Платформа цифрового рубля

Криптографическая защита на базе продуктов КриптоПро

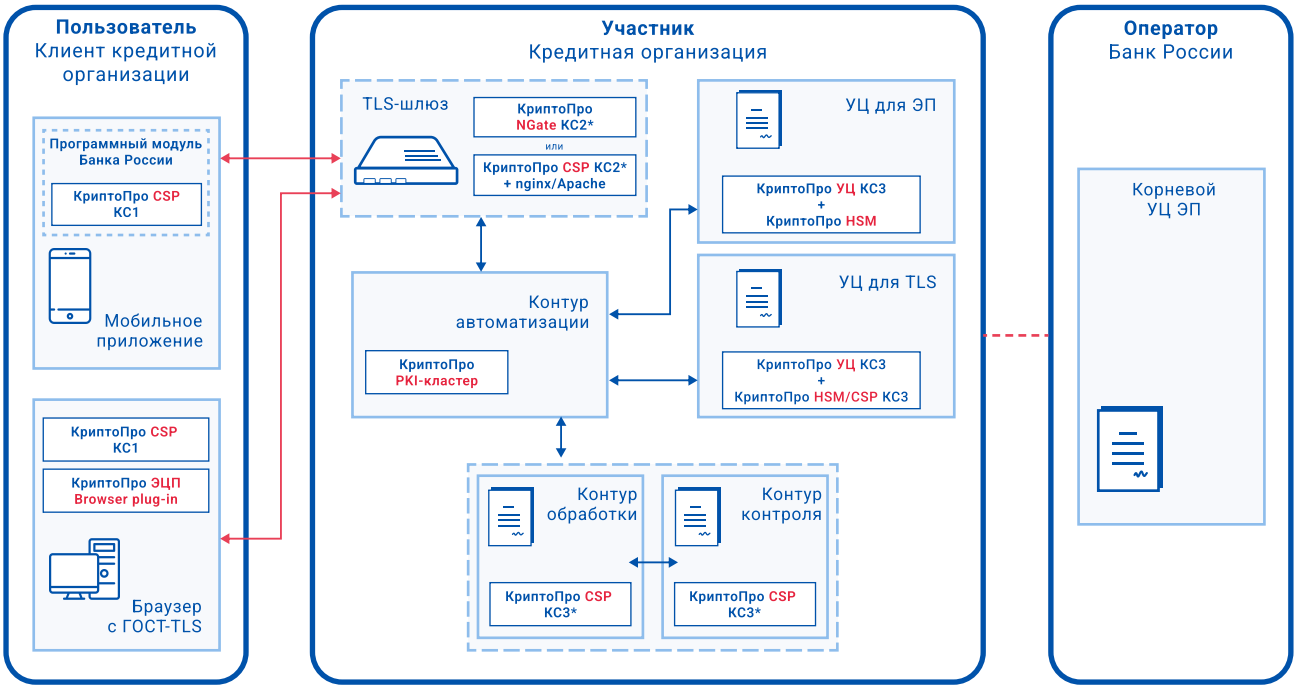
Что такое цифровой рубль?

В России введена новая, третья форма национальной валюты — цифровой рубль, который будет использоваться наряду с наличными и безналичными рублями.

Субъекты взаимодействия:

Пользователь: физическое лицо, юридическое лицо или ИП с доступом к ПлЦР в целях совершения операций с ЦР.
Участник: кредитная организация, предоставляющая доступ к сервисам ПлЦР своим Клиентам, либо использующая сервисы ПлЦР для выполнения своих финансовых операций.
Оператор: Банк России, обеспечивающий функционирование ПлЦР и контроль за соблюдением правил ПлЦР.

Схема взаимодействия:



Описание продуктов:

На стороне пользователя:

Компоненты ДБО, включая мобильное приложение со встроенным программным модулем Банка России, реализующим функционал совершения операций с ЦР.

Продукты КриптоПро:

- СКЗИ «КриптоПро CSP» версии 5.0 R3 КС1 (в составе ПМ БР разработки КриптоПро) в случае работы через мобильное приложение;
- СКЗИ «КриптоПро CSP» версии 5.0 R3 КС1 совместно с ПО «КриптоПро ЭЦП Browser Plugin» для обеспечения возможности работы с ПлЦР с использованием web-браузеров, поддерживающих российские криптоалгоритмы (например, Яндекс.Браузер, Atom, Chromium GOST).

На стороне участника:

Подчиненный Удостоверяющий центр для выдачи пользователям ПлЦР сертификатов ключей проверки электронной подписи (УЦ для ЭП), используемой при обмене электронными сообщениями. Является подчиненным Корневому УЦ ЭП Банка России.

