ПОЛИТИКА И ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНА УСЛУГА ЗА УПРАВЛЕНИЕ НА УСТРОЙСТВА

ЗА СЪЗДАВАНЕ НА КВАЛИФИЦИРАН ЕЛЕКТРОНЕН ПОДПИС/ПЕЧАТ ОТ РАЗСТОЯНИЕ

Версия 1.0

10 Март 2026 г.

СЪДЪРЖАНИЕ

ОБХВАТ И УПОТРЕБА 4
СТАНДАРТИ/ТЕХНИЧЕСКИ СПЕЦИФИКАЦИИ ЗА ОТДАЛЕЧЕНО ПОДПИСВАНЕ 5
1 ВЪВЕДЕНИЕ 6
2 ОПРЕДЕЛЕНИЯ И СЪКРАЩЕНИЯ 6
3 КОНЦЕПЦИЯ 10
4 КОНЦЕПТУАЛЕН МОДЕЛ 11
5 ПРИЛОЖЕНИЕ ЗА СЪРВЪРНО ПОДПИСВАНЕ (SSA) 13
6 ВЗАИМОДЕЙСТВИЕ МЕЖДУ SCASC И SSASC 14
6.1 Специфични изисквания към обслужващия компонент на приложението за създаване на електронен подпис (SCASC) 14
6.2 Специфични изисквания към обслужващия компонент на приложението за сървърно подписване (SSASC) 14
7 ГЕНЕРИРАНЕ НА ПОДПИСВАЩИ КЛЮЧОВЕ 15
8 СЪЗДАВАНЕ НА ADES ЦИФРОВ ПОДПИС 16
9 ФУНКЦИОНАЛЕН МОДЕЛ 17
9.1 Функционалност „Регистрация“ и „Издаване“ на Облачен КЕП 17
9.2 Функционалност „Управление“ на Облачен КЕП 18
9.3 Функционалност „Подписване“ с Облачен КЕП 18
9.3.1 Поддържани формати и нива на електронен подпис 18
10 ПРОФИЛИ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ, НА CRL И НА OCSP 19
10.1 ПРОФИЛ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ 19
10.1.1 Номер на версия 19
10.1.2 Допустими разширения във формата на удостоверение 19
10.1.3 Идентификатори на алгоритмите на електронен подпис 19
10.1.4 Форми на именуване 19
10.1.5 Ограничения на имената 19
10.1.6 Идентификатор на Политика 19
10.1.7 Означение на квалифицираното удостоверение 20
10.2 Профил на Списъка на прекратени удостоверения 20
10.2.1 Версия 20
10.2.2 Формат 20
10.2.3 Формат на елемент в CRL 20
10.3 Профил на OCSP 21
11 ПРОВЕРКА И КОНТРОЛ НА ДЕЙНОСТТА НА ДОСТАВЧИКА 21
11.1 Периодична и обстоятелствена проверка 21

11.2 Квалификация на проверяващите лица 21
11.3 Отношения на проверяващите лица с Доставчика 21
11.4 Обхват на проверката 21
11.5 Обсъждане на резултатите и действия с оглед извършената проверка 22
11.6 Срок и прекратяване 22
11.7 Уведомяване и комуникация между страните 22
11.8 Промени в Документа 22
11.9 Решаване на спорове и място (подсъдност) 23
11.10 Приложимо право 23
11.11 Съответствие с приложимото право 23

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 от 10.03.2026**
- съдържа изискванията за услугата „Облачен КЕП“ (отдалечен подпис) в съответствие с ЕС Регламент 910/2014 изменен с Регламент 2024/1183 и приложимите технически за него спецификации EN 419 241-1/2/3, EN 419 221-5 TS 119 101 за тази УСЛУГА, оперирана от Доставчик на квалифицирани удостоверителни услуги (ДКУУ) „БОРИКА“ АД (Доставчик);
- следва общата политика и практика на Доставчика при предоставяне на КЕП и техните квалифицирани удостоверения като включва определени специфични изисквания относно Облачния КЕП;
- служи за оценка на дейността на ДКУУ „БОРИКА“ АД да предоставя Облачен КЕП в съответствие с Регламент 910/2014 изменен с Регламент 2024/1183;
- ползва или реферира технически спецификации относно УСЛУГАТА;
- може да бъде променян от ДКУУ и всяка нова редакция на този документ, отменя предишната такава.

СТАНДАРТИ/ТЕХНИЧЕСКИ СПЕЦИФИКАЦИИ ЗА ОТДАЛЕЧЕНО ПОДПИСВАНЕ

- Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (eIDAS).
- Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework.
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation – GDPR).
- ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.
- ETSI EN 319 411 Policy and security requirements for Trust Service Providers issuing certificates – Part 1: General requirements.
- ETSI TS 119 431 Policy and security requirements for trust service providers – Part 1: TSP service components operating a remote QSCD/SCDev (remote signing).
- ETSI TS 119 101 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for applications for signature creation and signature validation.
- ETSI TS 119 102 Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures – Part 1: Creation and Validation.
- ETSI TS 119 461 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects.
- CEN EN 419 241 Trustworthy Systems Supporting Server Signing – Part 1: General System Security Requirements.
- IETF RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.

1 ВЪВЕДЕНИЕ

Настоящият документ (Политика и Практика) определя политиката, практиките и изискванията за сигурност, прилагани от „БОРИКА“ АД, в качеството му на квалифициран доставчик на удостоверителни услуги, при предоставянето на услуги за създаване на квалифициран електронен подпис и квалифициран електронен печат от разстояние.

Документът описва изискванията за управление и функциониране на компонентите на услугата за отдалечено подписване, включително компонентите, управляващи устройства за създаване на квалифициран електронен подпис/печат от разстояние (QSCD/SCDev), както и компонентите, поддържащи създаването на AdES електронни подписи (SCASC).

Политиката и Практиката са разработени в съответствие с изискванията на Регламент (ЕС) № 910/2014 (eIDAS), изменен с Регламент 2024/1183, както и със съответните технически стандарти и спецификации, включително ETSI EN 319 401, ETSI EN 319 411-1/2, ETSI TS 119 431-1, ETSI TS 119 431-2 и CEN EN 419 241-1.

Компонентите на услугата за отдалечено подписване осигуряват създаването на електронни подписи и електронни печати чрез защитени криптографски устройства (QSCD), които гарантират сигурното генериране и съхранение на частните ключове за подписване и тяхното използване под контрола на титуляра на подписа.

Компонентът за създаване на AdES електронни подписи (SCASC) осигурява обработката на заявките за подписване, подготовката на данните за подписване и взаимодействието със сървърния компонент за подписване (SSASC) и съответното QSCD устройство. В рамките на този процес могат да бъдат използвани външни удостоверителни услуги, като например услуги за удостоверяване на време или валидиране на удостоверения.

Предоставяната от „БОРИКА“ АД услуга за отдалечено подписване позволява създаването на усъвършенствани и квалифицирани електронни подписи и електронни печати, базирани на X.509 удостоверения, издавани в рамките на инфраструктурата за публични ключове B-Trust.

