Общодостъпен документ

B- TRUST КВАЛИФИЦИРАН ЕЛЕКТРОЕН ПОДПИС С ОТДАЛЕЧЕНО QSCD

(B-TRUST QUALIFIED ELECTRONIC SIGNATURE ON REMOTE QSCD)

КВАЛИФИЦИРАНА УСЛУГА „B-TRUST ОБЛАЧЕН КЕП“ НА ДКУУ „БОРИКА“ АД

(B-TRUST CLOUD QSCD SERVICE)

РЪКОВОДСТВО ЗА УСЛУГАТА

(SERVICE MANUAL)

Версия 1.0

Април 2018 г.

Хронология на измененията на документа				
Версия	**Автор (и)**	**Дата**	**Състояние**	**Коментар**
1.0	Димитър Николов	18.04.2017	Утвърден	Създаване на документа.

СЪДЪРЖАНИЕ

1 ОБХВАТ И УПОТРЕБА 3
2 ВЪВЕДЕНИЕ 4
3 ПРАВНИ АСПЕКТИ 5
4 СТАНДАРТИ/ТЕХНИЧЕСКИ СПЕЦИФИКАЦИИ ЗА ОТДАЛЕЧЕНО ПОДПИСВАНЕ 5
5 КОНЦЕПЦИЯ 6
6 КОНЦЕПТУАЛЕН МОДЕЛ 8
7 ФУНКЦИОНАЛЕН МОДЕЛ 11
7.1 Функционалност „Регистрация“ и „Издаване“ на Облачен КЕП 12
7.2 Функционалност „Управление“ на Облачен КЕП 14
7.3 Функционалност „Подписване“ с Облачен КЕП 14
8 ТЕХНИЧЕСКА СПЕЦИФИКАЦИЯ И РЕАЛИЗАЦИЯ 15

1 ОБХВАТ И УПОТРЕБА

Този документ:

- е разработен от „БОРИКА“ АД, юридическото лице, регистрирано в Търговския регистър към Агенцията по вписванията с ЕИК 201230426;
- съдържа изискванията за сигурност на услугата „Облачен КЕП“ (УСЛУГА) в съответствие с ЕС Регламент 910/2014 и приложимите технически за него спецификации EN 419 241-1/2/3, EN 419 221-5TS 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;
- не е публичен документ, но 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;
- служи за оценка на дейността на ДКУУ „БОРИКА“ АД да предоставя Облачен КЕП в съответствие с Регламент 910/2014;
- ползва или реферира технически спецификации относно УСЛУГАТА;
- може да бъде променян от ДКУУ и всяка нова редакция на този документ, отменя предишната такава.

Извън обхвата на документа са:

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

2 ВЪВЕДЕНИЕ

До утвърждаване и влизане в сила на ЕС Регламент 910/2014 (eIDAS), Титулярят на подписа (Signatory) трябваше да представи смарт карта с КЕП пред всяка услуга за подписване, изискваща правновалиден е-подпис. Смарт картата предоставя от една страна строго доказателство за идентичност и персонален контрол (sole control) за Титуляря, а от друга - функционалност за генериране на подписа в картата. Това изискване значително затруднява и прави финансово неефективно използването и управлението на смарт карти както за Потребителите (Титуляри и Доверяващи се страни) така и за Доставчици на КЕП, особено когато приложното поле на е-подписа рефлектира върху много Потребители. Крайният резултат за сега е ниско ниво на използването на смарт карти за електронно подписване с КЕП у нас (и в ЕС).

Регламент 910/2014 (eIDAS) въвежда важна алтернатива на смарт картите, като дава възможност на ДКУУ (TSP) да държат ключовете за подписи от името на своите потребители. Като рационализира правната и техническа рамка за е-подписа с цел хармонизиране и през гранична оперативна съвместимост на е-подписа, Регламентът запазва строгите технически изискванията към криптографските характеристики и функции за КЕП (QES), но в частност постановява:

(51) Следва да се предостави възможност титулярят на електронния подпис да възлага обслужването на устройства за създаване на квалифицирани електронни подписи на трета страна, при условие че са въведени подходящи механизми и процедури, гарантиращи, че титулярят разполага с едноличен контрол върху използването на данните, свързани със създаването на електронния му подпис, и че при използването на устройството са изпълнени изискванията по отношение на квалифицирания електронен подпис.

(52) Създаването на електронни подписи от разстояние, при което средата на създаване на електронен подпис се управлява от доставчик на удостоверителни услуги от името на титуляря на електронния подпис, се очаква да се развие поради многобройните икономически предимства, които предоставя. При все това, с цел да се гарантира, че тези електронни подписи получават същото правно признаване като електронните подписи, създавани в среда, изцяло управлявана от потребителя, доставчиците, които предлагат услуги на електронен подпис от разстояние, следва да прилагат специфични процедури за сигурността на управление и административната сигурност и да използват надеждни системи и продукти, включително сигурни електронни канали на комуникация, с цел да се гарантира надеждността на средата на създаване на електронния подпис и да се гарантира, че тази среда е използвана единствено под контрола на титуляря на електронния подпис. В случай на квалифициран електронен подпис, създаден чрез устройство за създаване на електронен подпис от разстояние, следва да се прилагат изискванията, приложими за доставчиците на квалифицирани удостоверителни услуги, които са изброени в настоящия регламент.

