Общодостъпен документ

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

B-TRUST CLOUD QES/REMOTE QSCD SERVICE

(CQES/RQSCD)

РЪКОВОДСТВО ЗА УСЛУГАТА

(SERVICE MANUAL)

Версия 2.0

1 Март 2020 г.

Хронология на измененията на документа				
Версия	**Автор (и)**	**Дата**	**Състояние**	**Коментар**
1.0	Димитър Николов	18.04.2017	Утвърден	Създаване на документа.
2.0	Димитър Николов	01.03.2020	Утвърден	Корекции на текстове

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;
- 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 419 221-5 и ETSI TS 119 431 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:

- Техническите аспекти на формати, синтаксисът, кодировката на е-подписа, конкретните формати, профили и кодировка на контейнера на подписани документи с облачен КЕП;
- Процесите на подписване, т.е. генерирането на контейнера на квалифицирания облачен КЕП;
- Правната приложимост (правила за приложимост) на дългосрочно съхраняван квалифициран облачен КЕП за различни бизнес-цели;

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 да подписват с облачен КЕП при ДКУУ, която включва сертифициран HSM. Чрез отдалеченото подписване, потребителите безопасно въвеждат своите идентификационни данни и подписват документи с помощта на телефон, браузър или друго устройство.

Сертифицираният HSM (QHSM) с подходяща софтуерна среда при ДКУУ като отдалечено QSCD (Remote QSCD/RQSCD) поддържа услугата за облачен КЕП като изпълнява следните функции:

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

- Гарантира, че документ ще бъде подписан само с ключът за подписване на оторизирания потребител, т.е. този ключ е под персонален контрол (sole control) на подписващия;
- Генерира цифровия подпис (PKSC#1)

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

3 ПРАВНИ АСПЕКТИ

Регламентът eIDAS въвежда правни норми, които определят следните фактори, гарантиращи надеждността/доверието на услугите за отдалечено подписване:

- Сертифициран HSM като отдалечено QSCD, който държи подписващия (частния) ключ на Потребителя;
- Активиране на подписа - процесът на удостоверяване и последващо активиране на частния ключ; важно е за да се гарантира, че този процес е под персонален контрол (sole control) на Потребителя по всяко време. Сигурността на активирането частния ключ 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 смарт 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 фактор доверие.
- ДКУУ (TSP), който оперира/управлява услуга за отдалечено подписване, като част от по-широк спектър квалифицирани удостоверителни услуги на този Доставчик. Регулярният одит гарантира доверието в 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 фактора се обезпечават чрез съдържащите се две изисквания в Регламента:

- Приложение II (Изисквания към устройствата за създаване на квалифициран електронен подпис) и допълненията, предоставяни от техническите спецификации EN 419 241-1/2/3 и EN 419 221-5 и тези на ETSI TS 119 431-1/2 и TS 119 432;
- Изискването ДКУУ да подлежи 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 119 431-1/2 - TSP service components operating a remote QSCD;
- ETSI TS 119 432 - Protocols for remote digital signature creation;
- 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).

ETSI TS 119 431-1 определя изискуемите компоненти на платформата за генериране на (цифров) подпис от разстояние (RQSCD) при ДКУУ, докато ETSI TS 119 431-2 – компонентите за създаване на контейнера на Облачен КЕП, т.е. на подписания документ с Облачен КЕП. Двете части на този документ заедно позволяват ДКУУ да специфицира, изгради и оперира цялостна услуга за подписване на е-документи (даннови обекти) от разстояние с Облачен КЕП.

ETSI TS 432 определя протоколите на взаимодействие (обмен) на приложна платформа с платформа за отделечено подписване на е-документи (даннови обекти) с Облачен КЕП.

