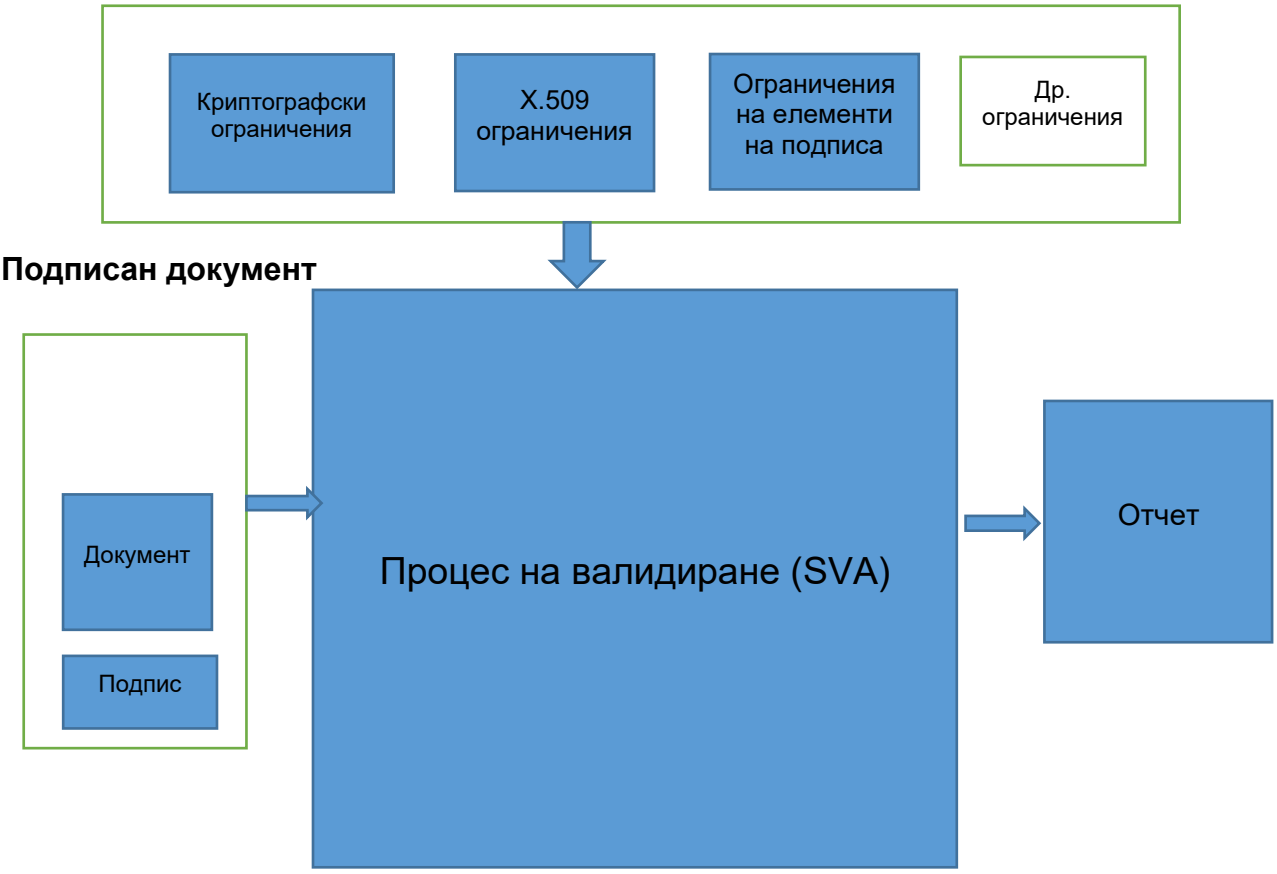
(7) изискванията по член 36 от Регламент (ЕС) № 910/2014 са били изпълнени към момента на подпечатването;

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

5.3 Модел на валидиране

5.3.1 Общи изисквания

Съгласно ETSI EN 319 102-1 концептуалният модел на валидиране на КЕП/КЕПечат или УЕП_КУ/УЕПечат_КУ е представен на Фиг. 1. Разделението в модела е условно, с цел по-точно позициониране на процеса на валидиране спрямо общите изисквания.



ФИГ. 1 КОНЦЕПТУАЛЕН МОДЕЛ НА ВАЛИДИРАНЕ

Компонент SVA в модела получава е-подписа/печата и съобразно Политиката за валидиране (набор/съвкупност от ограничения) го валидира и генерира статуса-индикатор и отчет от валидиране, който се интерпретира от Потребител (Доверяваща се страна) с оглед приложимостта на подписа/печата.

За да се валидира даден формат на подписа/печата, се изпълняват няколко съставящи подпроцеса в рамките на SVA (процеса за валидиране за избран формат/профил): проверка на формата на подписа/печата, проверка на КУ, проверка на криптографски характеристики, и т.н. Статус-индикаторът от всеки такъв единичен процес е ВАЛИДЕН (PASSED), НЕВАЛИДЕН (FAILED) или НЕОПРЕДЕЛЕН (INDETERMINATE) .

Статус-индикаторът, който SVA предоставя след валидиране на конкретния формат/профил спрямо Политиката на валидиране е:

- ВАЛИДЕН (TOTAL-PASSED) – проверките на всички криптографски характеристики/параметри на подписа/печата са успешни, както и тези в съответствие с Политиката (ограниченията); Потребителят/Доверяваща се страна приема подписа/печата за технически валиден, но това не означава, че е приложим за конкретната бизнес-цел;
- НЕВАЛИДЕН (TOTAL-FAILED) - проверките на всички криптографски характеристики/параметри на подписа/печата са неуспешни, или подписът/печатът е създаден след отмяна/прекратяване на КУ или форматът не съответства на някой от посочените в. 5.2 базови формати; Потребителят/Доверяваща се страна не приема подписа/печата за технически валиден;
- НЕОПРЕДЕЛЕН (INDETERMINATE) – резултатите от отделните/единични проверки не позволяват подписът/печатът да бъде оценен като ОБЩО-ВАЛИДЕН или ОБЩО-НЕВАЛИДЕН; приемането на подписа/печата е в прерогатива на Потребителя/Доверяваща се страна.

За всеки формат/профил на е-подпис/печат, SVA изпълнява логическа последователност от подпроцеси, съставящи следните процеси на валидиране:

- Процес на валидиране на Базов формат на подпис/печат (профил BASELINE_B) – SVA изпълнява този процес ако времето на валидиране е в периода на валидност на КУ и то не е отменено или времето на валидиране е извън периода на валидност на КУ и Удостоверяващият орган (CA) предоставя информация за отмяната/прекратяване;
- Процес на валидиране на подпис/печат с профил BASELINE_T и BASELINE_LT – SVA изпълнява процес на валидиране на базов подпис, на подпис/печат с удостоверено време (_T) и на подпис/печат с удостоверено време и статус за КУ (_LT);
- Процес на валидиране на подпис/печат с профил BASELINE_LTA - SVA изпълнява процес на валидиране на базов подпис/печат, на подпис/печат с удостоверено време (_T), на подпис/печат с удостоверено време и статус за КУ (_LT) и на подпис с архивен материал (_LTA).