Допускането и утвърждаването на такава функционалност е известно като отдалечено подписване (Remote signing, Server Signing, Cloud Signing). Вместо да подписват със смарт карти, потребителите могат да работят с отдалечена услуга за подписване, която включва сертифициран HSM. Чрез отдалечено подписване, потребителите могат безопасно да въвеждат своите идентификационни данни и да подписват документи с помощта на телефон, браузър или друго устройство.

Сертифицираният HSM като отдалечено QSCD (Remote QSCD) поддържа услугата за отдалечено подписване като изпълнява следните функции:

- Сигурно криптира/защитава авторизационните данни (пълномощия) за потребителите;
- Създава и съхранява ключ за подписване за всеки потребител

- Гарантира, че документ ще бъде подписан само с ключът за подписване (частния ключ) на автентичния потребител, т.е. този ключ е под персонален контрол (sole control) на подписващия.

В близката перспектива, преобладаващият подход за отдалечено подписване ще бъде чрез HSM и мобилни устройства (смартфони, таблети, др.).

3 ПРАВНИ АСПЕКТИ

Регламентът eIDAS въвежда правни норми (законодателство), които зависят от четири елемента и гарантират надеждността/доверието на услугите за отдалечено подписване,:

- Сертифициран HSM като отдалечено QSCD, който държи подписващия (частния) ключ на потребителя;
- Активиране на подпис - процесът на удостоверяване и активиране на ключове; важно е за да се гарантира, че тази функционалност е под персонален контрол (sole control) на потребителя по всяко време. Сигурността на активирането подписа зависи от функционалност, която се предоставя от външно приложение или от вътрешен код в HSM, като тези две опции визират съответно ниво 1 и ниво 2 на сигурност на персоналния контрол (според техническите спецификации за отдалечено подписване в съответствие с Регламента);
- Сигурност на персоналното устройство на потребителя; персонални устройства като смартфони трябва да бъдат защитени от злонамерен софтуер и да имат контролиран достъп, например чрез използване на ПИН код. Ако смартфонът съхранява ключът за автентификация или биометрична информация, може да е необходим елемент на доверие.
- ДКУУ (TSP), който оперира/управлява услугата за отдалечено подписване, като част от по-широк спектър квалифицирани удостоверителни услуги на този Доставчик. Регулярните одити гарантират доверието и надеждността на ДКУУ. Тези одити оценяват сигурността на цялата инфраструктура на Доставчика, включително физическите и операционните мерки и способността на ДКУУ да изпълни очакваните функционални изисквания на услугата за отдалечено подписване.

Три от посочените по-горе четири елемента се обезпечават чрез следните две изисквания в Регламента:

- Приложение II (Изисквания към устройствата за създаване на квалифициран електронен подпис) и разширенията, предоставяни от техническите спецификации EN 419 241-1/2/3 и EN 419 221-5;
- Изискванията ДКУУ да подлежат на регулярен одит (Чл. 20, Надзор на ДКУУ).

4 СТАНДАРТИ/ТЕХНИЧЕСКИ СПЕЦИФИКАЦИИ ЗА ОТДАЛЕЧЕНО ПОДПИСВАНЕ

В подкрепа на услугата за отдалечено подписване с КЕП, в съответствие с Регламент 910/2014 (eIDAS) са публикувани следните решения и технически стандарти/спецификации:

- РЕШЕНИЕ ЗА ИЗПЪЛНЕНИЕ (ЕС) 2016/650 НА КОМИСИЯТА от 25 април 2016 година за определяне на стандарти за оценка на сигурността на устройствата за създаване на квалифициран електронен подпис и печат съгласно член 30, параграф 3 и член 39, параграф 2 от Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета;
- ETSI TS 419 241 (Server Signing);
- ETSI EN 419 241-1, базиран на TS 419 241;
- ETSI EN 419 241-2 PP TSCM;
- ETSI EN 419 241-3 PP SAD+SAM (PP Signature Activation Module for Remote QSCD).

Законовото изискване по Регламент 910/2014 (eIDAS) за отдалечено подписване понастоящем е двусмислено. Решение ЕС 2016/650 относно Регламента за приложение на устройства за квалифицирано подписване и създаване на печати изисква сигурност, която е сравнима със сертифицирана смарт карта, докато Комисията не приеме специфични стандарти за отдалечено подписване. В частност, посочената в Решението спецификация EN 419 211 - Защитни профили за устройство за защитено създаване на подписи, части 5 и 6 може се прилага (частично) при оценка на услуга за отдалечено подписване, докато не бъдат утвърдени съответните стандарти и спецификации.