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

Ниво 1 се базира на защитен сървис за подписване в сървър (Server Signing Application Service/SSAS с HSM) при ДКУУ, който 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 SSAS сървиса 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 подписа 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 смарт-устройство на подписващия на SAM/SCC в HSM, за да се гарантира персонален контрол върху ключа за подписване, без да бъде нарушен, дори ако компонентата SSAS в сървъра на ДКУУ е компрометирана.

ETSI EN 419 241-2 (PP TSCM) покрива изискванията за сигурност (защитен профил/PP) " на „отдалеченото QSCD" (Remote QSCD) (SAM/SCC+HSM), 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), за да се гарантира Ниво 2 на „сигурност на персонален контрол" (sole control assurance) на Титуляря в съответствие с Приложение II към Регламент № 910/2014.Двете части на EN 419 241-2/3 и EN 419 221-5 заедно сертифицират „системата/устройството" за отдалечен квалифициран електронен подпис (Remote QSCD/RQSCD) 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 (3) съответстващото му удостоверение да е квалифицирано. Първите две изисквания за сигурен КЕП, визирайки неявно смарт картата 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 разпространение.

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 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 активира създаването на КЕП в отдалечена сървърна платформа (RQSCD) на ДКУУ. „Мобилността“ адресира Титуляря (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 смарт картата (локално QSCD) за КЕП на Титуляря/Signatory в HSM на сървърна платформа (RQSCD) при ДКУУ. В RQSCD се алокира ‚виртуален слот‘ като отдалечен ресурс на Титуляря с еквивалентни криптографски параметри и характеристики на смарт картата (локално QSCD). Физическата дистанция на Титуляря с неговото “Remote QSCD” относно персоналния контрол се ‘компенсира’ чрез използване на два отделни комуникационни канала – през Internet и мобилната мрежа, които се използват за автентификация (2FA) на Титуляря (Signatory) и за активиране създаването/генерирането на подписа с ПИН-код. Чрез дуалност на комуникационните канали се поддържат характеристики на SAP (Signature Activation Protocol), на SAD (Signature Activation Data) и на SAM (Signature Activation Module) съгласно посочените технически спецификации в т.4 на документа.

2FA механизмът (‘нещо което притежавам + нещо което знам’) в концепцията „Облачен КЕП” изпълнява аналогична роля за персонален достъп до и контрол на данните за създаване на подписа (т.е. на 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 подписа в HSM-а на сървъра (RQSCD). Факторът ‘притежавам’ се гарантира от инсталирано и активирано мобилно приложение в смартфона, идентифициращо смартфона на Титуляря с уникален ID (App_ID), а факторът ‘знам’ се гарантира чрез криптирани данни за активация (ПИН) в криптирана сесия на Титуляря до сървъра с HSM (RQSCD). HSM-ът в сървъра ще генерира КЕП само след успешна автентификация на Титуляря пред SSAS, респективно пред HSM-а („делегирана“ автентификация) чрез двата кода – TOTP-кода за 2FA и ПИН-кода за частния ключ по двата независими ‘канала’ (Интернет и мобилен Интернет).

Концепцията за „Облачен КЕП“ като ‘премества’ смарт картата (локално QSCD) на Титуляря в RQSCD (HSM в сървъра) на ДКУУ, 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 смарт картата (локалното QSCD).