Настоящият документ е предназначен за потребители на услугата, доверяващи се страни и одитори и има за цел да опише приложимите политики, контролни механизми и изисквания за сигурност при предоставянето на услугата за отдалечено създаване на електронни подписи и печати.

Документът е структуриран в съответствие с рамката, определена в IETF RFC 3647 „Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework“

2 ОПРЕДЕЛЕНИЯ И СЪКРАЩЕНИЯ

Термин	Определение
Електронен подпис	Данни в електронна форма, които се добавят към други данни в електронна форма или са логически свързани с тях и които титулярят използва, за да се подписва.
Signature Creation Application (SCA)	Приложение за създаване на електронен подпис.

Термин	Определение
Qualified Electronic Signature/Seal Creation Device (QSCD)	Устройство за създаване на квалифициран електронен подпис или печат, което отговаря на изискванията на Регламент (ЕС) № 910/2014.
Доверяващи се страни (Relying Parties)	Физически или юридически лица, които разчитат на удостоверителните услуги на БОРИКА АД.
Data to be Signed Representation (DTBS/R)	Форматирани данни, използвани за изчисляване на стойността на електронния подпис (например хеш стойност).
Квалифициран електронен подпис	Усъвършенстван електронен подпис, създаден чрез устройство за създаване на квалифициран електронен подпис и базиран на квалифицирано удостоверение.
Signature Activation Data (SAD)	Данни за активиране на подпис.
Електронна идентификация (eID)	Процес на използване на електронни данни за идентификация на физическо или юридическо лице.
Signature Creation Application Service Component (SCASC)	Обслужващ компонент на приложението за създаване на електронен подпис.
Server Signing Application (SSA)	Приложение за сървърно подписване, използващо устройство за създаване на подпис от разстояние.
Практика (CPS)	Документ, който определя процедурите и правилата за издаване, управление, спиране и прекратяване на удостоверения, както и условията за предоставяне на удостоверителни услуги.
Signature Creation System (SCS)	Система за създаване на електронни подписи.
Данни за създаване на електронен подпис	Уникални данни, използвани от титуляря на електронния подпис за създаването на електронен подпис.
Server Signing Application Service Component (SSASC)	Обслужващ компонент на приложението за сървърно подписване, който генерира стойности на електронния подпис от името на подписващия.
Удостоверителна услуга	Електронна услуга, която включва създаване, проверка и валидиране на електронни подписи, електронни печати, електронни времеви печати, услуги за електронна препоръчана поща или удостоверения за автентичност на уебсайтове.
Signature Activation Module (SAM)	Модул за активиране на подпис, представляващ конфигуриран софтуер, изпълняван в защитена среда.
Удостоверение за електронен подпис	Електронен атестат, който свързва данните за валидиране на електронен подпис с физическо лице.
Trustworthy System Supporting Server Signing (TW4S)	Надеждна система за сървърно подписване, използваща ключове за подписване под единствения контрол на подписващия.
AdES (digital) signature	Електронен подпис във формат CAdES, PAdES или XAdES.
Квалифицирана удостоверителна услуга	Удостоверителна услуга, която отговаря на изискванията на Регламент (ЕС) № 910/2014.

Термин	Определение
Server Signing Application Service Provider (SSASP)	Доставчик на услуга, предоставящ приложение за сървърно подписване.
Signature Creation Application Service Provider (SCASP)	Доставчик на услуга, предоставящ приложение за създаване на електронен подпис.
Remote Signature Creation Device (SCDev)	Устройство за създаване на електронен подпис или печат от разстояние, което осигурява операцията по подписване да се извършва под единствения контрол на подписващия.
Частен ключ	Криптографски ключ, използван за създаване на електронен подпис или за декриптиране на данни.
Signer Interaction Component (SIC)	Компонент за взаимодействие с подписващия.
Средство за електронна идентификация	Материална или нематериална единица, съдържаща данни за електронна идентификация, използвана за удостоверяване на самоличност при онлайн услуги.
Квалифицирано удостоверение за електронен подпис	Удостоверение, издадено от доставчик на квалифицирани удостоверителни услуги, което отговаря на изискванията на Регламент (ЕС) № 910/2014.
Доставчик на квалифицирани удостоверителни услуги	Доставчик на удостоверителни услуги, който предоставя една или повече квалифицирани удостоверителни услуги и е получил квалифициран статут от надзорния орган.
Квалифициран електронен печат	Усъвършенстван електронен печат, създаден чрез устройство за създаване на квалифициран електронен печат и базиран на квалифицирано удостоверение.
Удостоверение за електронен печат	Електронен атестат, който свързва данните за валидиране на електронен печат с юридическо лице.
Публичен ключ	Част от двойка ключове в асиметрична криптосистема, използвана за проверка на електронен подпис.
Електронен печат	Данни в електронна форма, които се добавят към други данни в електронна форма или са логически свързани с тях, с цел гарантиране на произхода и целостта на данните.
Signature Activation Protocol (SAP)	Протокол за активиране на подпис.
Създател на печат	Юридическо лице, което създава електронен печат.
Driving Application (DA) / Digital Identity Solution (DIS)	Управляващо приложение, което организира процесите по създаване, валидиране и разширяване на електронни подписи, както и взаимодействието с крайни потребители и външни услуги.
Титуляр на електронен подпис	Физическо лице, което създава електронен подпис.
Стойност на електронния подпис	Резултат от криптографска обработка на данни, който позволява проверка на произхода и целостта на информацията.
Устройство за създаване на квалифициран електронен подпис	Устройство за създаване на електронен подпис, което отговаря на изискванията на Регламент (ЕС) № 910/2014.

Термин	Определение
Устройство за създаване на квалифициран електронен печат	Устройство за създаване на електронен печат, което отговаря на изискванията на Регламент (ЕС) № 910/2014.
Автентификация	Електронен процес за удостоверяване на идентичността на физическо или юридическо лице или за потвърждаване на произхода и целостта на данни.
Данни за идентификация на лица	Набор от данни, които позволяват установяване на самоличността на физическо или юридическо лице.

3 КОНЦЕПЦИЯ

Квалифицираният електронен подпис (КЕП), реализиран чрез смарт карта, отговаря на основните изисквания на Регламент (ЕС) № 910/2014 (eIDAS):

(1) данните за създаване на електронния подпис (частният ключ) да бъдат защитени и съхранявани в квалифицирано устройство за създаване на електронен подпис (QSCD);

(2) използването на тези данни да бъде под единствения контрол на титуляря на подписа (Signatory);

(3) подписът да се основава на квалифицирано удостоверение.

Концепцията за „Облачен КЕП“ реализира тези изисквания чрез централизирано генериране, съхранение и управление на ключовете за електронен подпис в защитена сървърна инфраструктура на доставчика на квалифицирани удостоверителни услуги (ДКУУ). В този модел частните ключове се съхраняват в хардуерен криптографски модул (HSM), който функционира като отдалечено QSCD (Remote QSCD).

БОРИКА АД предоставя услуга за отдалечено създаване на електронни подписи и електронни печати чрез изграждане и поддържане на надеждна система за сървърно подписване съответстваща на изискванията за сигурност, определени в стандарт CEN EN 419 241-1.