ETSI EN 419 241-1, който се базира на TS 419 241 определя две нива на „сигурност на персонален контрол" (sole control assurance).

Ниво 1 се основава на приложение за подписване в сървър (Server Signing Application/SSA), което да гарантира, че е избран съответния (частен) ключ за подпис. Функционалността, която поддържа активирането на подписа и осигурява персонален контрол чрез т.н. „делегирана" автентификация, се изпълнява като част от SSA в сървъра . Може да се използва всеки HSM, сертифициран като QSCD в съответствие с Регламента (например, съгласно EN 419 221-5).

С цел да се гарантира Ниво 2 на сигурен персонален контрол, активирането на подпис трябва да се извършва чрез код (SAM/Signature Activation Module или SCC/Sole Control Code) в HSM. Този код е сертифициран за същото ниво на сигурност както общите криптографски функции на HSM. Данните за активиране на подписа се предават в защитена форма от персоналното устройство на подписващия на SAM/SCC в HSM, за да се гарантира, че ключа за подпис (частния ключ) на потребителя е под персонален контрол и не може да бъде злоупотребен, дори ако SSA в сървъра на ДКУУ е компрометирана.

Обхватът на EN 419 241-2 (PP TSCM) покрива изискванията за сигурност (защитен профил/PP на отдалечената част (SAM/SCC+HSM, при ДКУУ), т.е. на „отдалеченото" QSCD (Remote QSCD), които са еквивалентни на тези съгласно Приложение II на Регламента.

EN 319 241-3 (PP SAD+SAP) специфицира изискванията за сигурност (защитен профил/PP) относно управлението на SAD (Signature Activation Data management) и на оперирането на SAP (Signature Activation Protocol), съответстващи с Приложение II към Регламент № 910/2014, за да се гарантира Ниво 2 на „сигурност на персонален контрол" (sole control assurance) на Титуляря/Създателя на подпис/печат върху отдалеченото QSCD (Remote QSCD).

Двете части на EN 419 241-2/3 и EN 419 221-5 заедно сертифицират „системата/устройството" за отдалечен квалифициран електронен подпис/печат (Remote QSCD) и кореспондират с изискванията в Регламент № 910/2014 на ЕС относно КЕП (QES): *данните за създаване на електронен подпис са надеждно защитени от легитимния Титуляр (персонален контрол) срещу използването им от други лица, докато генерирането и управлението на данните за създаване на подпис (частния ключ) се извършва от квалифициран доставчик на доверителни услуги от името на подписващия/Титуляря*.

5 КОНЦЕПЦИЯ

Картовият КЕП (на смарт карта) като правно валиден е-подпис отговаря на три задължителни условия/изисквания съгласно ЕС Регламент 910/2014 : (1) частния ключ да бъде сигурно съхраняван и защитен в QSCD, (2) да е под персонален контрол само на Титуляря (Signatory) и съответстващото му удостоверение да е квалифицирано. Първите две изисквания за сигурен КЕП, визирайки неявно смарт карта като QSCD, са в конфликт с по-удобното, по-лесно и финансово изгодно прилагане и ползване в практиката на правно валидния е-подпис, т.е. възпрепятстват неговото разпространението (дори при сегашния ограничен брой на е-услуги!).

Дилемата „сигурен КЕП – удобно и лесно ползване“ рефлектира най-вече върху Титуляря, но влияе и на другите страни в процеса на подписване – Доставчици на е-услуги и Доверяващи се страни и ДКУУ/TSP (Trusted Service Provider).

Концепцията „Облачен/Сървърен КЕП“ отстранява тази дилема/конфликт като предоставя централизирано съхранение и управление/поддръжка на частните ключове (за е-подпис) при ДКУУ/TSP в среда с висока степен на сигурност и строги административно-оперативни процедури с физическа и логическа защита. Титулярят (Signatory) запазва пълен и персонален контрол (full and sole control) върху своя частен ключ чрез сигурен/защитен 2FA (2-Factor Authentication) механизъм за онлайн автентификация (TOTP/Time-based One-Time-Password). Когато този механизъм се имплементира чрез мобилно устройство (смартфон с мобилно приложение или таблет), Титулярят получава „мобилност“ на КЕП.

„Мобилността“ като характеристика на Облачния КЕП не означава, че той се генерира в съответното мобилно устройство (смартфон, таблет, др.), то само служи да инициира създаването на КЕП в отдалечена сървърна платформа, която е под контрола на ДКУУ. „Мобилността“ адресира Титулярят (Signatory), който вече е „освободен“ от специфичните технически изисквания да ползва КЕП (да има смарт карта и четец и да инсталира съответните драйвери за тях), като запазва/гарантира същите правни и технически изисквания за сигурността на правно валидния е-подпис.