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

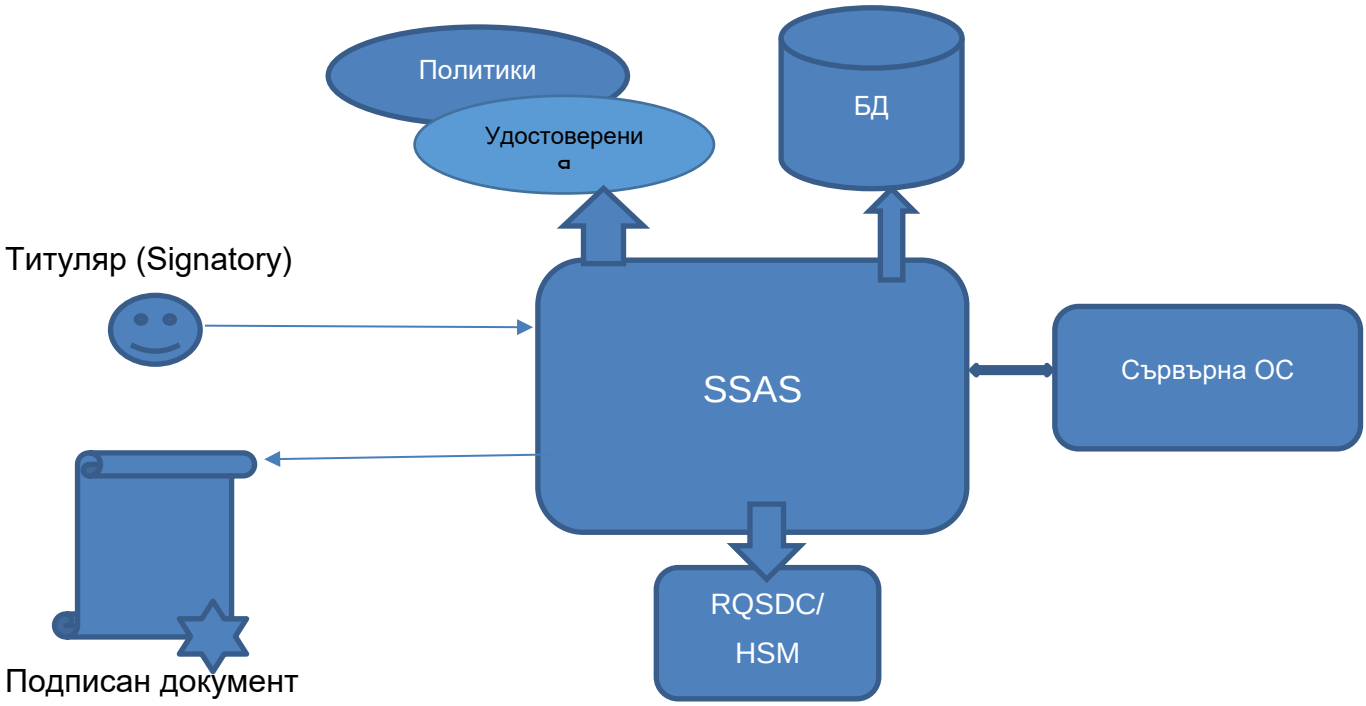
Създаването/генерирането на Облачен КЕП свежда локалната среда на Титуляря до:

- стандартен браузер в PC с Интернет-достъп;
- смартфон с инсталирано и инициализирано мобилно приложение, успешно регистрирано в RQSCD (сървър с SSAS и 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 RQSCD в модела се изпълнява от сървиса SSAS и HSM-а на сървъра при Доставчика. Отсъстват организационно-техническите изисквания и мерки, които обезпечават сигурността на персоналния контрол (sole control assurance).