5.3.2 Избор на процеса на валидиране

Потребител/Доверяваща се страна не може да определи избора на процеса на валидиране. SVA имплицитно/императивно следва посочената по-долу последователност на избор на процеса на валидиране:

(1) Ако подписът/печатът за валидиране е:
- с профил BASELINE_B – SVA изпълнява (4)
- с профил BASELINE_T и BASELINE_LT – SVA изпълнява (3)
- с профил BASELINE_LTA – SVA изпълнява (2)

(2) Ако SVA не поддържа валидиране на подпис/печат с профил BASELINE_LTA, SVA изпълнява (3); в противен случай, изпълнява процес на валидиране на подпис/печат с профил BASELINE_LTA и преминава към (5);

(3) Ако SVA не поддържа валидиране на подпис/печат с профил BASELINE_T и BASELINE_LT, SVA изпълнява (4); в противен случай, изпълнява процес на валидиране на подпис/печат с профил BASELINE_T и BASELINE_LT и преминава към (5);

(4) SVA изпълнява процес на валидиране на базов (формат) подпис/печат (профил BASELINE_B) и преминава към (5);

(5) Когато статусът на валидиране от избрания процес на валидиране е ВАЛИДЕН (PASSED), SVA връща статус-индикатор ОБЩО-ВАЛИДЕН (TOTAL-PASSED) и отчет от валидиране;

(6) Когато статусът на валидиране от избрания процес на валидиране е НЕВАЛИДЕН (FAILED), SVA връща статус-индикатор ОБЩО-НЕВАЛИДЕН (TOTAL-FAILED) и отчет от валидиране;

(7) При друг случай, SVA връща статус-индикатор НЕОПРЕДЕЛЕН (INDETERMINATE) и отчет от валидиране.

5.3.3 Статус-индикатори на валидиране и отчет от валидиране

Процесът на валидиране на подпис/печат завършва със:

- статус-индикатор на валидиране (ВАЛИДЕН, НЕВАЛИДЕН, НЕОПРЕДЕЛЕН);
- идентификатор на Политиката на валидиране (или описание на ограничения);
- дата и време на валидиране и данни за валидиране (на удостоверението на подписа/печата);
- избраният процес на валидиране (съгласно профила на подписа/печата);
- отчет от валидиране.

ДКУУ „БОРИКА“ АД имплементира представения по-горе концептуален модел на процеса на валидиране на е-подпис/печат като предоставя и поддържа УСЛУГАТА в съответствие с Регламент 910/2014, следвайки съдържащите се в този документ Практика и Политика.

6 УСЛУГА (B-Trust QSVS)

6.1 Функционален модел

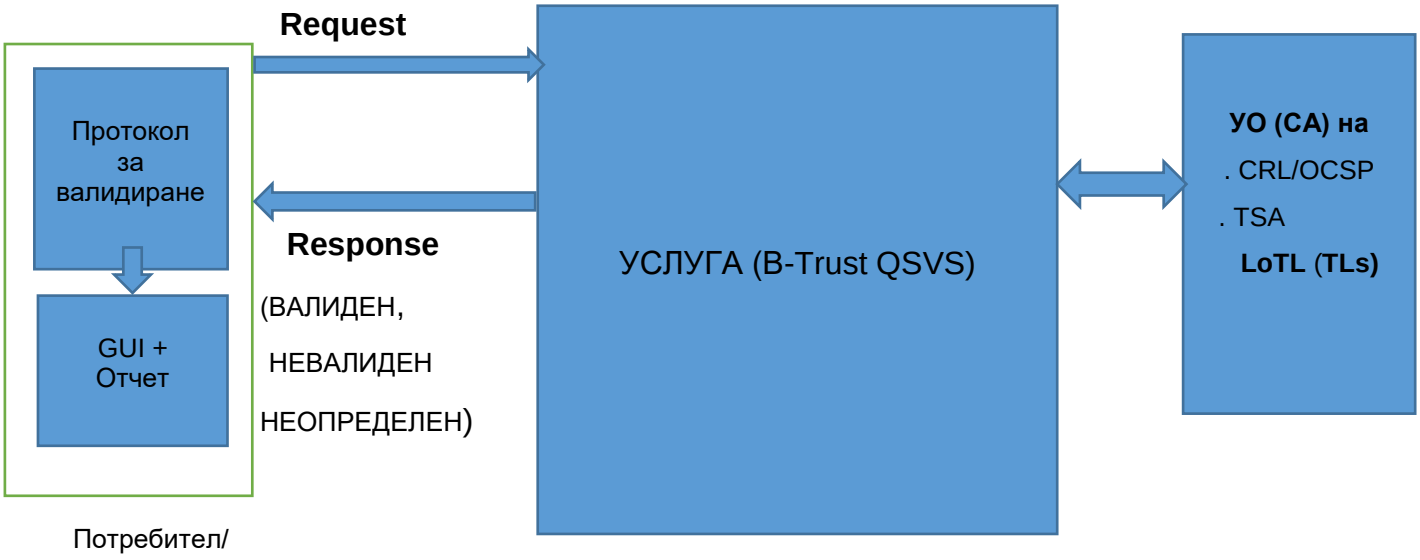
УСЛУГАТА (B-Trust Qualified Signature Validation Service/B-Trust QSVS) на Доставчика „БОРИКА“ АД включва следните софтуерни компоненти:

- Клиент за валидиране на подписа/печата (SVS_Client) – софтуерна компонента от страна на Потребителя. Може да бъде софтуерен клиент или уеб-браузърен -клиент с графичен интерфейс (GUI) със следната функционалност:
  - заявки за валидиране
  - протокол за валидиране
  - генерира и представя отчет на валидиране.
- Сървър за валидиране (SVS_Server) – уеб-сервиси от страна на Доставчика със следната функционалност:
  - протокола за валидиране
  - SVA (процеси и алгоритмите за валидиране на подписа/печата) съгласно ETSI EN 319 102-1 и ETSI TS 119 442
  - интерфейси към вътрешни и външни/косвени участници/страни за УСЛУГАТА – CRL/OCSP на Удостоверяващ(и) Орган(и), TSA, TL/LTL
  - генерира отчет (кратък или подробен) и статус-индикатор от валидиране на подписа/печата.

Комуникационният канал между клиента и SVS_Server е защитен (HTTPS/клиент-сървърна автентификация) и транспортира заявката за валидиране на подписа и отговора/резултата от валидирането. Комуникацията може да бъде синхронна или асинхронна.

Комуникационният канал между SVS_Server (УСЛУГАТА на ДУУ „БОРИКА“ АД) и „външни“ доставчици на удостоверителни услуги (CRL/OCSP, TSA, TL/LoTL) е извън обхвата на настоящия документ („външните“ доставчици определят типа на канала за комуникация).

На Фиг.2 е представен функционалния модел на УСЛУГАТА на Доставчика.



Фиг. 2 Функционален модел на УСЛУГАТА

6.2 Процес на валидиране

Заявките за валидиране на подпис/печат и отговорите на тези заявки ползват комуникационният канал между SVS_Client И SVS_Server. Обменът е защитен като се поддържа двустранна автентификация сървър-клиент. Протоколът за валидиране (заявки и отговори) съответства на техническата спецификация ETSI EN 119 442.

В съответствие с ETSI TS 319 172-1, УСЛУГАТА изпълнява процеса на валидиране в следните стъпки:

Стъпка 1: Клиентът SVS_Client генерира и изпраща заявка за валидиране, която съдържа подписания документ (ако подписът/печатът е опакован или опаковащ) или изпраща документ и подпис (при обособен подпис/печат);

Ограниченията за валидиране са имплицитно зададени чрез софтуера на УСЛУГАТА (в SVS_Server) и процесът на валидиране ги изпълнява съобразно профила на доставения в заявката подпис/печат.