Надеждната система функционира в контролирана и защитена среда, която включва организационни, технически и физически мерки за сигурност, свързани с управлението на персонала, процедурите за експлоатация на системата, както и поддържането на съответната техническа и оперативна документация. Тези мерки имат за цел да гарантират надеждното предоставяне на услуга за отдалечено създаване на електронни подписи и електронни печати.

Нивото на доверие относно контрола върху използването на подписващия ключ при създаването на електронен печат може да се различава от нивото, изисквано при създаване на електронен подпис, в зависимост от приложимите регулаторни изисквания и съответната политика за предоставяне на услугата.

Надеждната система на БОРИКА АД, поддържаща сървърно подписване (TW4S), предоставя услуга за отдалечено създаване на електронни подписи и електронни печати, като гарантира, че ключовете за подписване се използват единствено под контрола на техния притежател.

Системата поддържа две нива на осигуряване на контрол върху използването на подписващите ключове („sole control assurance levels“), съгласно изискванията на EN 419 241-1:

SCAL1 – ниво на контрол с ниска степен на доверие.

При това ниво ключовете за подписване могат да бъдат генерирани, съхранявани и използвани извън криптографски хардуерен модул, например в защитени файлови структури. В такива случаи системата прилага допълнителни организационни и технически мерки за защита срещу неоторизирана модификация, изтриване или компрометиране на ключовете.

Операцията по подписване се разрешава след успешно удостоверяване на подписващия в приложението за сървърно подписване (SSA), което свързва идентификационните фактори на подписващия с използването на съответния ключ за подписване.

SCAL2 – ниво на контрол с висока степен на доверие.

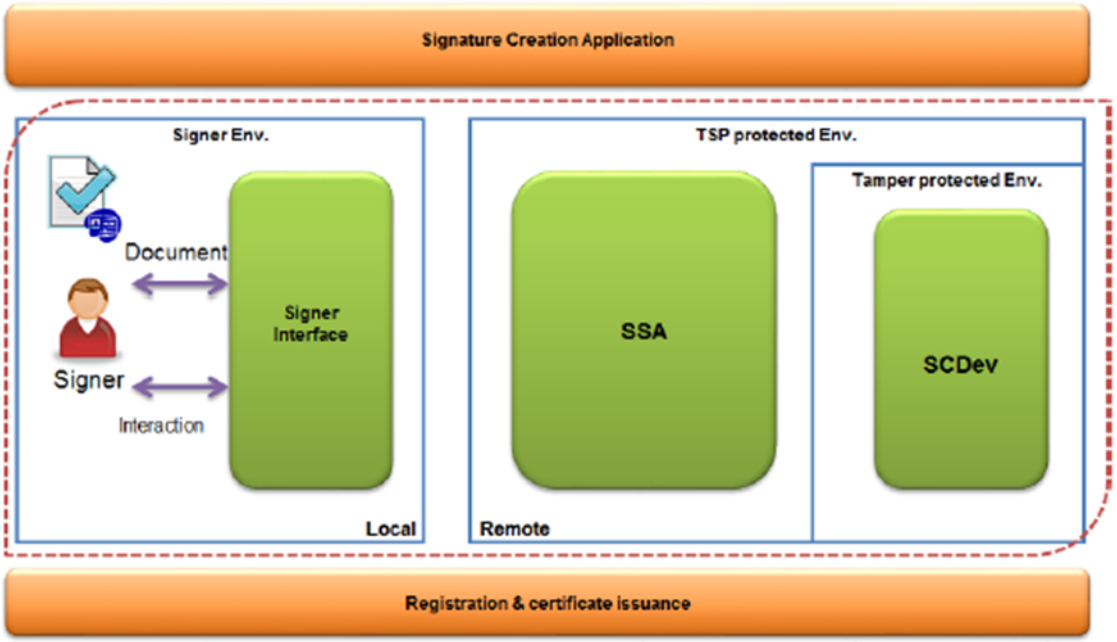
При това ниво се използват специализирани защитени компоненти за управление на процеса по активиране на подписа. Взаимодействието между модула за активиране на подпис (Signature Activation

Module – SAM) и компонента за взаимодействие с подписващия (Signer Interaction Component – SIC), чрез приложението за сървърно подписване (SSA), води до формиране на данните за активиране на подписа (Signature Activation Data – SAD).

Тези данни позволяват изпълнението на операцията по подписване върху конкретни данни за подписване. В рамките на SCAL2 модулът SAM управлява използването на SAD и прилага протокол за активиране на подпис (Signature Activation Protocol – SAP), който осигурява ниво на сигурност, еквивалентно на това, което се постига при използване на самостоятелно устройство за създаване на квалифициран електронен подпис (QSCD), съгласно Регламент (ЕС) № 910/2014.

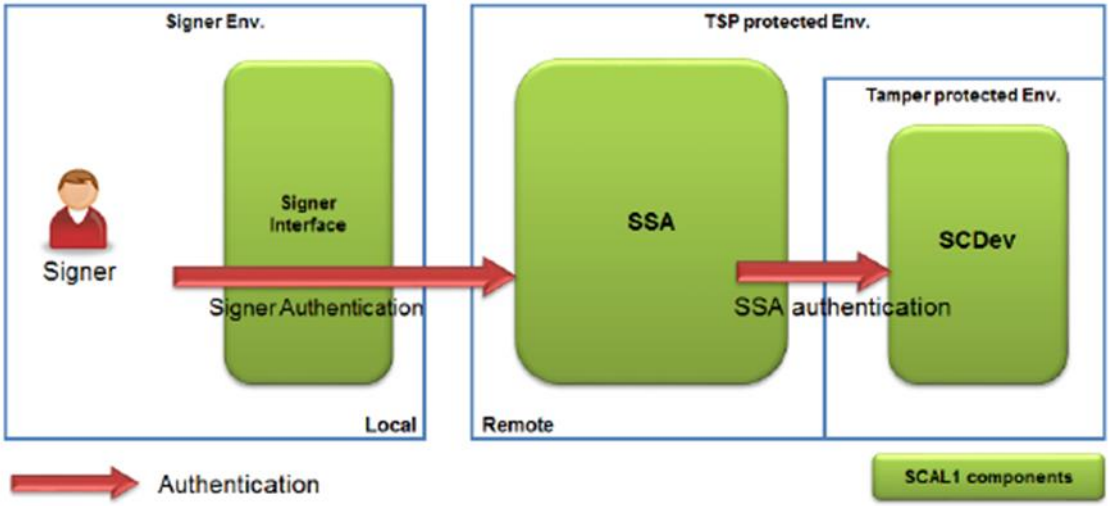
4 КОНЦЕПТУАЛЕН МОДЕЛ

На Фиг. 1 е представен най-общия концептуален модел на отдалечено (сървърно) подписване с КЕП. Ролята на отдалечено QSCD в модела се изпълнява от HSM на сървъра при Доставчика. Отсъстват организационно-техническите изисквания и мерки, които обезпечават сигурността на персоналния контрол (sole control assurance).