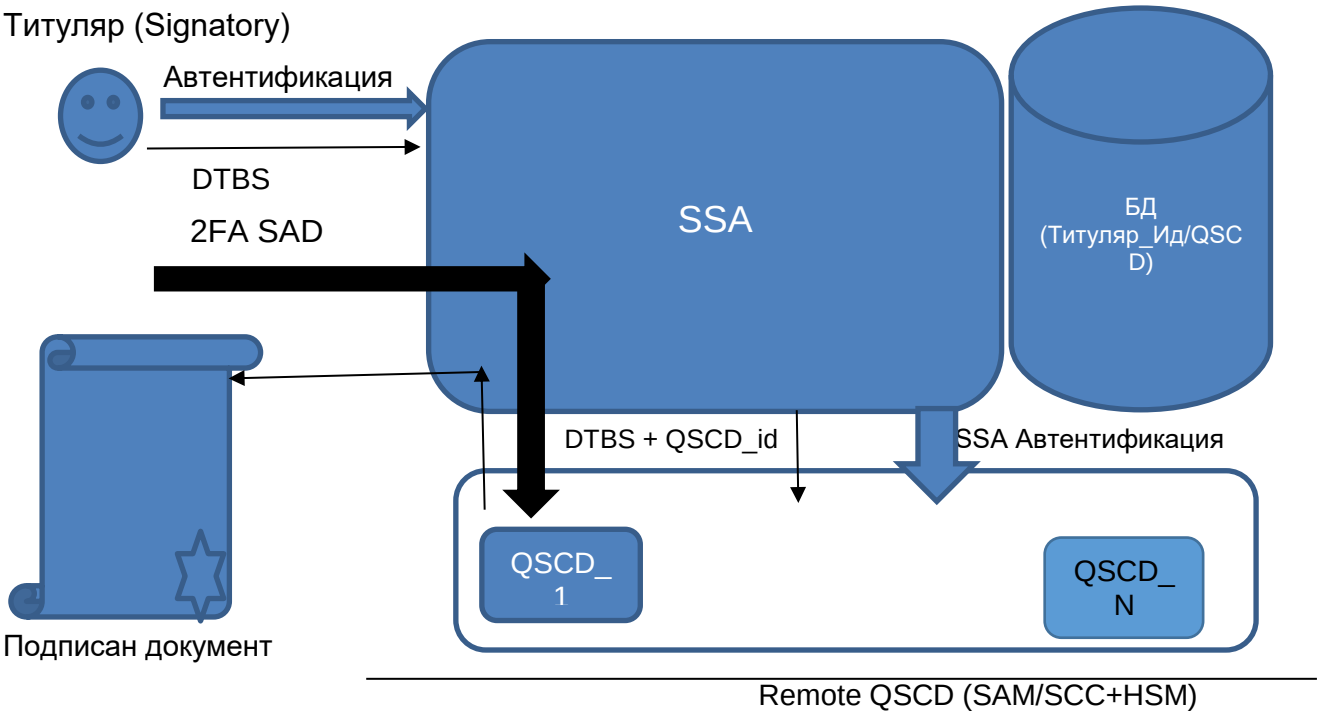


Фиг. 1 Общ концептуален модел на отдалечено подписване

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).

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



Фиг. 2 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 (RQSCD), базирано на QSCD/HSM 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 SSAS 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. 1). Ниво 1 на сигурност на персоналния контрол в този модел се имплементира чрез т.н.делегирана‘ автентификация (Титуляр пред SSAS и чрез SSAS 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 през мобилната мрежа (мобилен Интернет) се използва за активиране и потвърждаване на облачния КЕПс с помощта на персоналното/лично устройство (смартфона).

7 ФУНКЦИОНАЛЕН МОДЕЛ

Платформата за Облачен КЕП включва:

- Отдалечена сървърна компонента на ДКУУ „БОРИКА“ АД, включваща RQSCD (SSAS и HSM) под негово управление и контрол;
- Мобилно приложение за смартфон (за платформи Android и iOS).

RQSCD е част от инфраструктурата B-Trust, идентифицира се като неин обект с идентификатор 1.3.6.1.4.1.15862.1.6.8, който следва общите Практика и Политика на ДКУУ „БОРИКА“ съгласно документите B-Trust CPS-eIDAS и B-Trust CP-eIDAS, както и специфичните условия и изисквания посочени в този документ. Включва две части със следните функционалности:

- “Издаване на Облачен КЕП” – генерира двойка ключове за облачен КЕП, оперира вътрешни криптограми за защита и сигурност на на достъпа до двойката ключове и поддържа и съхранява защитен/криптиран частния ключ за създаване на цифров подпис за облачен КЕП ;
- “Подписване с Облачен КЕП” – оперира протокол за поддържане на персонален достъп/контрол до частен ключ и автентифицира държателя на данните за активация на подписа (SAP), определя валидността на асоцираното удостоверение за публичен ключ, съответстващ на частния такъв, активира чрез ПИН-код (SAD) генериране на цифров подпис (PKCS#1) в HSM-а и предоставя генерирания подпис и асоциираното с него удостоверение за последващо формиране на контейнера на облачен КЕП съобразно заявен формат и профил.