Стъпка 2: Сървърът SVS_Server изпълнява валидиране на подписа/печата; изпълнението на тази стъпка (в съответствие с т. 5.3); изпълнението на тази стъпка предполага използване на допълнителни вътрешни удостоверителни услуги на Доставчика (B-Trust CRL/OCSP, B-Trust QTSA) или при необходимост, на други външни Доставчици.

Стъпка 3: Сървърът SVS_Server генерира, подготвя и изпраща отчет от валидирането в отговор на направената заявка за валидиране на подписа/печата; подробният отчет от валидиране съдържа статус-индикатор (ДА/НЕ) от валидирането на всяко ограничение и следствия от него, в зависимост от избрания процес на валидиране на УСЛУГАТА и следва техническата спецификация ETSI TS 119 102-2; отчетът от валидиране е подпечатан/удостоверен от УСЛУГАТА с КЕПечат (профил BASELINE_LT). Генерира се по един отчет за валидиране за всеки подпис/печат на документа.

Стъпка 4: Представя се отчета от валидиране; уеб-клиентът визуализира отчета от валидиране в подходящ вид (в pdf-формат) и може да бъде разпечатен. На базата на отчета от валидиране, Потребителят/Доверяващата се страна приема или отхвърля техническата валидност на подписа/печата.

УСЛУГАТА изпълнява следните процеси на валидиране в зависимост от профила на представения подпис/печат:

- Процес на валидиране на подпис/печат с профил BASELINE_B;
- Процес на валидиране на времеви печат;
- Процес на валидиране на подпис/печат с профил BASELINE_T и BASELINE_LT; този процес е общ/един за двата профила;
- Процес на валидиране на подпис/печат с профил BASELINE_LTA.

Изборът на процеса на валидиране на УСЛУГАТА следва указанията в т. 5.3.2 на концептуалния модел и избрания процес изпълнява горепосочените стъпки, включващи базови функционални процедури (подпроцеси), чрез които се изграждат логическата последователност от проверки в рамките на процеса на валидиране на подписа/печата.

6.3 Базови процедури (подпроцеси)

Следва кратко описание на съставящите процедури (подпроцеси) в рамките на избрания процес на валидиране за всеки поддържан от УСЛУГАТА формат/профил следва по-долу.

6.3.1 Проверка на формат (Format Checking)

В случай, че подписът/печатът е в съответствие с приложимия базов формат, резултатът от тази проверка е ВАЛИДЕН. В противен случай резултатът от проверката е НЕУСПЕШЕН.

6.3.2 Определяне на удостоверението на подписа/печата (Identification of signing certificate)

В случай, че удостоверението се определи успешно, изходът от тази проверка е удостоверението на подписа/печата. В случай, че удостоверението за подписване не може да бъде определено, изходът е със статус-индикация НЕОПРЕДЕЛЕН (INDETERMINATE) и под статус NO_SIGNING_CERTIFICATE_FOUND.

Този подпроцес завършва само със статус INDETERMINATE ако удостоверението не се съдържа в подписа/печата и не може да бъде извлечено от външен източник, посочен от референтния номер на подписа/печата.

6.3.3 Инициализация на ограниченията (Validation context initialization)

Този подпроцес инициализира ограниченията за валидиране (имплицитно заложени в софтуера), които се използват за потвърждаване на подписа/печата. В случай на неуспешна инициализация, подпроцесът завършва със статус-индикатор НЕОПРЕДЕЛЕН (INDETERMINATE) заедно с подиндикатор POLICY_PROCESSING_ERROR или SIGNATURE_POLICY_NOT_AVAILABLE. В противен случай статусът-индикатор е УСПЕШЕН (PASSED) с набора ограничения, които се ползват в хода на валидирането на подписа/печата.

6.3.4 Проверка на актуалност на статуса на отмяна (Revocation freshness checker)

Този подпроцес проверява дали дадена статус-информация за отмяна/прекратяване е актуална към момента на валидиране. Процесът се използва от други подпроцеси за проверката на отмяна на удостоверението.

6.3.5 Валидиране на X.509 удостоверение (X.509 certificate validation)

Този подпроцес верифицира удостоверението за подписа/печата в момента на валидиране. Верифицирането се извършва към текущото време за УСЛУГАТА. При успешно верификация, изходът от подпроцеса е УСПЕШЕН, в противен случай – НЕОПРЕДЕЛЕН с указан брой подиндикатори (ДА/НЕ).

6.3.6 Криптографска верификация (Cryptographic verification)

Проверява се целостта на подписаните данни, чрез извършване на криптографски проверки. При успешна проверка изходът от подпроцеса е УСПЕШЕН, в противен случай – НЕУСПЕШЕН с подиндикатор HASH_FAILURE или SIG_CRYPTO_FAILURE, или НЕОПРЕДЕЛЕН с подиндикатор SIGNED_DATA_NOT_FOUND.

6.3.7 Приложимост на подписа/печата (Signature acceptance validation)

Този подпроцес обхваща допълнителна проверка, която се извършва върху самия подпис/печат или върху характеристиките на подписа/печата. При успешна проверка на подписа/печата за съответствие с утвърдените ограничения, изходът е УСПЕШЕН, в противен случай – НЕОПРЕДЕЛЕН с подиндикатори IG_CONSTRAINTS_FAILURE или CRYPTO_CONSTRAINTS_FAILURE_NO_POE.

6.3.8 Представяне на валидността на подписа/печата (Signature validation presentation)

Този подпроцес представя на Потребителя (Доверяваща се страна) резултатите от цялостния процес на валидиране - общ статус-индикатор на валидиране на подписа/печата - ВАЛИДЕН, НЕВАЛИДЕН или НЕОПРЕДЕЛЕН, както и отчета от валидиране.

6.4 Статус-индикатори и отчет на валидиране

УСЛУГАТА завършва със статус-индикатор, както следва:

- ВАЛИДЕН – криптографските проверки за подписа/печата (включително всички хеш-стойности) са успешни, както са успешни и всички проверки срещу ограниченията, имплицитни (директни) за УСЛУГАТА (съгласно тази Политика);
- НЕВАЛИДЕН – криптографските проверки за подписа/печата (включително всички хеш-стойности) са неуспешни, или генерирането на подписа/печата е след отмяната/прекратяване на удостоверението на подписа/печата, или подписът/печатът не отговаря на един от допустимите формати/профили за УСЛУГАТА;
- НЕОПРЕДЕЛЕН – резултатът от проверката не позволява УСЛУГАТА да удостовери, че подписът/печатът ВАЛИДЕН или НЕВАЛИДЕН.

Статус-индикаторът се придружава от допълнителна информация, която се съдържа в:

- Кратък отчет на процеса на валидиране (заявява се чрез опция „ПРОВЕРКА“ на УСЛУГАТА);
- Подробен отчет на процеса на валидиране (заявява се чрез опция „ПОДРОБНА ПРОВЕРКА“ на УСЛУГАТА).

Краткият отчет на валидиране, за всеки валидиран подпис/печат включва:

- Политиката на валидиране (по-подразбиране, общо описание);
- Статус-индикатора;
- Идентификатор на подписа;
- дата и време на създаване на подписа/печата;
- формата/профила на валидирания подпис/печат (т.е., избрания процес на валидиране);
- Титуляря/Създателя на подписа/печата;
- Обхвата на подписа/печата;
- Информация за подписания/подпечатан документ (име, брой подписи).

Подробният отчет включва пълна информация за проверка на всички ограничения съгласно Политиката относно атрибути/характеристики на обектите в структурата на подписа/печата (според неговия формат/профил).