„Облачният КЕП“ е концепция, която „премества“/виртуализира локално QSCD за КЕП (смарт картата на Титуляря/Signatory) в HSM на сървърна платформа. В HSM-а на сървъра, в ролята на ‘Remote QSCD’ се алокира ‚виртуален слот‘ като отдалечен ресурс на Титуляря с еквивалентни криптографски параметри и характеристики на локално QSCD (смарт карта). Физическата дистанция относно персонален контрол на Титуляря върху неговото “Remote QSCD” се ‘компенсира’ като се използват два отделни комуникационни канала – през Internet и мобилната мрежа/комуникация, чрез които се имплементира 2FA (TOTP двуфакторна автентификация) на Титуляря (Signatory) и се активира създаване/генериране на КЕП с ПИН-код, тоест се поддържат елементи на SAP (Signature Activation Protocol) и на SAD (Signature Activation Data).

2FA механизмът (‘нещо което притежавам + нещо което знам’) в концепцията „Облачен КЕП” изпълнява аналогична роля за персонален достъп до данните за създаване на подписа (т.е. частния ключ), както ПИН-кода при картовия КЕП (КЕП на смарт карта), т.е. персонално автентифицира Титуляря. В случая, техническия фактор ‘притежавам смарт карта’ се замества от ‚притежавам регистриран смартфон’, а персоналният фактор ‘знам PIN’ се замества от ‘знам Парола/PIN за подписване’, които са под персонален контрол единствено (само) на Титуляря, когато се създава/генерира КЕП (в HSM-а на сървъра). Факторът ‘притежавам’ се гарантира от инсталирано и инициализирано мобилно приложение в смартфона, идентифициращо смартфона на Титуляря с уникален ID (App_ID), а факторът ‘знам’ – чрез криптирана сесия и криптирани данни за активация (ПИН) в потребителския интерфейс на Титуляря до сървъра с HSM. HSM-ът в сървъра ще генерира КЕП само след успешна автентификация на Титуляря пред сървиса за подписване и на този сървис пред HSM-а („делегирана“ автентификация) чрез двата фактора – TOTP-кода и ПИН-кода по двата независими ‘канала’ (Интернет и мобилен Интернет).

Концепцията за „Облачен КЕП“ като ‘премества’ локално QSCD на Титуляря в ‘Remote QSCD’ на HSM в сървъра, изисква допълнителни организационно-технически процедури, които гарантират двуфакторен механизъм за автентификация и защита на данните за създаване на КЕП, с ниво на сигурност еквивалентно с това за локалното QSCD (смарт картата).

Съгласно тази концепция, ‘Облачен КЕП’ означава КЕП на Титуляр (Signatory), който използва смартфон с мобилното приложения и мобилен Интернет за да инициира отдалечено създаване/генериране на КЕП в сървърна платформа с HSM под управление на ДКУУ посредством ‚делегирана‘ двуфакторна автентификация за Титуляря.

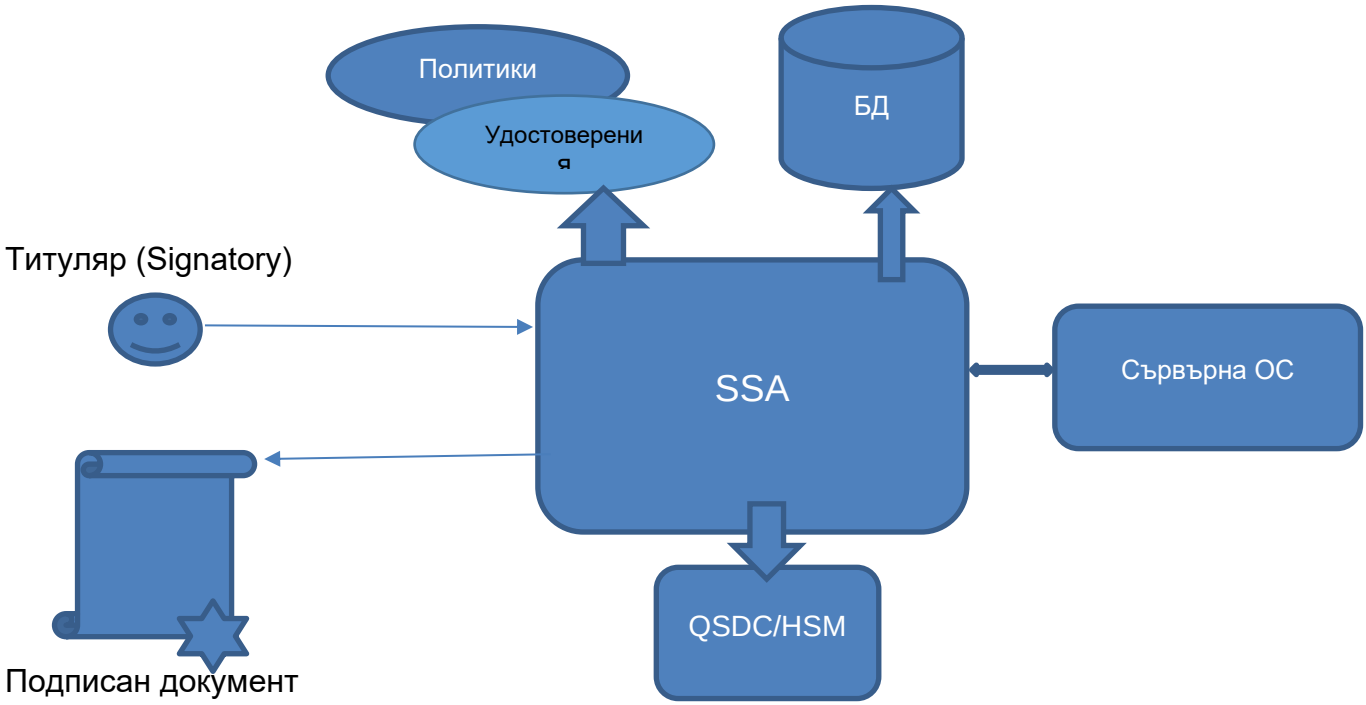
Създаването/генерирането на Облачен КЕП свежда локалната среда на Титуляря до:

- стандартен браузер в PC с Интернет-достъп;
- смартфон с инсталирано и инициализирано мобилно приложение, успешно регистрирано в сървърната платформа с HSM при ДКУУ.

Отпада потребността от комплект за КЕП (смарт карта, четец и драйвери) както и инсталация и поддръжка на софтуера от комплекта за КЕП при клиента.

6 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

Съгласно Модела на Фиг.1 данните за създаване на подписа (частния ключ) се съхранява в криптомодул (HSM) на отдалечения сървър.

Стандартен подход да се идентифицира Титуляря и да получи достъп до данните за създаване на подписа (частния ключ) може да бъде използване на Име/Парола и защитена сесия (SSL/TLS) до сървъра. Такъв подход създава проблеми:

a) Име/Парола е уязвим метод на различни атаки (като phishing or replay attacks) и не се приема като сигурен за персоналния контрол;

b) Ако SSL/TLS сесията се терминира извън HSM-а, Паролата е в явен вид в отдалечения сървър и е уязвима (memory snapshots) от страна на (злонамерен) системен администратор.

За да се предотврати (а), се препоръчва да се въведе по-силна автентификация на Титуляря, т.е. да се въведе двуфакторно удостоверяване, където паролата представлява един фактор. Вторият фактор може да бъде метод за (за предпочитане) динамично удостоверяване, базиран на напр. OTP. Това предполага, че към решението следва да се въведе надежден 2-факторен механизъм.

При (б) следва да се гарантира, че (i) нито един системен администратор не може да получи достъп до частния ключ или (ii) да използва този ключ.

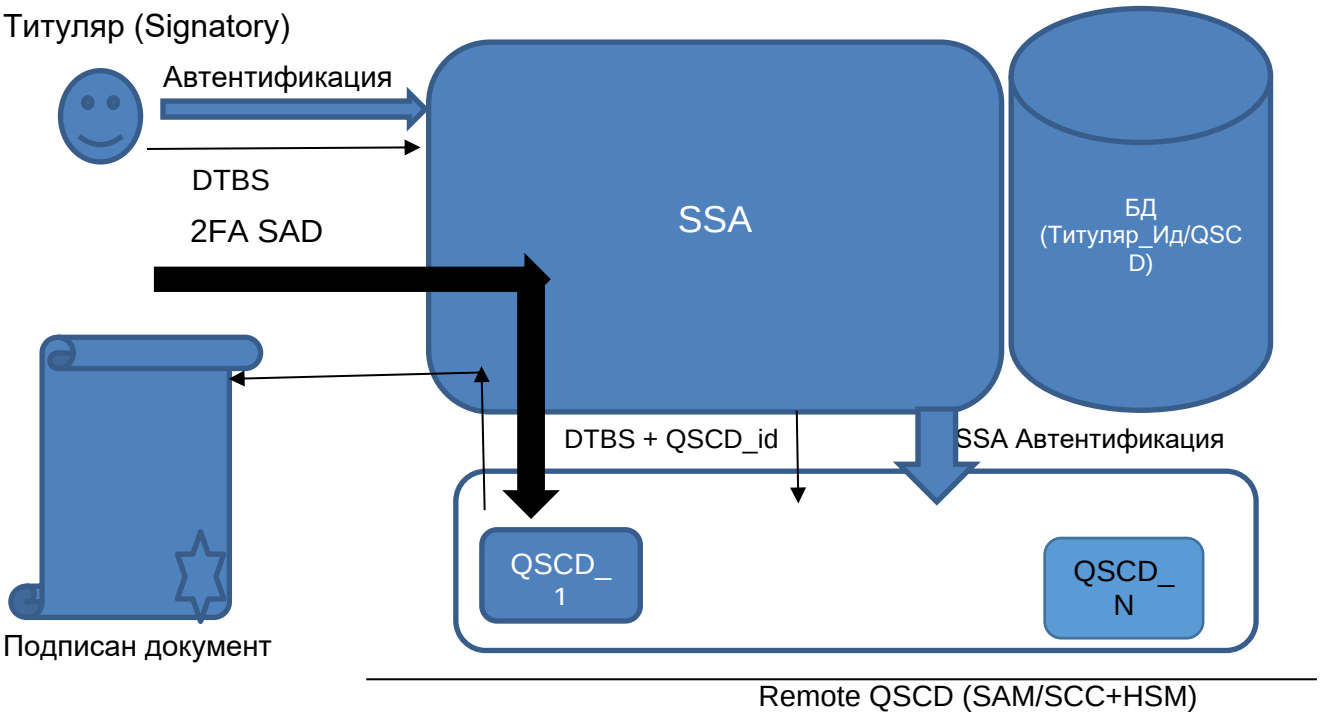
Частният ключ е защитен в HSM, така че трябва ключът да не се появява в явен вид извън HSM, т.е. (i) е изпълнено.