“Издаване на Облачен КЕП” използва възможно най-пълно текущата имплементация на B-Trust инфраструктурата, чрез която ДКУУ „БОРИКА“ АД издава и поддръжка на картовия КЕП (КЕП на смарт карта) както и свързаните с него удостоверителни услуги - издаване, подновяване и управление (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 (по-точно, на квалифицираните удостоверения за картов КЕП) и не ползва RQSCD (SSAS и HSM-а).

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.

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

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

Функционалност „Регистрация“ и „Издаване” на частта за “Издаване на облачен КЕП” 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 частта "Подписване с облачен КЕП" 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 B-Trust Портала 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 (МРС/Местана Регистрираща Служба) 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 персонализиране и регистрация 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). Активацията и регистрацията на B-Trust Mobile създава уникален ID (App_ID) и парола и регистрира този ID в частта за "Издаване на облачен КЕП" в RQSCD 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 частта “Издаване на облачен КЕП”; 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";
- Частта “Издаване на облачен КЕП“ 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 съхраняват криптирани с паролата в мобилното приложение;
- В следваща страница в браузъра на Агента се получава покана да се въведе 2FA TOTP-код от смартфона на Заявителя за проверка за притежание/държане на смартфона; Заявителят генерира TOTP-код на смартфона си;;
- В страницата на браузъра се въвежда генерирания TOTP-код от B-Trust Mobile и се изпраща на частта “Издаване на облачен КЕП”, където се проверява; с това приключва проверката за притежания на смартфона;
- Платената заявка за издаване на Облачен КЕП преминава в статус „Confirmed”; частта “Издаване на облачен КЕП” изпраща push нотификация към мобилното приложениес искане да се въведе ПИН-код;
- Въвежда се ПИН за Облачен КЕП на смартфона, който се криптира със съхранявания крипто ключ за ПИН в мобилното приложение; криптирания ПИН се предава на частта“Издаване на облачен КЕП“ на QRSCD и участва в процеса на генериране на двойката ключове за Облачен КЕП и създаване на публичните криптограми за защита на частния ключ за Облачен КЕП чрез HSM-а;
- Генерира се двойката ключове за Облачен КЕП и се създават публичните криптограми за частния ключ на Облачен КЕП чрез HSM, -които се асоциират със съответното APP_ID в базата данни за облачен КЕП;
- 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);
- частта“Издаване на облачен КЕП” 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-подписа.

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, а не на Агента в MPC.

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.

. ДКУУ „БОРИКА“ АД издава квалифицираните удостоверения за Облачен КЕП със срок на валидност, съответстващ на Политката за квалифицирани удостоверения. След този срок на валидност, Титулярят на облачен КЕП може да продължи (Renew) действието на Облачен КЕП или да заяви издаване на нов такъв.Доставчикът поддържа смяната на ПИН и блокиране/разблокиране на блокиран потребителски ПИН на издаден Облачен КЕП.

Посочената по-горе функционалност „Управление/Поддръжка“ на Облачен КЕП се изпълнява чрез 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 частта “Използване за Облачен КЕП” на RQSCDизпълнява само генериране на цифров подпис (PKCS#1) след строга автентификация на Титуляра на Облачния КЕП. Генерираният цифров подпис и асоциитаното удостоверение за публичния ключ, съответстващ на частния такъв на подписа се предоставят на обособена приложна УСЛУГА на ДКУУ „БОРИКА“ АД за подписване с Облачен КЕП, която ги интегрира и формира контейнера на е-подписа съобразно заявен/изискван формат на КЕП (CAdES, XAdES, PAdES, ASiCS/E) и профил (ниво на сигурност) на подписа (BASELINE_B, BASELINE_T, BASELINE_LT, BASELINE_LTA). Виж документ „УДОСТОВЕРИТЕЛНА УСЛУГА ЗА ДИСТАНЦИОННО ПОДПИСВАНЕ С ОБЛАЧЕН КЕП – ПОЛИТИКА И ПРАКТИКА“ на ДКУУ „БОРИКА“ АД.