Двата вида отчети на валидиране се предоставят на софтуерния клиент или чрез уеб-клиента в браузера на Потребител/Доверяваща се страна в PDF-формат. И двата отчета са подпечатани/удостоверени чрез квалифицирано удостоверение за КЕПечат на УСЛУГАТА, удостоверяващ техния произход, ненарушимост на данните в тях и времето на поставяне на печата (т.е., времето на валидиране).

6.5 Интерфейси и протокол на валидиране

Доставчикът оперира и поддържа УСЛУГАТА чрез набор от уеб-сервиси, които се достъпват чрез:

- OASIS DSS интерфейс;

- GUI интерфейс.

И двата интерфейса използват защитен комуникационен/транспортен канал, поддържащ двустранна автентификация сървър-клиент заУСЛУГАТА.

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

Потребител/Доверяваще се страна се автентифицира пред УСЛУГАТА със съответно за тях квалифицирано удостоверение издадено от ДККУ „БОРИКА“ АД.

6.5.1 OASIS DSS интерфейс

SVS_Client достъпва УСЛУГАТА чрез OASIS DSS Интерфейс, който дефинира набор от XML-команди за двата протокола на УСЛУГАТА:

- Протокол за подписване/подпечатване на документ с КЕП/КЕПечат;
- Протокол за валидиране на подписан/ подпечатан документ.

Двата протокола на OASIS DSS интерфейса използват за транспорт SOAP-протокол, който пренася XML-командите за подписване/подпечатване, респективно за валидиране на подписа/печата.

6.5.2 GUI интерфейс

УСЛУГАТА се достъпва/ползва от Потребителя/Доверяваща се страна посредством уеб-клиент, което работи с неговия браузър и ползва графичен интерфейс. Посредством него Доверяваща се страна зарежда файл, избира параметри на заявката, зарежда подписан/ подпечатан документ за валидиране на подписа/печата, след което уеб-клиента в браузъра изпраща XML-команда (Request/Response) към сървърната компонента на УСЛУГАТА.

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

6.6 Външни източници на удостоверения

В определени случаи, УСЛУГАТА изисква достъп до външни източници на удостоверения, свързани с процеса на валидиране на подписа/печата към подписан/подпечатан документ. Такива външни (косвени) участници във валидиращия процес са:

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

УСЛУГАТА използва стандартизирани програмни интерфейси за достъп до тези външни източници на квалифицирани удостоверения, които верифицира при изпълнение на процеса на валидиране на КЕП/КЕПечат и/или УЕП/УЕПечат_КУ.

LoTL се публикува от Европейската Комисия (ЕК/EC) на адрес: https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-mp.xml .

Този XML-файл съдържа Доверителните списъци на страните членки, включително и националния доверителен списък. Информацията за това кой подписва и публикува LoTL се намира на адрес http://eur-lex.europa.eu/legal-content/BG/TXT/PDF/?uri=CELEX:52015XC1224(01)&from=EN .

Форматът на подписа на LoTL и на националните TL е XAdES BASELINE_B. УСЛУГАТА се доверява на LoTL като верифицира подписа чрез удостоверението, публикувано на горепосочения адрес.

7 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/съответни 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).

8 ПРАКТИКА

Посочените в този документ процедури, механизми по контрол и технически характеристики на B-Trust УСЛУГАТА са допълнение към тези части на 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.

Практиката на Доставчика при предоставяне на УСЛУГАТА се осъществява от обекта B-Trust Qualified Signature Validation Service (B-Trust QSVS) обозначен с идентификатор 1.3.6.1.4.1.15862.1.6.6 в B-Trust инфраструктурата съгласно документа B-Trust CPS-eIDAS:

Квалифицирана УСЛУГА за валидиране на квалифициран електронен подпис/печат (B-Trust QSVS)	Идентификатор
Практика на Доставчика на УСЛУГАТА	**1.3.6.1.4.1.15862.1.6.6**

Тази Практика е в основата на оперативната работа на Доставчика на УСЛУГАТА и обслужва съдържащата се в този документ Политика с посочените по-долу идентификатори:

УСЛУГАТА (B-Trust QSVS)	Идентификатор(и)
Политика на УСЛУГАТА	**1.3.6.1.4.1.15862.1.6.6.1** **0.4.0.19441.1.1** **0.4.0.19441.1.2**

Доставчикът поддържа тази Политика при следните условия:

- прилага се едновременно за валидиране на КЕП/КЕПечат и на УЕП_КУ/УЕПечат_КУ;
- позволява на Потребителя/Доверяваща се страна да оценява приложимостта на технически валидния подпис/печат за конкретната бизнес-цел;
- текущата версия подлежи на промяна и се преустановява използването на предишната версия;
- отчетът на валидация сочи политиката;
- предишни версии са достъпни за Потребители/Доверяващи се страни.

8.1 Служебни удостоверения на УСЛУГАТА

УСЛУГАТА има две публични удостоверения:

- квалифицирано удостоверение за квалифициран електронен печат;
- квалифицирано удостоверение за автентичност на уеб-сайт (организация).

Удостоверението за е-печат на B-Trust QSVS е квалифицирано удостоверение за електронен печат и е електронно подпечатано с частния ключ на Оперативния удостоверяващ орган B-Trust Operational Qualified CA на Доставчика. С частния ключ на УСЛУГАТА, съответстващ на публичния такъв в това удостоверение, Доставчикът електронно подпечатва отчета от валидиране на подписа/печата, който се предоставя на Потребител/Доверяваща се страна.

Това удостоверение автентифицира УСЛУГАТА като източник на генерирания статус-индикатор и отчет от валидиране на електронно подписан/подпечатан документ и утвърждава целостта на данните в отчета от процеса на валидирането.

Удостоверението за уеб-сайт на B-Trust QSVS е квалифицирано удостоверение за уеб-сайт и е електронно подпечатано с частния ключ на Оперативния удостоверяващ орган B-Trust Operational Advanced CA на Доставчика. Това удостоверение онлайн автентифицира УСЛУГАТА пред Потребителя и обслужва защитена SSL/TLS сесия с Потребителя.

Профилът на квалифицираното удостоверение за квалифициран е-печат на УСЛУГАТА е съгласно документа „Политика при представяне на квалифицирани удостоверения за квалифициран подпис и печат (B-Trust QCP-eIDAS QES/CQES/QESeal) на „БОРИКА“ АД и е посочен по-долу:

Поле	Атрибути	Значение/Стойност
Version	-	V3
Serial number	-	67 93 0c 9b 53 f1 2c 8b
Signature algorithm	-	Sha256RSA
Signature hash algorithm	-	Sha256
Issuer	CN =	B-Trust Operational Qualified CA
	OU =	B-Trust
	O =	BORICA AD
	OrganizationIdentifier(2.5.4.97) =	NTRBG-201230426
	C =	BG
Validity from	-	2018-05-11T10:48:56Z
Validity to	-	2024-05-11T10:48:56Z
Subject	CN =	B-Trust Qualified Signature Validation Service
	OU =	B-Trust
	O =	BORICA AD
	OrganizationIdentifier(2.5.4.97) =	NTRBG-201230426
	C =	BG
Public key	-	RSA(2048 Bits)
Subject Key Identifier		fd 1b 8e f2 76 d4 b1 ab b1 c1 94 62 be 84 c6 f7 ea cf a1 7b
Authority Key Identifier	KeyID =	27 cf 08 43 04 f0 c5 83 37 67 81 17 4d fc 05 e6 db 65 8b b0
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=1.3.6.1.4.1.15862.1.6.1.3 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.b-trust.org/documents/cps [2]Certificate Policy Policy Identifier=1.3.6.1.4.1.15862.1.6.6.1 [3]Certificate Policy Policy Identifier=0.4.0.19441.1.1 [4]Certificate Policy Policy Identifier=0.4.0.19441.1.2 [5]Certificate Policy: Policy Identifier=0.4.0.1456.1.1 [6]Certificate Policy: Policy Identifier=0.4.0.194112.1.3
CRL Distribution Points	-	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.b-trust.org/repository/B-TrustOperationalQCA.crl
Authority Information Access	-	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name:

		URL=http://ocsp.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-TrustOperationalQCA.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-QcCompliance (QcSSCD) (oid=0.4.0.1862.1.4)	
		id-etsi-qcs-QcType (oid=0.4.0.1862.1.6)	id-etsi-qct-eseal (oid=0.4.0.1862.1.6.2)
		id-etsi-qcs-QcPDS (oid=0.4.0.1862.1.5)	PdsLocations PdsLocation=https://www.b-trust.org/documents/pds/pds_en.pdf language=en
Thumbprint (Sha1)		b4 f5 00 6c 27 8e fb ec 67 4b 44 b5 d4 3a 82 e6 31 a9 42 a3	
Thumbprint (Sha256)		da 4c 80 0c 0e 21 11 5f 85 e4 5c 51 22 f1 dd 7f b6 a8 40 5b c9 be 48 8c 50 b0 54 c4 4d 47 46 44	

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 QWAC) на „БОРИКА“ АД и е посочен по-долу:

Поле	Атрибути	Значение/Стойност
Version	-	V3
Serial number	-	29 b9 2a 53
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	-	2019-02-27T11:37:27Z
Validity to	-	2021-06-01T12:37:27Z
Subject	CN =	qsvs.b-trust.org
	O =	Borica AD
	2.5.4.97= (organizationIdentifier)	NTRBG-201230426
	OU=	OV SSL
	L=	Sofia
	C =	BG
Public key	-	RSA(2048 bits)
SubjectAlternativeName		DNS Name=qsvs.b-trust.org RFC822 Name=support@borica.bg
Subject Key Identifier	-	b8 09 80 0c 5a 78 5e 48 ff 5a 08 cc ec 7f 87 fa 5d 98 4f 1e
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=1.3.6.1.4.1.15862.1.6.6.1 [3]Certificate Policy Policy Identifier=0.4.0.19441.1.1 [4]Certificate Policy Policy Identifier=0.4.0.19441.1.2[5] Certificate Policy: Policy Identifier=2.23.140.1.2.2 [6] Certificate Policy: Policy Identifier=0.4.0.2042.1.7 [7] 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/qsvs_pds_en.pdf language=en
Thumbprint (Sha1)		d9 0a 02 a2 87 40 87 93 a9 b2 68 38 87 3a d1 b9 0f 80 86 84	
Thumbprint (Sha256)		6b 1d f3 a6 71 5f 69 b2 cc 4f 95 69 c2 03 c9 7c 4f cb d8 07 b5 ae 52 47 62 4b 1f 95 a4 76 3d d2	

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

Наименование	**Алгоритъм**
Хеш-алгоритми:	SHA 256
Асиметрични алгоритми:	RSA

8.2 Управление и опериране на УСЛУГАТА

8.2.1 Вътрешна организация при Доставчика

„БОРИКА“ АД, регистриран ДКУУ по смисъла на Регламент 910/2014 и Закона за електронния документ и електронните удостоверителни 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.

8.2.2 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)“ (виж т. 5.2 и 5.3).

8.2.3 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.

8.2.4 Управление на достъп

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.

8.2.5 Криптографска сигурност – управление на ключове

8.2.5.1 Генериране на двойката ключове

Двойката RSA ключове към удостоверението за квалифициран печат на УСЛУГАТА се генерира в HSM-среда с най-висока степен на сигурност от персонал на Доставчика, който има право да изпълнява тази роля. Генерираната двойка RSA ключове е с дължина 2048 бита.

Двойката RSA ключове към удостоверението за автентичност на уебсайт 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. Генерираната двойка RSA ключове е с дължина 2048 бита.

Процедурите и средата за генериране на тези двойка ключове е в съответствие с документи B-Trust CPS-eIDAS. Описанието и ролята на персонала на Доставчика, изпълняващ процедурите по генетиране на двойките ключове са посочени в същия документ.

8.2.5.2 Защита на частен ключ

Генерираният частен ключ за печат на УСЛУГАТА се съхранява върху HSM (QSCD).

Генерираният частен ключ за автентичност на уебсайт 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 (срив на сървър, изтриване на ключа, др.).

8.2.5.3 Разпространение на публичния ключ

Публичният ключ на УСЛУГАТА за печат е удостоверен чрез удостоверение за квалифициран печат, издадено от УО B-Trust Operational Qualified CA в PKI-йерархията на B-Trust.

Публичният ключ на УСЛУГАТА за SSL е удостоверен чрез удостоверение за автентичност на уебсайт, издадено от УО B-Trust Operational Advanced CA в PKI-йерархията на B-Trust.

Тези удостоверения с публичен ключ са заредени в платформата на УСЛУГАТА и служат за:

- подпечатване на генерирания от УСЛУГАТА отчет от валидиране на подпис/печат;
- автентификация на УСЛУГАТА (QSVS_Server) пред Потребителите/Доверяващи се страни, които я използват.

Допълнително, Доставчикът публикува удостоверенията на УСЛУГАТА на интернет страница на сайта си. Потребител/Доверяваща се страна може свободно да го достави на свой компютър/система, ако това е необходимо.

За да автентифицира УСЛУГАТА, Потребител/Доверяваща се страна следва да е заредил на своя компютър/система оперативните удостоверения на УО B-Trust Operational Qualified CA и B-Trust Operational Advanced CA (част от удостоверителните вериги на B-Trust, също публикувани на страница на сайта на Доставчика).

8.2.5.4 Продължаване на срока и/или преиздаване на удостоверението

Периодът на валидност на удостоверението на УСЛУГАТА е 5 години. След изтичане на този период, срокът на валидност на удостоверението се продължава за период от 1 година. След този период се генерира нова двойка ключове, частният ключ от която се съхранява в HSM, съответно в нов криптографски файл PKCS#12, а публичният ключ се удостоверява, чрез издаване на ново удостоверение на УСЛУГАТА. Двойките ключове с изтекъл период на валидност се съхраняват, както следва:

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

8.2.6 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.

8.2.7 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).

8.2.8 Мрежова сигурност

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

8.2.9 Управление на инциденти

Съгласно общата политика за сигурност на „БОРИКА“ АД.

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

8.2.10 Архив

Съгласно документа „Практика при предоставяне на квалифицирани удостоверения и удостоверителни услуги за тях от „БОРИКА“ АД (B-Trust CPS-eIDAS)“ (т. 5.5).

8.2.11 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.

8.2.12 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).

8.3 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).

Подписани/подпечатени е-документи с КЕП/КЕПечат 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.

9 ПОЛИТИКА

Политиката на Доставчика относно УСЛУГАТА дефинира набор от ограничения спрямо избрания процес на валидиране на КЕП/КЕПечати и на УЕП_КУ/УЕПечати_КУ.

УСЛУГАТА следва Политика на валидиране по подразбиране, т.е. ограниченията при валидиране са имплицитно дефинирани в нейния софтуер (конфигурационен файл, XML-файлове).

9.1 Общи принципи

(1) Политиката е обща за КЕП/КЕПечат и УЕП_КУ/УЕПечат_КУ и определя правилата (ограниченията) на валидиране на допустимите за УСЛУГАТА формати/профили.

(2) Тези правила важат също за съответстващите на Регламент 910/2014 усъвършенствани електронни подписи/печати.