Фиг. 1 Общ концептуален модел на отдалечено подписване

Към този концептуален модел се въвеждат допълнителни технико-организационни мерки за силна автентификация на Титуляря на база динамично двуфакторно удостоверяване, където TOTP-кода представлява единият фактор, а вторият фактор е притежавания смартфон с активирано регистрирано мобилно приложение. Частният ключ е защитен в SSAS, така че ключът не се появява в явен вид извън HSM. Достъп до използването на ключа е възможно единствено след успешно удостоверяване на Титуляря (трябва да има процедури, които да гарантират, че системни администратори, включително администратори на HSM, не могат да получат достъп до данните за автентификация на Титуляря - парола/ПИН-код и OTP-код).



Фиг.2 Концептуален модел на отдалечено подписване SCALl 1

На Фиг. 2 е представен концептуален модел на Облачен КЕП с въведени технико-организационни мерки, обезпечаващи Ниво I на сигурност на персонален контрол (**Level I** sole control assurance).

При ниво SCAL1 поверителността и целостта на подписващия ключ се осигуряват от устройството за създаване на подпис (SCDev). Това устройство съхранява ключа за подписване и гарантира, че той не може да бъде извлечен или използван извън защитената среда на системата.

Активирането на устройството за създаване на подпис се извършва чрез приложението за сървърно подписване (SSA). Преди да бъде разрешено използването на ключа за подписване, подписващият трябва да бъде успешно удостоверен от SSA. След като автентификацията бъде извършена, системата може да активира ключа за подписване и да разреши извършването на операции по подписване от името на подписващия.

В рамките на SCAL1 активирането на ключа може да бъде валидно за определен период от време или за определен брой операции по подписване. Това означава, че след успешното удостоверяване на подписващия, ключът може да бъде използван за подписване на няколко документа в рамките на предварително определен времеви интервал или до достигане на определен брой подписи.

Този модел позволява приложението за сървърно подписване да се използва ефективно за масово или пакетно подписване на документи (batch signing), при което множество документи могат да бъдат подписани след еднократно удостоверяване на подписващия.

Тази архитектура може да се използва за създаване на стойност на цифров подпис (например хеш, криптиран с частния ключ на подписващия) при по-ниско ниво на осигуряване на контрол.

При ниво на сигурност SCAL2 операцията по подписване се извършва чрез взаимодействие между компонентите SIC, SSA, SAM и SCDev (HSM). Данните за активиране на подписа (SAD) се генерират в процеса на протокола за активиране на подпис (SAP) и свързват удостоверяването на подписващия, избрания ключ за подписване и данните за подписване.

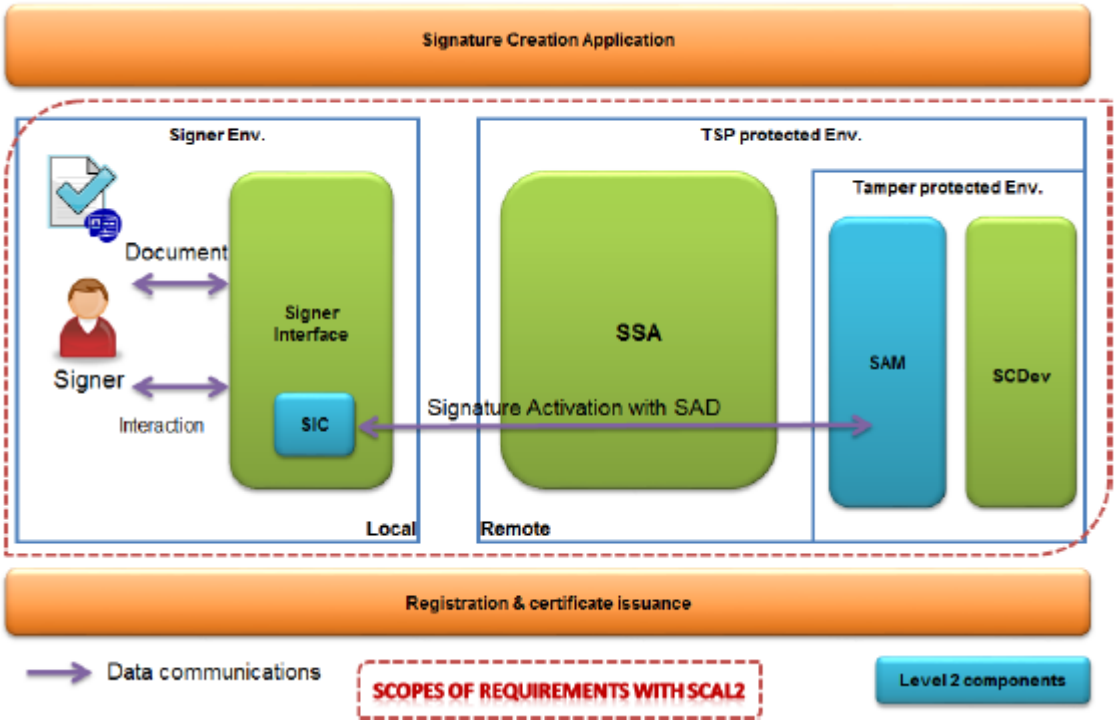
Модулът за активиране на подпис (SAM), разположен в защитена среда, валидира SAD и управлява активирането на ключа за подписване в криптографския модул. По този начин се гарантира, че

използването на ключа за подписване се извършва под единствения контрол на подписващия („sole control“) съгласно изискванията на Регламент (ЕС) №910/2014.

Системата за сървърно подписване (TW4S) на БОРИКА АД се състои от приложение за сървърно подписване (SSA) и устройство за създаване на отдалечен подпис (SCDev), управлявано чрез SAM. Подписващият взаимодейства със системата чрез компонент за взаимодействие със подписващия (SIC), който осигурява връзката между подписващия и конкретната операция по подписване.

След успешна автентификация на подписващия SSA и валидиране на SAD от SAM се активира ключът за подписване в SCDev и се генерира стойността на цифровия подпис. Генерираният подпис се връща към приложението за създаване на подпис (SCA), което създава подписания електронен документ.

TW4S поддържа и пакетно подписване, при което един набор от данни за активиране на подпис (SAD) може да бъде използван за подписване на повече от един документ.



Фиг.3 Концептуален модел на отдалечено подписване SCALI 2

5 ПРИЛОЖЕНИЕ ЗА СЪРВЪРНО ПОДПИСВАНЕ (SSA)

Приложението за сървърно подписване (SSA) е компонент на системата за отдалечено създаване на електронни подписи, чрез който се управлява процесът по генериране на стойност на цифровия подпис върху данните за подписване (DTBS/R). Подписването се извършва чрез обслужващия компонент на приложението за сървърно подписване (SSASC), който използва ключ за подписване, съхраняван в криптографски модул (SCDev).

Ключовете за подписване се създават и съхраняват в защитена среда на криптографския модул, като тяхното използване се разрешава единствено след успешно удостоверяване на подписващия. Управлението на активирането на ключа за подписване се извършва чрез модул за активиране на подпис (SAM), който използва данни за активиране на подписа (SAD) за удостоверяване на подписващия и разрешаване на операцията по подписване.