Функционалността на тази УСЛУГА за дистанционно подписване с облачен КЕП може да бъде изнесена като част на приложни системи при Доставчици на приложни е-услуги.

Формирането на контейнера на е-подпис базиран на Облачен КЕП е извън обхвата на сървърната компонента RQSCD и този документ. .

Документ за подписване (може да) се съхранява на приложен (корпоративен) сървър или локалната система (PC) на Титуляря. С цел конфиденциалност, на УСЛУГАТА за дистанционно подписване с Облачен КЕП се предоставя хеш-данна за документа за подпис.

Функционалността на частта ”Подписване с облачен КЕП“ на RQSCD в съчетание с УСЛУГАТА за подписване с облачен КЕП включва:

- След като Потребител (или Доверяваща се страна)на УСЛУГАТА избере е-документ за подпис и предостави четим PROFILE_ID (генериран на базата на APP_ID) от мобилното приложение в смартфона на Титуляря, се формира хеша на документа, който се извежда на страница в браузъра на Титуляря заедно с поле за въвеждане на TOTP-код;
-
- Потребителят въвежда TOTP-кода, генериран от мобилното приложение;
- Браузърът на Титуляря се редиректва към УСЛУГАТА за подписване, която работи с частта “Подписване с облачен КЕП” на RQSCDc параметри – идентификатора, TOTP, хеш-данната и адрес за връщане (callback URL) към Доверяваща се страна;
- Частта Подписване на RQSCD автентифицира Титуляря на подписа като проверява TOTP и изпраща push нотификация на мобилното приложение с информация за чакащия за подписване документ- хеша на документа и искане да актиивира генерирането на подписа (цифров);
-
- Потребителят преглежда и сравнява получения хеш на документа с този в страницата на браузъра и потвърждава подписването като въвежда ПИН-кода за да активира генериране на цифров подпис (PKCS#1) в RQSCD чрез HSM-а;
- Вързешен протокол (SAP/Signature Activation Protocol) доставя криптиран ПИН-кодът (SAD) за частта Подписване на RQSCD;
- Чрез въведения ПИН-код се изпълняват криптографски операции с публичните крипограми, създадени в RQSCD при издаване на (удостоверението за) Облачния КЕП; чрез тях се обслужва персоналния контрол на Титуляря върху частния ключ за генериране на цифров подпис (PKCS#1);
- В HSM-а на RQSCD се генерира цифров подпис (PKCS#1) само след успешна проверка за валидност на квалифицираното удостоверение за публичния ключ, съответстващ на адресирания частен ключ в HSM-а;
- Генерираният цифров подпис (PKCS#1) заедно с квалифицираното удостоверение на Облачния КЕП се доставя на УСЛУГАТА за подписване, която генерира контейнера на Облачния КЕП, в съответствие на заявен формат и профил, респективно на Доверяващата се страна/Потребителя, инициирала подписването;
- Информация за успешно подписан документ се визуализира на смартфона на Титуляря.

8 ТЕХНИЧЕСКА СПЕЦИФИКАЦИЯ И РЕАЛИЗАЦИЯ

Практическата реализация на RQSCD за услугата Облачен КЕП се имплементира съгласно функционалният модел в Глава 7 на този.

ДКУУ „БОРИКА“ АД планира бъдещо развитие на квалифицираната услуга Облачен КЕП чрез изпълнение на RQSCD с HSM + SAM/SCC код, сертифицирани в съответствие с EN 419 241-2/3.