(3) Наборът от ограничения за валидиране е комбинация от общите ограничения за УСЛУГАТА и имплицитно определените ограничения от нейните базови компоненти, включително:

- правилата за валидиране, съгласно стандартите/спецификациите за формати/профили на поддържаните подписи/печати;
- правилата за валидиране, съгласно функционалните характеристики на софтуера (софтуерни библиотеки) на УСЛУГАТА, т.е. налаганите ограничения от използвания софтуер (библиотеки).

(4) Квалифицирано валидиране на УЕП/УЕПечати с публично удостоверение (неквалифицирано) не дава положителен резултат от валидирането (резултатът е НЕВАЛИДЕН или НЕОПРЕДЕЛЕН).

9.2 Формати и профили на подписа/печата

В съответствие с изпълнение на РЕШЕНИЕ ЗА ИЗПЪЛНЕНИЕ (ЕС) 2015/1506 на Комисията (виж т. на документа) УСЛУГАТА валидира следните формати и профили на КЕП/КЕПечат и УЕП_КУ/УЕПечат_КУ:

Формат/ Профил	**BASELINE_B**	**BASELINE_T**	**BASELINE_LT**	**BASELINE_LTA**	**Бележка**
CAdES	Валидира се	Валидира се	Валидира се	Валидира се	TS 103 173
XAdES	Валидира се	Валидира се	Валидира се	Валидира се	TS 103 171
PAdES	Валидира	Валидира	Валидира	Валидира	TS 103 172
ASiCS/ ASiCE (*)	Валидира се	Валидира се	Валидира се	Валидира се	TS 103 174

(*) УСЛУГАТА валидира този формат и профилите за него в допълнение към изпълнение на РЕШЕНИЕТО с оглед на функционална пълнота.

Приложение 1 на документа представя структурите на профилите на е-подписи/печати, които УСЛУГАТА валидира.

9.3 Типове подписи/печати

За посочените по-горе формати и профили, УСЛУГАТА валидира следните типове квалифицирани подписи/печати, според тяхното разположение относно подписаните/подпечатени данни:

Тип/Формат	**CAdES**	**XAdES**	**PAdES**	**ASiCS**	**ASiCE**

Опакован (Enveloped)	NA(*)	Валидира .xml формат	Валидира .pdf формат	Валидира .asics формат	Валидира .asice формат
Опаковащ (Enveloping)	Валидира .p7m формат	Валидира .xml формат	NA(*)	Валидира .asics формат	Валидира .asice формат
Обособен (Detached)	Валидира .p7s формат	Валидира .xml формат	NA(*)	Валидира .asics формат	Валидира .asice формат

(*) Неприложим (NA)

9.4 Условия за валидиране на квалифицирани подписи/печати

В съответствие с чл. 32 на Регламент 910/2014, УСЛУГАТА потвърждава валидността на КЕП/КЕПечат и на УЕП_КУ/УЕПечат_КУ при следните условия:

- удостоверението в подкрепа на подписа/печата към момента на подписването/подпечатването е било квалифицирано удостоверение за електронен подпис/печат;
- квалифицираното удостоверение е издадено от доставчик на квалифицирани удостоверителни услуги и е било валидно към момента на подписването;
- данните за валидиране на подписа/печата съответстват на данните, предоставени от доверяващата се страна;
- уникалният набор от данни, представляващи Титуляря или Създателя от удостоверението, е надлежно предаден на Доверяващата се страна;
- ако към момента на подписването/подпечатването е бил използван псевдоним, то това е ясно указано на Доверяващата се страна;
- квалифицираният електронен подпис/печат е създаден от устройство за създаване на квалифициран електронен подпис/печат;
- целостта на подписаните данни не е застрашена;
- изискванията по чл. 26 на Регламента са били изпълнени към момента на подписването.

9.5 Ограничения при валидиране

Ограниченията при валидиране на подписа/печата адресират атрибути и характеристики на обектите, съдържащи се в структурата на валидирания подпис/печат, който Потребител/Доверяваща се страна представя на УСЛУГАТА.

Следните общи групи на ограничения са приложими за УСЛУГАТА:

- Относно удостоверенията, участващи в процеса на валидиране;
- Относно криптографските характеристики на подписа/печата;
- Относно елементите на подписа/печата.

9.5.1 Общи ограничения за валидиране

- Статус-индикаторът от валидацията, връщан от УСЛУГАТА определя само дали даден подпис е технически валиден съгласно Политиката за валидиране в този документ. Тази Политика може да не е подходяща за подписи/печати, създадени на други територии (от страни-членки).
- Резултатът от УСЛУГАТА съдържа статус-индикатори от валидирането на всички подписи в контейнера на подписа (при обособен (detached) подпис) или на всички подписи в контейнера на подписан документ (при опаковани или опаковащи подписи).
- Следователно, в случай на множество обособени/опаковани/опаковащи подписи, крайният резултат от валидирането на подписан/подпечатен документ с множество от подписи, не е определен;
- Максимален размер на подписан/подпечатен файл с данни – 10 Мегабайта.

9.5.2 Ограничения към формати

УСЛУГАТА валидира КЕП/КЕПечати и УЕП/УЕПечати във формат XML (XAdES), CMS (CAdES) или PDF (PAdES), профили _B, _T или _LT, които се поддържат чрез квалифицирани удостоверения съгласно РЕШЕНИЕ 2015/1506 на ЕК. В допълнение, УСЛУГАТА валидира подписи/печати с профил _LTA и универсален контейнер на подпис/печат в zip-формат (ASiCS/E).

9.5.3 Ограничения към профил и нива на съвместимост

Съгласно т. 4.2 на този документ.

9.5.4 Ограничения за типа на подпис/печат

Съгласно т. 4.3 на този документ.

9.5.5 Ограничение за софтуера (софтуерна библиотека)

УСЛУГАТА безусловно изпълнява ограниченията, наложени от базовата софтуерна библиотека, която тя използва:

- OASIS DSS.

9.5.6 Ограничения за X.509 удостоверение

УСЛУГАТА безусловно изпълнява ограниченията, наложени от профила на X.509 v.3 квалифицирани удостоверения за КЕП/КЕПечат, за УЕП/УЕПечат съгласно техническите и стандарти ETSI EN 319 412-1/5, както следва:

- За квалифицирани удостоверения за КЕП/КЕПечат:

Атрибут в удостоверение X.509 v.3	**Стойност на атрибут**
КЕП/КЕПечат – Physical/Legal Person	
Key Usage (critical)	*Non-Repudiation*
Qualified Statement:	
id-qcs-pkixQCSyntax- v2	*oid=1.3.6.1.5.5.7.11.2*
id-etsi-qcs-semanticsId-Natural или	*oid=0.4.0.194121.1.0*
(id-etsi-qcs-semanticsId-Legal)	*(oid=0.4.0.194121.1.2)*
id-etsi-qcs-QcCompliance (QcSSCD)	*oid=0.4.0.1862.1.4*
id-etsi-qcs-QcType	*oid=0.4.0.1862.1.6*
id-etsi-qct-esign или	*oid=0.4.0.1862.1.6.1*
(id-etsi-qct-eseal)	*(oid=0.4.0.1862.1.6.2)*

- За квалифицирани удостоверения за УЕП/УЕПечат:

Атрибут в удостоверение X.509 v.3	**Стойност на атрибут**
УЕП/УЕПечат – Physical/Legal Person	
Key Usage (critical)	*Non-Repudiation*
Qualified Statement:	
id-qcs-pkixQCSyntax- v2	*oid=1.3.6.1.5.5.7.11.2*
id-etsi-qcs-semanticsId-Natural или	*oid=0.4.0.194121.1.0*
(id-etsi-qcs-semanticsId-Legal)	*(oid=0.4.0.194121.1.2)*

id-etsi-qcs-QcCompliance	*oid=0.4.0.1862.1.1*
id-etsi-qcs-QcType	*oid=0.4.0.1862.1.6*
id-etsi-qct-esign или	*oid=0.4.0.1862.1.6.1*
(id-etsi-qct-eseal)	*(oid=0.4.0.1862.1.6.2)*

9.5.7 Криптографски ограничения

Криптографските ограниченията за УСЛУГАТА относно криптографските алгоритми и хеш-функция са както следва (съгласно ETSI TS 119 312):

- Криптографски алгоритми за подписване – RSA2048, RSA4096, ECC;
- Хеш-алгоритъм – SHA1, SHA256, SHA512.