Системата поддържа две нива на осигуряване на „sole control“ върху подписващия ключ:

SCAL1 – ключът за подписване се използва след успешно удостоверяване на подписващия от SSASC. Активирането на ключа може да бъде валидно за определен период от време или за определен брой операции по подписване.

SCAL2 – ключът за подписване се активира чрез модул SAM, който проверява данните за активиране на подписа (SAD), генерирани чрез протокол за активиране на подпис (SAP). По този начин се гарантира, че ключът за подписване се използва с висока степен на увереност под единствения контрол на подписващия.

Създаването на стойността на цифровия подпис се извършва в отдалеченото устройство за създаване на подпис (SCDev), като SSA управлява комуникацията между компонентите на системата и осигурява достъп до услугата за подписване за оторизираните подписващи.

6 ВЗАИМОДЕЙСТВИЕ МЕЖДУ SCASC И SSASC

Архитектурата на услугата за отдалечено сървърно подписване включва взаимодействие между обслужващия компонент на приложението за създаване на подпис (SCASC) и обслужващия компонент на приложението за сървърно подписване (SSASC).

SCASC получава документите или техните хеш стойности, които трябва да бъдат подписани, и подготвя данните за подписване. Тези данни се изпращат към SSASC, който чрез отдалеченото устройство за създаване на подпис (SCDev) генерира стойността на цифровия подпис.

Генерираната стойност на подписа се връща към SCASC, който я включва в съответния електронен подпис или електронен печат в съответствие с използвания формат (например CAdES, PAdES или XAdES).

SCASC и SSASC могат да взаимодействат и с външни удостоверителни услуги, като сертифициращ орган (CA), регистрационен орган (RA), услуги за проверка на статуса на удостоверения (OCSP/CRL), услуги за времеви печати (TSA) и услуги за удостоверяване.

Системата поддържа и пакетно (batch) подписване, при което множество документи или хешове на документи могат да бъдат подписани в рамките на една операция по подписване.

6.1 Специфични изисквания към обслужващия компонент на приложението за създаване на електронен подпис (SCASC)

БОРИКА прилага следните изисквания към обслужващия компонент на приложението за създаване на електронен подпис (**SCASC**), в съответствие с приложимите стандарти за сървърно подписване:

SCASC поддържа създаване на усъвършенствани и квалифицирани електронни подписи (**AdES/QES**) и възможност за добавяне на удостоверено време (**time-stamp**) към подписа.

SCASC поддържа създаване на електронни подписи в съответствие с приложимите стандарти и формати за електронно подписване, както е описано в настоящата политика.

SCASC осигурява взаимодействие със сървърния компонент за подписване (**SSASC**) и с устройството за създаване на подпис (**SCDev/QSCD**) чрез защитени комуникационни канали.

SCASC гарантира принципа **WYSIWYS,** като осигурява възможност подписващият да прегледа документа или неговото представяне преди потвърждение на операцията по подписване.

Архитектурата на системата допуска участие на външни системи или доверяващи се страни чрез защитени интерфейси, при условие че са изпълнени всички изисквания за сигурност и идентификация, определени в настоящата политика.

6.2 Специфични изисквания към обслужващия компонент на приложението за

сървърно подписване (SSASC)

БОРИКА АД прилага специфични изисквания при предоставянето на услугата за отдалечено създаване на електронни подписи чрез обслужващия компонент на приложението за сървърно подписване (SSASC). Тези изисквания гарантират сигурността на криптографските операции, управлението на ключовете и съответствието с приложимите стандарти и регулаторни изисквания.

Криптографските алгоритми и дължината на ключовете, използвани в инфраструктурата на БОРИКА, са съобразени с изискванията на ETSI TS 119 312 и с добрите практики за сигурност при предоставяне на квалифицирани удостоверителни услуги.

Ключовете за електронен подпис или електронен печат на титулярите се генерират и съхраняват в защитена криптографска среда (SCDev/QSCD), разположена в инфраструктурата на БОРИКА и отговаряща на приложимите стандарти за сигурност. Частните ключове не се извеждат извън защитената среда на криптографския модул.

Системата за сървърно подписване използва криптографски алгоритми и хеш функции, които осигуряват достатъчно ниво на сигурност за целия жизнен цикъл на удостоверенията и подписите. При необходимост БОРИКА извършва периодичен преглед на използваните алгоритми и предприема актуализация при установяване на намалено ниво на сигурност или при промяна в нормативните или стандартни изисквания.

Управлението и използването на подписващите ключове се извършва чрез защитена инфраструктура за сървърно подписване, която гарантира, че ключовете се използват единствено след успешно удостоверяване и авторизация на подписващия и при условията на „единствен контрол“ (sole control) съгласно изискванията на Регламент (ЕС) № 910/2014 (eIDAS).

Политиките и практиките, свързани с предоставянето на услугата за квалифициран електронен подпис и печат, са публично достъпни за всички заинтересовани страни чрез интернет страницата на БОРИКА. Документи, съдържащи чувствителна информация, включително вътрешни процедури по информационна сигурност, не се публикуват и са достъпни само за оторизиран персонал.

7 ГЕНЕРИРАНЕ НА ПОДПИСВАЩИ КЛЮЧОВЕ

БОРИКА АД прилага изискванията на приложимите политики и стандарти за отдалечено създаване на електронни подписи съгласно Регламент (ЕС) № 910/2014 (eIDAS) при генерирането и управлението на подписващите ключове.

Ключовете за подписване на потребителите се генерират и съхраняват в устройство за създаване на електронен подпис (SCDev/QSCD), което функционира в съответствие със своята сертифицирана конфигурация.

При генериране и управление на подписващи ключове БОРИКА АД прилага следните изисквания:

- Частните ключове се генерират и използват единствено в SCDev. Устройството представлява сертифицирана криптографска система с ниво на сигурност най-малко Common Criteria EAL4+ или еквивалентно, съответстваща на изискванията на стандарт EN 419 221.
- Подписващите ключове се генерират и съхраняват в защитената среда на SCDev и не могат да бъдат извеждани извън устройството, което гарантира тяхната поверителност и целостта им.
- Използваните криптографски алгоритми и параметри са съобразени с техническата спецификация ETSI TS 119 312, БОРИКА извършва периодичен преглед на използваните алгоритми и при необходимост актуализира криптографските параметри или генерира нови ключове.
- Инициализацията и управлението на SCDev се извършват чрез контролирани процедури, които изискват участие на минимум двама упълномощени оператори.

- Криптографските алгоритми, използвани за създаване на подписи, се избират така, че да осигуряват необходимото ниво на сигурност за целия период на валидност на съответното удостоверение.
- Ключовете за подписване могат да бъдат генерирани предварително, независимо от процеса по издаване на удостоверение.
- При ниво на сигурност SCAL2 генерирането и използването на ключовете за подписване се управлява чрез модул за активиране на подпис (SAM), който гарантира, че ключът се използва под единствения контрол на подписващия. SAM функционира в защитена среда и използва данните за активиране на подписа (SAD), генерирани чрез протокола за активиране на подпис (SAP).
- Отдалеченото устройство за създаване на подпис (SCDev) представлява криптографски модул, който работи в защитена среда и позволява генерирането и използването на ключовете за подписване единствено след успешно удостоверяване на подписващия.