Казусът (ii) се решава по различни начини:

- Дуален контрол на физическия и логически достъп до HSM, така че един администратор да не може да подписва данни от името на Титуляря;
- 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, като например парола/ПИН-код или OTP);

- Частният ключ на Титуляря може да бъде приложен само към (хеш) данни, които са удостоверени от него.

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).



Фиг. 3 Концептуален модел – Ниво II на сигурност на персонален контрол

Активирането на подпис се извършва чрез код (SAM/Signature Activation Module или SCC/Sole Control Code) в HSM. Този код е сертифициран на същото ниво на сигурност както общите криптографски функции на HSM. Техническият стандарт EN 419 241-3 (PP SAD+SAP) специфицира защитения профил на отдалеченото QSCD (Remote QSCD), базирано на QSCD с имплементиран код (SAM/SCC) в него.

Данните за активиране на подписа се предават в защитена форма директно от персоналното устройство (PC, смартфон, таблет, др.) на подписващия до SAM/SCC в HSM, чрез сигурен/защитен канал за да се гарантира персонален контрол на Титуляря върху ключът за подписа (частния ключ) и невъзможност за злоупотреба с този ключ, дори ако SSA в сървъра на ДКУУ е компрометирана.

В практическата реализация на концепцията за Облачен КЕП, ДКУУ „БОРИКА“ АД следва концептуалния модел за облачен КЕП с Ниво I на сигурност на персонален контрол на данните за активация на е-подписа (Фиг. 2). Ниво 1 на сигурност на персоналния контрол в този модел се имплементира чрез т.н ‚делегирана‘ автентификация (Титуляр пред SSA и SAA пред HSM). Моделът е разширение на този от Фиг.1 чрез използване на два отделни комуникационни канала. Един комуникационен канал, обикновено през Интернет, се използва за подготовка на документи и изпращане на удостоверена заявка за подпис на услугата за подписване (SSA), а друг комуникационен канал, обикновено ползващ мобилна мрежа (мобилен Интернет), се използва за потвърждаване на тази транзакция с помощта на личното устройство (смартфона).

7 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.

Подсистемата за Издаване на Облачния КЕП използва възможно най-пълно текущата имплементация на B-Trust платформата, чрез която се издава и поддръжка на картовия КЕП (КЕП на смарт карта) както и свързаните с него удостоверителни услуги - издаване, подновяване и управление (подновяване, спиране/възобновяване и прекратяване/отмяна) на удостоверения за КЕП.

Поддръжката/управлението на Облачен КЕП се имплементира изцяло чрез съществуващата функционалност на B-Trust Портала за поддръжка/управление на картовия КЕП (то-точно, на квалифицираните удостоверения за картов КЕП) и не ползва Платформата за Облачен КЕП (конкретно, SSA и HSM-а в нея).

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 „Регистрация“ и „Издаване” на Подсистемата за Издаване използва следните работещи компоненти на B-Trust инфраструктурата:

- Удостоверяващ орган - издава квалифицирани удостоверения в съответствие с ЕС Регламент 910/2014;
- B-Trust Портал – с допълнителен web-интерфейс към Подсистемата за Издаване на Облачен КЕП;
- Публичен регистър и CRL на квалифицирани удостоверения (LDAP-сървър).

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.

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

Информацията в тази част на документа следва да се ползва съвместно с информацията в т.3 (т. 3.2) и т.4 (т.т. 4.1, 4.2, 4.3, 4.4 и 4.5) на документа B-Trust CPS-eIDAS.

Заявителят на удостоверителната услуга Облачен КЕП следва да регистрира искане (е-форма) за издаване на квалифицирано удостоверение за Облачен КЕП пред ДКУУ „БОРИКА“ АД. Допустими са следните варианти (канали) за регистриране на искане за издаване на Облачен КЕП:

(1) Онлайн първоначално искане, от смартфон;

(2) Онлайн първоначално искане, от браузър на PC чрез уеб сайта B-Trust на ДКУУ и последващо посещение на офис на ДКУУ;

(3) Офлайн първоначално искане, на място в офис на ДКУУ чрез Агент-служител на Доставчика;

(4) Онлайн искане от браузър на PC чрез уеб сайта B-Trust на ДКУУ и издадено валидно удостоверение за КЕП (картов).