При всички случаи, дължината на ключ RSA трябва да бъде най-малко 1024 бита, а дължината на ключа ECC - най-малко 192 бита.

9.5.8 Ограничения към елементи на подпис/печат

Няма.

9.5.9 Ограничения за обхват на УО (CA)

Подписът/печатът съдържа удостоверението на подписа/печата със референция(и) към оперативното, респективно базово удостоверение на УО (CA), необходими да се изгради верификационния път за процеса на валидиране. Това важи за удостоверението на Титуляря/Създателя и за удостоверенията на ДКУУ, които публикуват данни за статуса на удостоверенията (CRL/OCSP), референтни към процеса на валидиране.

9.5.10 Ограничения за статус на удостоверение

Подписът/печатът, който се валидира от УСЛУГАТА трябва да съдържа доказателство, което утвърждава валидността на удостоверението към момента на подписване/подпечатване.

Статусът за валидност на удостоверението на подписа/печата трябва да бъде под формата на OCSP-потвърждение от страна УО, издал това удостоверение.

Процесът на валидиране на УСЛУГАТА не изисква допълнителни данни за прекратяване на удостоверение, различни от данните (OCSP статуса), които първоначално са били включени в подписа/печата.

Проверка за прекратяване на удостоверения, приети за база на доверие (например, на Оперативен или Базов УО (CA)) се изпълнява въз основа на данните в TL/Trust Lists.

9.5.11 Ограничения за актуалност на удостоверения

За подпис/печат с профил BASELINE_T или BASELINE_LT: Актуалността на данните за прекратяване (т.е., OSCP-статусът за удостоверение) се проверяват съгласно следните правила:

- Данните за отмяна (OCSP-статусът) трябва да бъдат издадени след времето за генериране на времевия печат на подписа/печата.

9.5.12 Ограничения за доверено време

Достоверното време на подписване/подпечатване (най-близкото време до момента на генерация на подписа), в което може да се вярва (доказано от Proof-of-Existence/POE в подписа), че подписът/печатът е съществувал, се определя така:

- За подпис/печат с времеви печат (профил BASELINE_T, BASELINE_LT или BASELINE_LTA) – това е стойността в полето genTime на най-ранния валиден времеви печат в подписа/печата;

- За базов подпис (профил BASELINE_B) – довереното/вярно време на подписване/подпечатване не може да бъде определено, понеже липсва Proof-of-Existence/POE за подписа/печата.

10 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)“.

11 СЪОТВЕТСТВИЕ С РЕГЛАМЕНТ 910/2014 (чл.32 и 33)

Приведената по-долу Таблица представя съответствието на квалифицираната УСЛУГА (B-Trust QSVS) за квалифицирано валидиране на квалифицирани електронни подписи/печати (КЕП/КЕПечат) и на усъвършенствани електронни подписи съпроводени с квалифицирани удостоверения (УЕП_КУ/УЕПечат_КУ):

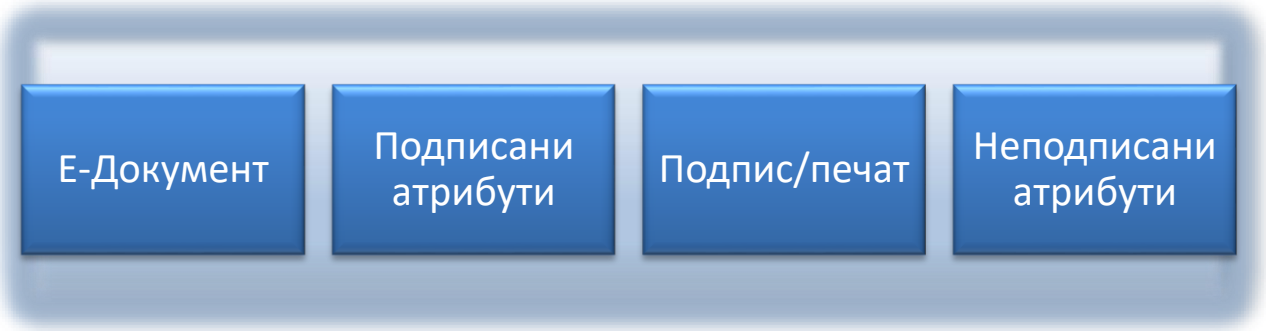
Изисквания по чл. 32	**Изпълнение от УСЛУГАТА**	**Бележки**
а) удостоверението в подкрепа на подписа към момента на подписването е било квалифицирано удостоверение за електронен подпис, отговарящо на Приложение I	Валидира профили на КУ съгласно B-Trust Политики за КЕП/КЕПечат и УЕП/УЕПечат на ДКУУ „БОРИКА“ АД	ETSI EN 319 412-1/5
б) квалифицираното удостоверение е издадено от доставчик на квалифицирани удостоверителни услуги и е било валидно към момента на подписването	КУ се верифицира следвайки верификационна верига, която започва от доверен източник (CA), включен в национален TL	Решение 1505/2015 за TL
в) данните за валидиране на подписа съответстват на данните, предоставени от доверяващата се страна	Процесът на валидиране предоставя на Потребителя/Доверяваща се страна отчет, включващ удостоверението на Титуляря/Създател, съдържащи данните за валидиране (публичен ключ, др.)	Виж Отчет на валидиране в Ръководство за работа с DSS
г) уникалният набор от данни, представляващи Титуляря/Създателя на електронния подпис/печат в удостоверението, е	Виж в)	Виж Отчет от валидиране в „Ръководство за работа с DSS“

надлежно предаден на доверяващата се страна		
д) ако към момента на подписването е бил използван псевдоним, то това е ясно указано на доверяващата се страна	Виж в)	
е) електронният подпис/печат е създаден от устройство за създаване на квалифициран електронен подпис/печат	Задължително ограничение за КЕП/КЕПечат е изискването за използване на QSSCD; за УЕП/УЕПечат това изискване отпада. Удостоверението на подписа/печата съдържа това изискване – виж „Ограничения за X.509 удостоверение“.	Регламент/Приложение II (QSSCD) B-Trust Политики за КЕП/КЕПечат на ДКУУ „БОРИКА“ АД ETSI EN 319 412-5
ж) целостта на подписаните данни не е застрашена	Процесът на валидиране сравнява хеша от подписа/печата с хеша на данните от документа, който е подписан	Свойство на цифровия подпис и използваните криптографски алгоритми за подпис/печат и за хеш-функции Виж „Криптографски ограничения“ ETSI TS 119-312
з) изискванията по член 26 са били изпълнени към момента на подписването	Процесът по валидиране на подписа/печата верифицира статуса и атрибутите на удостоверението към момента на генериране на подписа	За базов профил BASELINE_B това е Неудостоверено време; За профили BASELINE_T, _LT И _LTA – използва удостоверено време (квалифициран времеви печат).
Изисквания по чл. 33	**Изпълнение от УСЛУГАТА**	**Бележки**
Услугата по квалифицирано валидиране на квалифицирани електронни подписи/печати може да се предоставя единствено от доставчик на квалифицирани	„БОРИКА“ АД е ДКУУ в съответствие с Регламент 910/2014 и Закон за електронния подпис и електронните удостоверителни услуги в страната	http://www.crc.bg/files/_bg/Register_site_bg_30092017_Last_LAST.pdf