8 СЪЗДАВАНЕ НА ADES ЦИФРОВ ПОДПИС

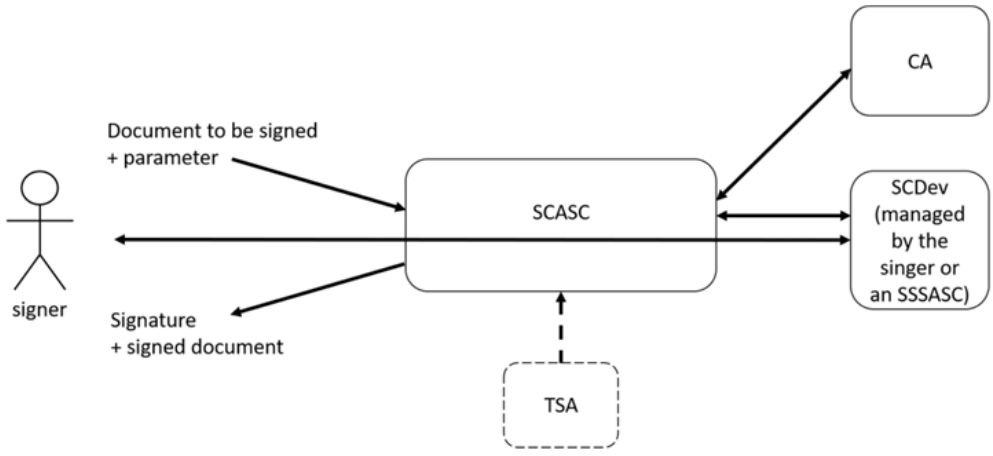
В процеса на създаване на електронен подпис участва обслужващ компонент на приложението за създаване на подпис (**SCASC – Signature Creation Application Service Component**). Този компонент получава документа, който следва да бъде подписан, или неговата хеш стойност, както и допълнителни параметри, необходими за създаване на подписа.

След получаването на документа SCASC събира и подготвя цялата необходима информация за подписването. На тази основа се формират данните за подписване (**DTBSR – Data To Be Signed Representation**), които представляват подготвената информация, върху която ще бъде изчислена стойността на цифровия подпис. Тези данни се изпращат към устройство за създаване на електронен подпис (**SCDev – Signature Creation Device**).

Преди създаването на подписа системата извършва удостоверяване на подписващия и потвърждение на неговото съгласие за подписване на конкретния документ. Това удостоверяване може да се извърши чрез компонентите на системата за подписване или чрез директно взаимодействие между подписващия и устройството за създаване на подпис.

След успешното удостоверяване и потвърждение на операцията по подписване, SCDev използва частния ключ на подписващия и изчислява стойността на цифровия подпис. Получената стойност се връща обратно към SCASC, който я включва в окончателния електронен подпис върху документа.

По този начин SCASC управлява процеса по създаване на подписа, докато SCDev реализира самата криптографска операция по подписване с използване на частния ключ на подписващия.



9 ФУНКЦИОНАЛЕН МОДЕЛ

Платформата за Облачен КЕП включва две компоненти:

- Отдалечена сървърна компонента, под управление и контрол на ДКУУ „БОРИКА“ АД;
- Мобилно приложение за смартфон (за платформите Android и iOS).

Сървърната част на Платформата за Облачен КЕП е част от инфраструктурата B-Trust на ДКУУ „БОРИКА“ АД и включва две обособени подсистеми:

- Подсистема за Издаване на Облачен КЕП
- Подсистема за Подписване с Облачен КЕП

Първоначално издаване, подновяване и управление (спиране/възобновяване и прекратяване/отмяна) на Облачен КЕП следват общите функционални изисквания и съответните процедури за КЕП, представени в документа “ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ И УДОСТОВЕРИТЕЛНИ УСЛУГИ ЗА ТЯХ ОТ „БОРИКА” АД” (B-Trust CPS-eIDAS). Настоящият документ съдържа само особеностите и отличията при тези функционални процедури относно Облачния КЕП.

Мобилното приложение B-Trust Mobile е специализирано приложение за двете мобилни платформи – Android и iOS за смартфон на Титуляря и служи да активира създаването/генерирането Облачния КЕП. Мобилното приложение B-Trust Mobile е свободно достъпно за зареждане и се инициализира чрез смартфона на Титуляря.

Сървърната част на Платформата за Облачен КЕП в обхвата на B-Trust инфраструктурата поддържа две основни функционалности:

- „Регистрация“ и „Издаване“ на Облачен КЕП – имплементират се чрез Подсистемата за Издаване на Облачен КЕП;
- „Подписване“ с Облачен КЕП – имплементира се чрез Подсистемата за Подписване с Облачен КЕП.

Функционалност „Подписване” на Подсистемата за Подписване използва следните работещи компоненти на B-Trust инфраструктурата:

- Публичен регистър и CRL на квалифицирани удостоверения (LDAP-сървър); и/или
- OCSP-сървър.

9.1 Функционалност „Регистрация“ и „Издаване“ на Облачен КЕП

Информацията в тази част на документа следва да се ползва съвместно с информацията в B-Trust CPS-eIDAS.

Потребителят използва смарт устройство (смартфон или таблет) с инсталирано мобилно приложение B-Trust. Процесът започва със съгласие с приложимите условия за отдалечена идентификация и обработка на лични данни, както и с преглед на съответните политики и общи условия, свързани с предоставянето на квалифицирани удостоверителни услуги.

За регистрация потребителят предоставя мобилен номер и електронна поща, които се валидират чрез изпращане на еднократен код (OTP). След успешна валидация потребителят заснема своя документ за самоличност, като системата извършва автоматично извличане на данните чрез OCR, проверка на защитните елементи на документа и контрол на качеството на изображението.

Следва идентификация чрез заснемане на лицето (selfie) и извършване на проверка за „liveness“, която удостоверява, че лицето е реално и присъства по време на процеса. Полученото изображение се сравнява със снимката от документа за самоличност.

Извлечените данни се валидират спрямо налични надеждни източници на национално ниво чрез интеграция с регистри за гражданска идентификация. При наличие на съответствие се извършва допълнително сравнение между снимката от регистъра, изображението от документа и заснетото selfie.

Методът за отдалечена идентификация е признат на национално ниво от компетентния регулаторен орган и е част от регистрирана услуга за електронна идентификация. След успешното преминаване на автоматичните проверки процесът се подлага и на допълнителна проверка от оператор на БОРИКА АД.

9.2 Функционалност „Управление“ на Облачен КЕП

Функционалност „Управление/Поддръжка“ на Облачен КЕП включва:

- Спиране (временно) на действието на Облачен КЕП;
- Възобновяване на действието на временно спрян Облачен КЕП;
- Прекратяване/отмяна на действието на Облачен КЕП.