Сравнително големият обем данни за попълване в е-формата при първоначално искане за издаване на Облачен КЕП прави неудобен и тромав вариант (1) и не се поддържа (за сега) от ДКУУ „БОРИКА“ АД.

Варианти (2) и (3) са сходни, с тази разлика, че при вариант (3) е-формата на искането за първоначално издаване на Облачен КЕП се попълва от Агент в офиса на Доставчика в присъствие на Заявителя/Титуляря.

Изисквания към Заявителя/Титуляр:

- Смартфон (мобилна платформа Android или iOS) с мобилен Интернет;
- Персонален компютър с Интернет достъп;
- Документ(и) за самоличност;
- Да посети удобен за него офис на Доставчика;
- Регистрационен номер на онлайн искане за Облачен КЕП (предоставя се от B-Trust Портала);
- Заредено и инициализирано/персонализирано мобилно приложение B-Trust Mobile в смартфона(*)

(*) Информация за зареждане и инициализиране/персонализиране на мобилното приложение B-Trust Mobile се съдържа в документа “B-Trust Мобилно приложение за Облачен КЕП – Ръководство на Потребителя” (B-Trust Mobile application B-Trust Mobile – User Manual). Инициализацията/персонализация на B-Trust Mobile създава уникален ID (App_ID) и парола и го регистрира във WS на Подсистемата за Издаване на Платформата за Облачен КЕП.

Вариант (2) включва:

- Заявителят попълва онлайн е-формата (пълна или частично) и прави заявка за издаване на Облачен КЕП. Подава заявката като я изпраща към WS от Application layer на Подсистемата за Издаване, заявката се записва в база данни (за Облачен КЕП) и Заявителя получава номер на заявка;
- Заявителят посещава офис на Доставчика, където се извършва идентификация на Заявителя/Титуляря – предоставят се необходимите документи, извършва се заплащане;
- Агентът допълва заявката с необходимата информация, потребителя се съгласява със съдържанието на удостоверението за бъдещия Облачен КЕП и Агентът утвърждава заявката, която се запива в база данни за Облачен КЕП със статус „Pending";
- WS на Подсистемата за Издаване връща QR-код на екрана на Агента след записа в базата данни;

- Заявителят сканира QR-кода със смартфона съдържаш URI; мобилното приложение адресира това URI като изпраща App_ID и получава инициализираща структура с данни (2FA Shared Secret Key, крипто ключ за ПИН-а, както и акаунт-информация за Заявителя); двата ключа се и се съхраняват криптирани с паролата в мобилното приложение;
- В следваща страница в браузъра на Агента се получава покана да се въведе TOTP-код на 2FA на смартфона за проверка за притежание/държане на смартфона от страна на WS в Подсистемата за Издаване;
- В страницата на браузъра се въвежда генерирания TOTP-код от B-Trust Mobile и се изпраща на WS, където се проверява; с това приключва проверката за притежания на смартфона;
- Платената заявка за издаване на Облачен КЕП преминава в статус „Confirmed”; WS на Подсистемата за Издаване изпраща push нотификация към мобилното приложение;
- Изисква се да се въведе ПИН за Облачен КЕП, който се криптира с съхранявания крипто ключ за ПИН в мобилното приложение; криптирания ПИН се предава на WS в Подсистемата за Издаване и участва в процеса по генериране на двойката ключове за Облачен КЕП и създаване на публичните криптограми за Облачен КЕП чрез HSM-а на сървърната компонента в Платформата за Облачен КЕП;
- Генерира се двойката ключове за Облачен КЕП и се създават публичните криптограми за Облачен КЕП чрез HSM-а (Виж ПРИЛОЖЕНИЕ 4 на документа); Криптограмите EK_sig и EK_user се асоциират с и се записват в таблица към съответното APP_ID на базата данни;
- публичният ключ за Облачния КЕП участва в следващите процедури на B-Trust платформата за издаване на квалифицирано удостоверение за КЕП (формира се PKCS#10/CSR заявка, генерира се и се подписва издаденото удостоверение за тази заявка от УО на B-Trust, публикува се издаденото удостоверение в Публичния регистър);
- WS на Подсистемата за Издаване изпраща push нотификация към мобилното приложение или потребителят сам проверява статуса на заявката в мобилното приложение за издаден Облачен КЕП.

Вариант (4):

Този вариант е разработен и се поддържа с цел да се улесни и да се ускори прехода/трансформацията от вече издаден и валиден картов КЕП към Облачен КЕП за Титуляри, които желаят този преход и не следва да посещават офис на Доставчика. Целта е ускорено разширение на приложното поле на Облачния КЕП сред Потребители и Доставчици на е-услуги с оглед на удобството и предимствата, които предоставя на страните, ползващи е-подпис.