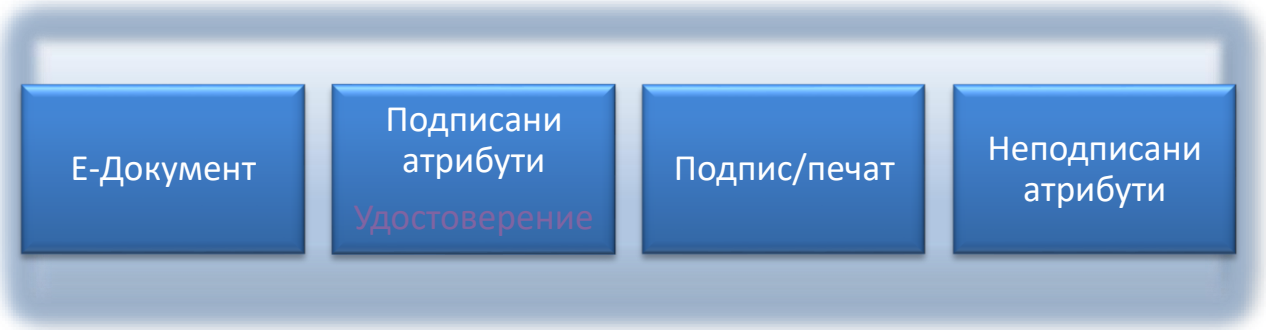
удостоверителни услуги		
извършва се валидиране в съответствие с член 32, параграф 1	УСЛУГАТА изпълнява изискванията по чл.32, параграф 1	Виж „Съответствие с Регламент 910/2014, чл. 32“
дава възможност на Доверяващите се страни да получат резултата от процеса на валидиране по автоматизиран начин, който е надежден и ефикасен и носи усъвършенстван електронен подпис или усъвършенстван електронен печат на доставчика на услугата по квалифицирано валидиране	УСЛУГАТА предоставя на Потребителя/Доверява-ща се страна Отчет от валидиране както следва: • За уеб-клиент в браузъра с GUI (графичен интерфейс) четим документ в .pdf формат; • За приложение/система със SOAP-интерфейс (Request/Response команди) автоматичен (програмен) режим на получаване на резултата от валидиране през този интерфейс.	Виж т. 6.5. „Интерфейси и протоколи на валидиране“ в този документ Виж т. 6.4 „Статус-индикатори и Отчен от валидиране“ в този документ

Приложение 1. Профили на е-подпис/печат валидирани от УСЛУГАТА

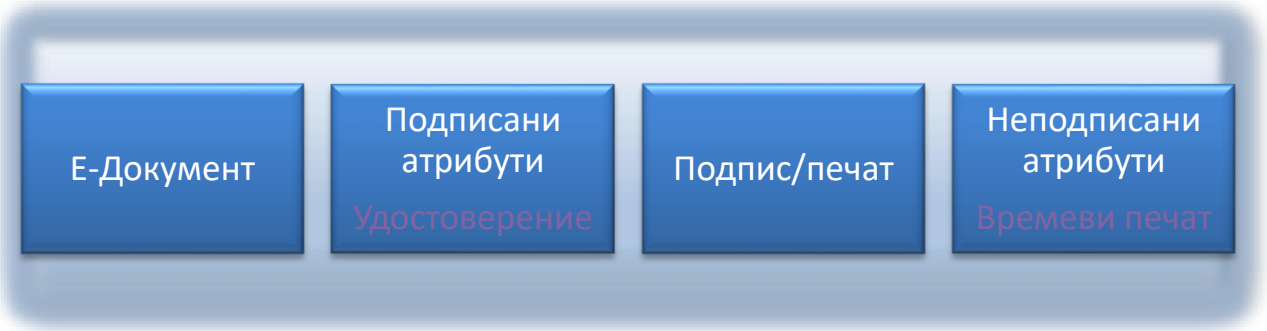
1. Обща структура на Е-подпис/печат



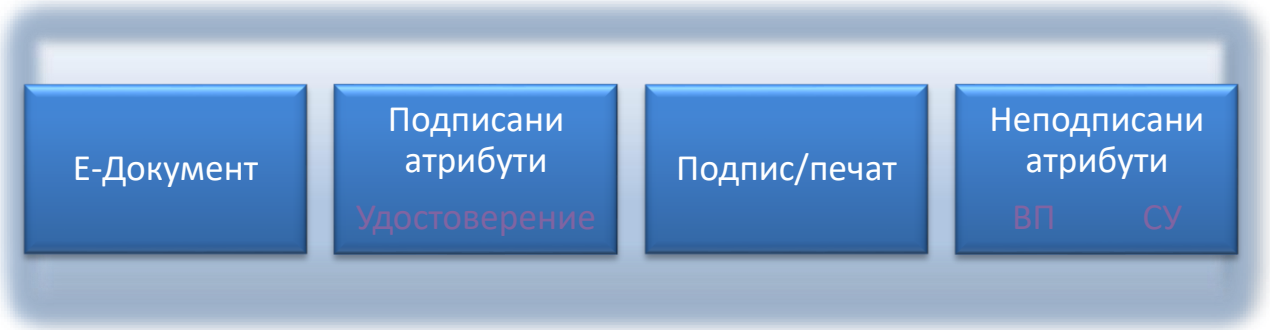
2. Базов е-подпис/печат (**BASELINE_B**)



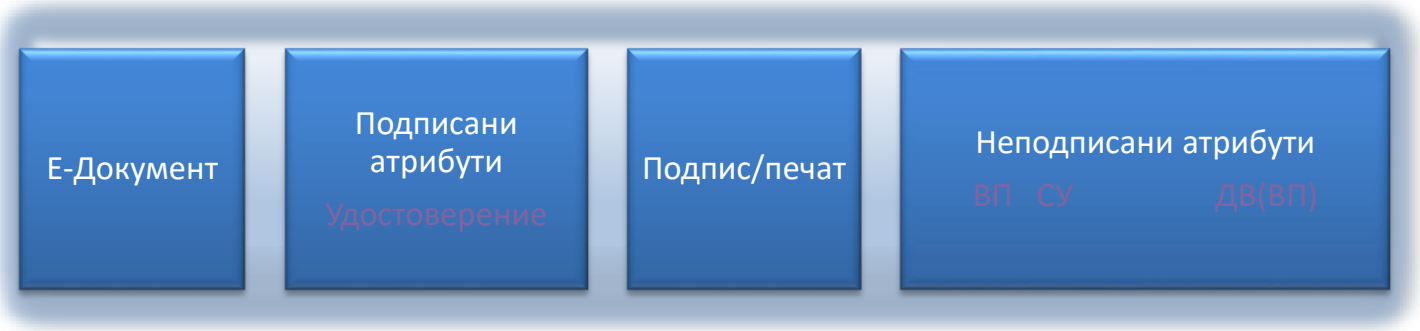
3. Профил **BASELINE_T** (с удостоверено време на подписа/печата)



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