Продължаване (Renew) на действието на Облачен КЕП не се поддържа. ДКУУ „БОРИКА“ АД издава квалифицираните удостоверения за Облачен КЕП със срок на валидност 3 (три) години. След този срок на валидност, Титулярят на облачен КЕП може да заяви издаване на нов такъв.

9.3 Функционалност „Подписване“ с Облачен КЕП

Тази функционалност в обхвата на Подсистемата за Използване в сървърната компонента на Платформата за Облачен КЕП изпълнява само генериране на цифров подпис (PKCS#1) за Облачния КЕП. Генерираният цифров подпис и съответстващото удостоверение за публичния ключ на подписа се предоставят на обособена приложна система, която интегрира формира контейнера на е-подписа съобразно заявен/изискван формат/профил на КЕП (CAdES, XAdES, PAdES, ASiCS/E) и ниво на подписа (BASELINE_B, BASELINE_T, BASELINE_LT, BASELINE_LTA).

9.3.1 Поддържани формати и нива на електронен подпис

Ниво на AdES подпис	Описание	CAdES	XAdES	PAdES
Baseline B	Базов електронен подпис, гарантиращ целостта на подписания документ и неотменимостта на подписа	CAdES-B-B	XAdES-B-B	PAdES-B-B
Baseline T	Базов подпис с добавен удостоверен времеви печат (timestamp), доказващ момента на подписване	CAdES-B-T	XAdES-B-T	PAdES-B-T
Baseline LT	Подпис с дългосрочна валидност чрез включени данни за проверка на удостоверението (CRL/OCSP)	CAdES-B-LT	XAdES-B-LT	PAdES-B-LT
Baseline LTA	Подпис с дългосрочна валидност и архивни времеви печати за гарантиране на валидността при дългосрочно съхранение	CAdES-B-LTA	XAdES-B-LTA	PAdES-B-LTA

Формат	Описание	Поддържани типове подпис
CAdES	Формат за електронен подпис, базиран на CMS/PKCS#7, позволяващ подписване на произволни файлове и поддържащ дългосрочна валидност на подписа	ENVELOPING, DETACHED
PAdES	Формат за електронен подпис на PDF документи, при който подписът е интегриран в самия PDF файл	ENVELOPED

Формат	Описание	Поддържани типове подпис
XAdES	Формат за електронен подпис на XML документи, поддържащ разширени атрибути за дългосрочна валидност	ENVELOPED, ENVELOPING, DETACHED

Тип на подпис	Описание
ENVELOPED	Подписът е включен вътре в подписания документ
ENVELOPING	Подписът съдържа самия подписан документ
DETACHED	Подписът е отделен от подписания документ

10 ПРОФИЛИ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ, НА CRL И НА OCSP

10.1 ПРОФИЛ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ

Пълното съдържание (профил) на КУ се съдържа в публикуваните документите за съответните Политики на Доставчика.

10.1.1 Номер на версия

Доставчикът издава КУ във формат X.509, v3.
Версията се вписва в издаваното КУ.

10.1.2 Допустими разширения във формата на удостоверение

Атрибут „Subject Key Identifier"- формира се от публичния ключ, удостоверен в удостоверението като хеш-стойност на публичния ключ.
Атрибут „Authority Key Identifier"- формира се като хеш-стойност на публичния ключ на оперативния УО на Доставчика.
Атрибут „Issuer Alternative Name"- съдържа URL-стринг като алтернативно име на Доставчика.
Атрибут „Basic Constrains"- определя типа на удостоверението и има стойност „End entity" в удостоверението на Потребителя.
Атрибут „Certificate Policy" - определя идентификатора на Политиката за КУ.
Атрибут „Key Usage" - атрибут, който определя употребата и ограниченията в употреба на удостоверението.
Атрибут „Extehanced Key Usage" - допълва значението на атрибут "Key Usage" и указва допълнителните и специфични приложения на удостоверението.
Атрибут „CRL Distribution Point" - съдържа линк към актуалния CRL на оперативния УО на Доставчика.
Атрибут „Authority Information Access" - съдържа URL-адреса на OCSP сървъра за валидация на удостоверението.
Атрибут „Qualified Statements" - атрибутът съдържа указание, че удостоверението е квалифицирано и дали частния ключ е генериран и се съхранява върху QSCD.

10.1.3 Идентификатори на алгоритмите на електронен подпис

Атрибутът „Signature algorithm" идентифицира алгоритмите (криптографските механизми), които се използват.

10.1.4 Форми на именуване

Виж секция „Именуване" от този документ.

10.1.5 Ограничения на имената

Виж секция „Именуване" от този документ.

10.1.6 Идентификатор на Политика

КУ се издават съгласно Политика на Доставчика, идентификаторът (OID) на която се вписва в атрибута „Certificate Policy" на удостоверението. Тази Политика на Доставчика е в съответствие с международно установените политики, съгласно ETSI/ITU-T в документи EN 319 411-1/2. Виж Таблица в т.1.3 на

документа.

10.1.7 Означение на квалифицираното удостоверение

Доставчикът използва в КУ с профил по стандарта X.509 v.3 атрибута „Qualified Statements" с идентификатори: „id-etsi-qcs-QcCompliance" (OID=0.4.0.1862.1.1), „id-etsi-qcs QcSSCD" (OID=0.4.0.1862.1.4) и „id-etsi-qcs-QcType" (OID=0.4.0.1862.1.6) със стойност „id-etsi-qct esign" (oid=0.4.0.1862.1.6.1) и „id-etsi-qct-eseal" (oid=0.4.0.1862.1.6.2) и „id-etsi-qcs QcPDS" (oid=0.4.0.1862.1.6.5).

10.2 Профил на Списъка на прекратени удостоверения

10.2.1 Версия

Доставчикът, чрез своите УО издава, публикува и поддържа Списъци на прекратени удостоверения (CRL) във формата X.509 v.2.

Версията се вписва в издадения CRL.

10.2.2 Формат

Доставчикът издава, публикува и поддържа CRL, чийто формат е в съответствие с изискванията в международната препоръка RFC 5280.

УО на Доставчика издават, публикуват и поддържат самостоятелни пълни CRL-и като в тях записват само прекратени удостоверения, които са издадени от съответния УО.

Доставчикът не издава и не поддържа схема на „частичен" (delta) CRL, но запазва право при необходимост да въведе такава схема.

Основните CRL-атрибути са:

- „Version"- версия;
- „Issuer Name" - идентифицира УО, издал и подписал Списъка;
- „Effective Date"/"This update" - време на издаване на Списъка;
- „Next Update"- времето на валидност на Списъка. След посоченото време, УО издава периодично нов Списък. През периода на валидност, в случай на прекратяване/спиране на удостоверение, УО издава незабавно нов CRL;
- "Signature algorithm" - означава криптографския механизъм/алгоритъма за електронен подпис на CRL;
- "Signature hash algorithm" - хеш-функцията в механизма на електронния подпис.

Допълнителни CRL-атрибути са:

- „Authority Key Identifier"- идентификатора на УО, който издава и подписва Списъка. Съдържа значението на „subjectKeyIdentifier" от удостоверението на УО, който подписва Списъка.

10.2.3 Формат на елемент в CRL

CRL на УО съдържа елементи за всички прекратени удостоверения от УО. Тези елементи са постоянни в Списъка.