Продукты КриптоПро:

- ПАКМ «КриптоПро HSM» версии 2.0 R3 (комплектация 1, исполнение 1К), является обязательным в случае автоматизации выдачи сертификатов. В случае отсутствия автоматизации выдачи сертификатов вместо этого возможно применение СКЗИ «КриптоПро CSP» версии 5.0 R3 КС3*, либо ПАКМ «КриптоПро HSM» версии 2.0 R3 (комплектация 2, исполнение 3К).
- ПАК «КриптоПро УЦ» версии 2.0 класса КС3*

Удостоверяющий центр для выдачи сертификатов безопасности (УЦ для TLS) для защиты сетевых соединений по протоколу ГОСТ-TLS между пользователем и участником ПлЦР (УЦ TLS).

Продукты КриптоПро:

- СКЗИ «КриптоПро CSP» версии 5.0 R3 КС3* или ПАКМ «КриптоПро HSM» версии 2.0 R3 (комплектация 2, исполнение 3К);
- ПАК «КриптоПро УЦ» версии 2.0 класса КС3*.

Контур обработки и контур контроля для обеспечения шифрования и расшифрования электронного сообщения, формирования и проверки ЭП.

Продукты КриптоПро:

- СКЗИ «КриптоПро CSP» версии 5.0 R3 КС3*.

*Требования вступают в силу с 01.01.2025 (п.14.2, 833-П)

TLS-шлюз для защищенного TLS-соединения между клиентом и банком.

Продукты КриптоПро:

- КСПК «КриптоПро NGate» версии 1.0 R2 класса КС3*/СКЗИ «КриптоПро CSP» версии 5.0 R3 КС3* для обеспечения защиты канала при взаимодействии с ЕСИА и устройством пользователя ПлЦР;

Контур автоматизации предназначен для обеспечения возможности реализации функционала автоматической выдачи сертификата;

Продукты КриптоПро:

- ПК «КриптоПро PKI-Кластер».

На стороне оператора:

Корневой Удостоверяющий центр для выдачи участникам ПлЦР сертификатов ЭП, используемой при обмене электронными сообщениями;

Нормативные документы:

Положения Банка России:

«О платформе цифрового рубля» № 820-П от 03.08.2023

Устанавливает функции оператора ПлЦР, требования к участникам и пользователям ПлЦР, порядок предоставления доступа к ПлЦР и пр.

«О требованиях к обеспечению защиты информации для участников платформы цифрового рубля» № 833-П от 07.12.2023

Устанавливает требования к обеспечению защиты информации для участников ПлЦР, в том числе с использованием СКЗИ.

Документы, выдаваемые Банком России участникам ПлЦР по запросу:

«Временные требования по обеспечению ИБ для автоматизации выпуска сертификатов пользователя платформы цифрового рубля»

Определяет требования по ИБ при построении инфраструктуры участника ПлЦР для обеспечения возможности автоматического выпуска сертификатов пользователя ПлЦР.

«Порядок проведения работ по оценке влияния аппаратных, программно-аппаратных и программных средств сети (системы) конфиденциальной связи, совместно с которыми предполагается штатное функционирование программного модуля Банка России, на выполнение предъявленных к входящему в его состав СКЗИ требований»;

В документе определены требования к порядку проведения работ по оценке влияния мобильного приложения со встроенным программным модулем Банка России (ПМ БР) и исследований в рамках дальнейших доработок мобильного приложения.

*Требования вступают в силу с 01.01.2025 (п.14.2, 833-П)

Описание продуктов:

СКЗИ «КриптоПро CSP» версии 5.0

СКЗИ «КриптоПро CSP» при работе в составе ПМ БР обеспечивает возможность шифрования/расшифрования электронных сообщений, создание и проверка ЭП электронных сообщений, обеспечение двустороннего TLS-соединения с поддержкой российских криптографических алгоритмов.

ПК «КриптоПро ЭЦП Browser Plug-in»

Плагин КриптоПро обеспечивает возможность выполнения криптографических операций из web-браузера (генерация ключей, создание запросов на сертификат, создание и проверка ЭП данных, шифрование/расшифрование данных).

ПАКМ «КриптоПро HSM»

Аппаратный криптографический модуль КриптоПро HSM используется для обеспечения высокого уровня безопасности криптографических операций, связанных с обработкой, хранением и использованием криптографических ключей и цифровых подписей.

ПК «КриптоПро УЦ»

КриптоПро УЦ обеспечивает в контуре участника выдачу сертификатов ключей проверки ЭП.

КСПК «КриптоПро NGate»

Универсальный TLS-шлюз используется для организации защищенного TLS-соединения между клиентом и банком.

ПК «КриптоПро PKI-Кластер»**

Данный продукт предназначен для обеспечения возможности реализации функционала автоматической выдачи сертификатов (сертификатов ключей проверки ЭП и сертификатов безопасности) пользователю ПлЦР. Обеспечивает интеграцию компонентов ДБО Участника, сервисов, обеспечивающих взаимодействие с ЕСИА и УЦ. Реализует функции обработки получаемых от пользователя запросов на сертификат и выданных УЦ сертификатов (проверку корректности запроса, в том числе форматно-логический контроль по заданным правилам и проверку ЭП, соответствия данных пользователя, полученным из ЕСИА и указанных в полученном запросе и выданном сертификате).

**Находится в стадии сертификации