Функционалността при този вариант е различна от тази на предишния вариант само в първите четири стъпки:

- Титуляр на валиден картов КЕП адресира B-Trust WEB уеб сайт в браузъра на PC. Автентифицира се с картовия си КЕП (двустранна SSL сесия). Квалифицираното удостоверение за този КЕП се извлича от сесията и удостоверените в него данни се предоставят за следващите стъпки;
- В браузъра се показва известната информация за Титуляря на картовия КЕП като автоматично се попълва форма, на базата на която се прави заявка за Облачен КЕП. Някои от данни могат да се променят, може да се добавя допълнителна информация (идентификатори, нужни при процеса на използване);
- След редакция (ако е необходимо) заявката за издаване на Облачен КЕП се записва в база данни (акаунт) за Облачен КЕП. Потребителят получава номер на заявка за мобилен КЕП;
- Следват същите стъпки от вариант (2), с тази разлика, че страниците в браузъра се получават на PC-то на Титуляря, заявител на Облачен КЕП.

7.2 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 1 (една) година. След този срок на валидност, Титулярят на облачен КЕП може да заяви издаване на нов такъв.

Смяна на ПИН на издаден Облачен КЕП не се поддържа (за сега).

Не се подържа (засега) разблокиране на блокиран потребителски ПИН на Облачен КЕП.

Посочената по-горе функционалност на „Управление/Поддръжка“ на Облачен КЕП се изпълнява от стандартната B-Trust платформа за КЕП, следвайки условията и процедурите за управление на картов КЕП. Виж документ “ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ И УДОСТОВЕРИТЕЛНИ УСЛУГИ ЗА ТЯХ ОТ „БОРИКА” АД” (B-Trust CPS-eIDAS)“, т. 3 (т.т. 3.4, 3.5, 3.6) и т.4 (т.т. 4.8, 4.9, 4.10).

7.3 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).

Формирането на контейнера на е-подписа е извън обхвата на Платформата за облачен КЕП. Тази функционалност е част от приложни системи на Доставчиците на е-услуги и/или на Доставчици, опериращи платформи за подписване (Signing Services).

Документ за подписване (може да) се съхранява на приложен (корпоративен) сървър или локалната система (PC) на Титуляря. С цел конфиденциалност, в Подсистемата за Подписване се предоставя хеш-данна за документа за подпис.

Функционалност „Подписване“ на Платформата за Облачен КЕП включва:

- Потребителят адресира уеб-сайт на Доверяваща се страна и избира да подпише е-документ; избира опция за подписване с Облачен КЕП и въвежда четим PROFILE_ID (генериран на базата на APP_ID), предоставен от мобилното му приложение;
- Приложната система на Доверяващата се страна формира хеш на документа и извежда страница в браузъра на Титуляря с хеша на документа и поле за въвеждане на TOTP-код;
- Потребителят въвежда TOTP, генериран от мобилното приложение;
- Приложната система на Доверяваща се страна редиректва Титуляря към Подсистемата за Използване в сървърната компонента на Платформата за Облачен КЕП с параметри – идентификатора, TOTP, хеш-данната и адрес за връщане (callback URL) към Доверяваща се страна;
- TOTP се проверява от WS на Подсистемата за Използване; WS изпраща push нотификация към мобилното приложение с информация за чакащия за подписване документ (хеша);
- Мобилното приложение взема документа за подписване от WS на Подсистемата за Използване;

- Потребителят преглежда/сравнява хеш на документа и потвърждава подписването като въвежда ПИН;
- Мобилното приложение изпраща потвърждението за подписване към WS на Подсистемата за Използване, заедно с криптиран ПИН на Облачния КЕП;
- Чрез въведения ПИН и крипто-схемите се изпълняват криптографските операции и се генерира цифров подпис (PKCS#1) в HSM-а на Подсистемата за Използване (Виж ПРИЛОЖЕНИЕ 4 на документа);
- WS на Подсистемата изпраща асинхронно генерирания цифров подпис (PKCS#1) заедно с квалифицираното удостоверение на Облачния КЕП към Доверяващата се страна, инициирала подписването;
- Информация за подписания документ се визуализира в страницата на Доверяващата се страна за Титуляря.

8 ТЕХНИЧЕСКА СПЕЦИФИКАЦИЯ И РЕАЛИЗАЦИЯ

Практическата реализация на услугата за Облачен КЕП се имплементира съгласно функционалният модел в Глава 7 на документа чрез Платформа за Облачен КЕП.

Доставчикът планира развитие на квалифицираната услуга Облачен КЕП чрез подмяна HSM-а (сертифициран съгласно Регламента за ниво на сигурност CC EAL 4+, EN 419 221-5) в Платформа за Облачен КЕП с “Remote QSCD” (HSM + SAM/SCC код), който ще се сертифицира за същото ниво на сигурност, но и в съответствие с EN 419 241-2/3.