CRL на УО съдържа елемент за всяко спряно удостоверение от УО. Такъв елемент е временен в Списъка до момента на възобновяване на удостоверението.

Атрибутите на елемент в CRL са:

- "Serial number" - серийният номер на прекратено/спряно удостоверение; "Revocation date"- време на прекратяване/спиране на удостоверение;
- "CRL Reason Code" – код, идентифициращ причината на прекратяване/спиране.

Значенията на причината за прекратяване/спиране на удостоверение са както следва:

- "keyCompromise" - компрометиран частен ключ на Потребителя;
- "CACompromise" - компрометиран частен ключ на оперативен УО на Доставчика;
- "affiliationChange" - променен статус на Потребител спрямо друго лице - промяна в представителната власт, отнемане на представителната власт, прекратяване на трудово правоотношение и т.н.;

- "superseded" - удостоверението е заместено с друго;
- "certificateHold" - действието на удостоверението временно е спряно.

10.3 Профил на OCSP

OCSP сървъра на Доставчика работи и предоставя услугата „онлайн проверка на статус на удостоверение в реално време" в съответствие с международно утвърдената препоръка IETF RFC 6960. Информация за профила на заявка и на отговор при работа с OCSP сървъра се съдържа в горепосочената техническа препоръка, публично достъпна от сайта на IETF.

11 ПРОВЕРКА И КОНТРОЛ НА ДЕЙНОСТТА НА ДОСТАВЧИКА

11.1 Периодична и обстоятелствена проверка

Контрол на правно-регламентираната дейност на Доставчика, свързана с удостоверенията за електронен подпис и нейната съобразност с изискванията на ЗЕДЕУУ и нормативната уредба се осъществява от Комисията за регулиране на съобщенията, в рамките на нейните компетенции.

Вътрешен контрол на дейността на Доставчика се назначава от оперативното ръководство и/или Съвета на директорите на юридическото лице на Доставчика като редът и обхватът на проверките е съобразен с вътрешни документи на юридическото лице.

Ръководството на Доставчика осъществява постоянен оперативен контрол за точното изпълнение на инструкциите при работа от персонала на Доставчика.

Ръководството на „БОРИКА“ АД назначава периодични проверки за съответствие на текущата дейност с утвърдените Практика и Политики относно дейността на Доставчика.

Доставчикът изпълнява постоянен контрол върху дейността на РО/МРС.

11.2 Квалификация на проверяващите лица

Проверяващи лица могат да бъдат само лица, които имат право да изпълняват такива функции в съответствие с възприети в международната практика изисквания и документи.

Проверяващите лица следва да са акредитирани от международна акредитационна организация да изпълняват такива проверки.

Вътрешните проверки на работата на РО/МРС се изпълняват от служители на Доставчика, които са оторизирани за тази дейност.

Проверяващи лица не могат да упълномощават други лица да извършват част или цялата проверка, освен с изричното съгласие на Доставчика.

Проверяващите лица носят отговорност за проверените факти и обстоятелства, независимо дали са превъзложили част или цялата проверка на други лица със съгласието на Доставчика.

11.3 Отношения на проверяващите лица с Доставчика

Проверяващите лица трябва да бъдат независими, да не са пряко или косвено свързани и да нямат конфликт на интереси с Доставчика.

Отношенията между Доставчика и проверяващо външно лице се уреждат с договор.

11.4 Обхват на проверката

Проверката от страна на Органи за оценяване на съответствието с Регламент (ЕС) № 910/2014 (изменен с Регламент (ЕС) 2024/1183) обхваща нормативно регламентираните изисквания към дейността на Доставчика съгласно ЗЕДЕУУ .

Вътрешната проверка може да обхваща всяко обстоятелство или дейност, посочени в този документ, както и:

- съпоставка на практики и процедури посочени в този документ с тяхната практическа реализация при изпълнение на дейността на Доставчика;
- проверка на дейността на подизпълнители - външни РО/МРС;
- други обстоятелства, факти и дейности, свързани с инфраструктурата B-Trust, по преценка на Ръководството на Доставчика.

11.5 Обсъждане на резултатите и действия с оглед извършената проверка

Въз основа на направените оценки и доклада от проверката, Ръководство на Доставчика набелязва мерки и срокове за отстраняване на констатираните пропуски и несъответствия.

Персоналът на Доставчика предприема конкретни действия за тяхното отстраняване в посочените срокове.

Резултатите от извършената проверка се съхраняват надлежно в архива на Доставчика.

11.6 Срок и прекратяване

Разпоредбите в настоящия документ, както и асоциираните с него Политики на предоставяне на КУ и удостоверителни услуги от Доставчика са валидни до издаване и публикуване на следваща тяхна версия/редакция в хранилището за документи на сайта на Доставчика.

Договорът за удостоверителни услуги между Доставчика и Потребител е със срок една година или до изтичане на срока на валидност на последното издадено по силата на договора удостоверение.

С прекратяване на дейността на Доставчика се прекратяват разпоредбите, Практиката и Политиките асоциирани с този документ.

В случай на недействителност на отделна клауза от този документ, валидността на целия документ се запазва и не се нарушава договора с Потребителя. Недействителната клауза се замества от повелителните норми на закона.

Договорът за удостоверителни услуги между Доставчика и Потребител се прекратява с изтичане на срока на валидност на последното издадено удостоверение по договора или с прекратяване на всички издадени удостоверения по договора.

Доставчикът съхранява надлежно и сигурно всички предишни версии на този документ и асоциираните с него Политики.

11.7 Уведомяване и комуникация между страните

Доставчикът използва изявления, писма и съобщения на РО/МРС както и електронни уведомления, които публикува на своята Интернет-страница.

Клиентите на B-Trust могат да изпращат съобщения, писма, препоръки, въпроси и жалби до Доставчика като използват следния адрес за контакти:

пощенски адрес: София 1612, бул. „Цар Борис III" 41

телефон: 0700 199 10

имейл адрес: info@b-trust.org

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

В случай на получаване на жалба, Доставчикът извършва незабавна проверка и изпраща отговор до жалбоподателя в срок от 2 работни дни.

11.8 Промени в Документа

Доставчикът може да прави редакционни промени в този документ, които не засягат съдържанието на правата и задълженията в него.

Промени, които водят до нова версия/редакция на документа се публикуват на Интернет страницата на Доставчика.

Промените се съобщават на КРС и заинтересуваните лица.

Всяко лице може да отправя предложения за промени и отстраняване на допуснати грешки, като използва посочените по-горе контакти с Доставчика.

11.9 Решаване на спорове и място (подсъдност)

Всички възникнали спорове между страните по договора за удостоверителни услуги се уреждат по споразумение между страните, чрез разбирателство и в дух на добра воля, а ако такова не бъде постигнато, се решават от компетентния български съд.

11.10 Приложимо право

За всички въпроси, неуредени в настоящия документ се прилагат разпоредбите на българското законодателство.

11.11 Съответствие с приложимото право

Настоящият документ е разработен в съответствие със ЗЕДЕУУ и действащата нормативна уредба.