инфотекс

Защита инфраструктуры цифрового рубля

Цифровой рубль

>> Цифровой рубль (ЦР) – это новая форма российской национальной валюты, которая будет выпускаться в дополнение к существующим формам денег – наличной и безналичной.

Цифровой рубль создается как средство для проведения платежей и переводов, при этом необходимо отметить, что цифровой рубль – это не криптовалюта, а национальное денежное средство, выпуском которого занимается Банк России.

Цифровой рубль будет храниться на цифровых счетах граждан и организаций – цифровых кошельках, открытых на платформе Банка России и не привязанных к какому-то конкретному банку.

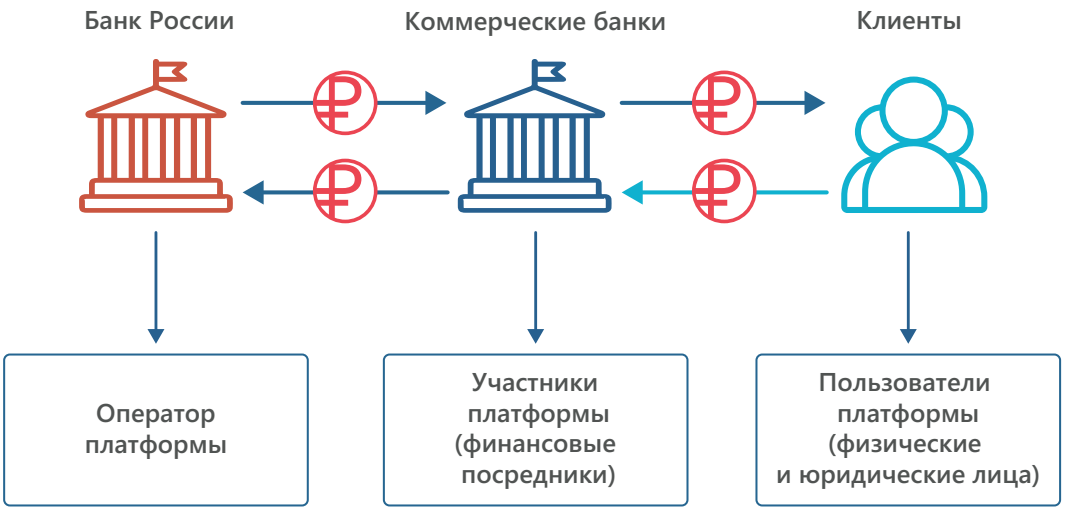


Схема 1. Роли в платформе цифрового рубля

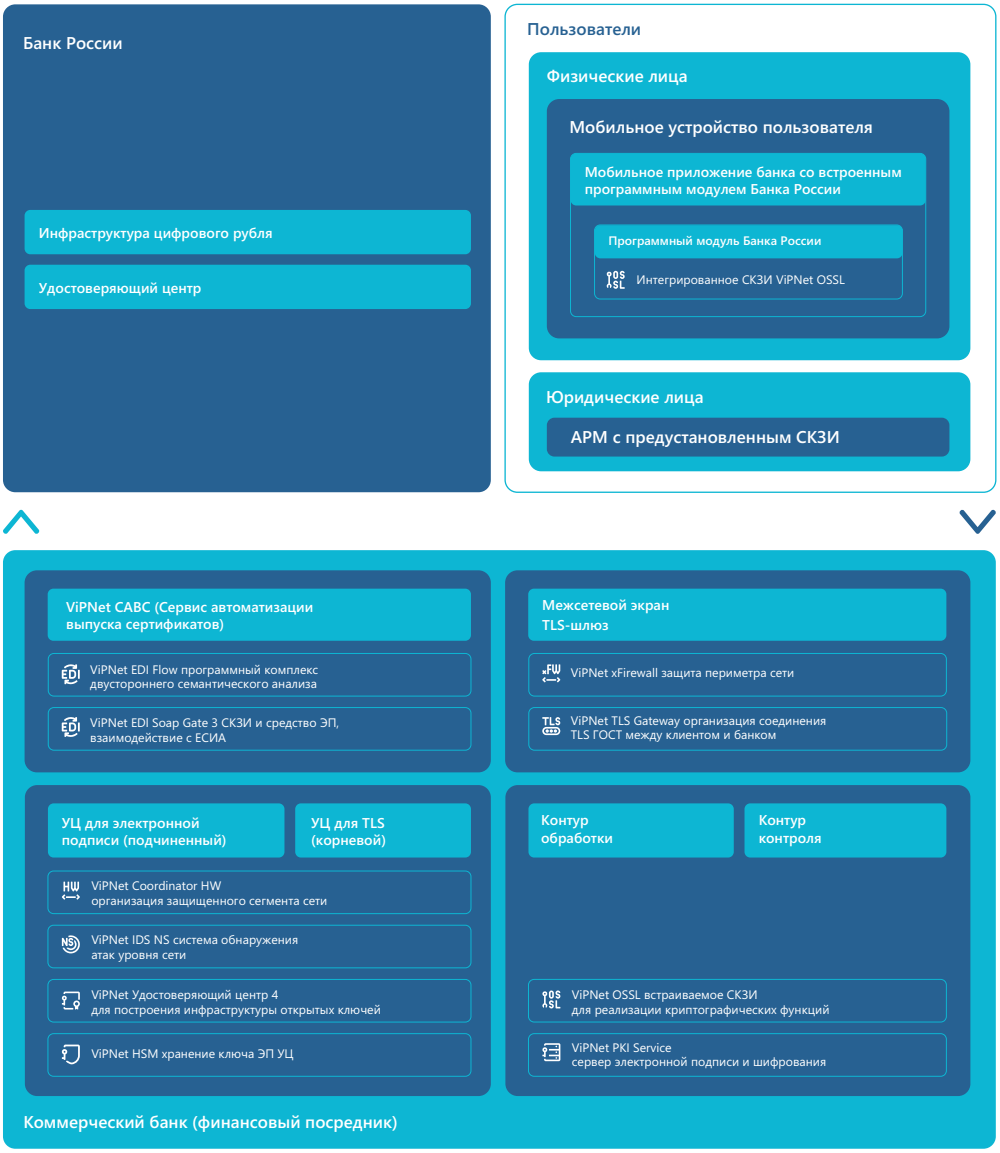


Схема 2. Продукты ViPNet для защиты платформы цифрового рубля

ПРЕИМУЩЕСТВА

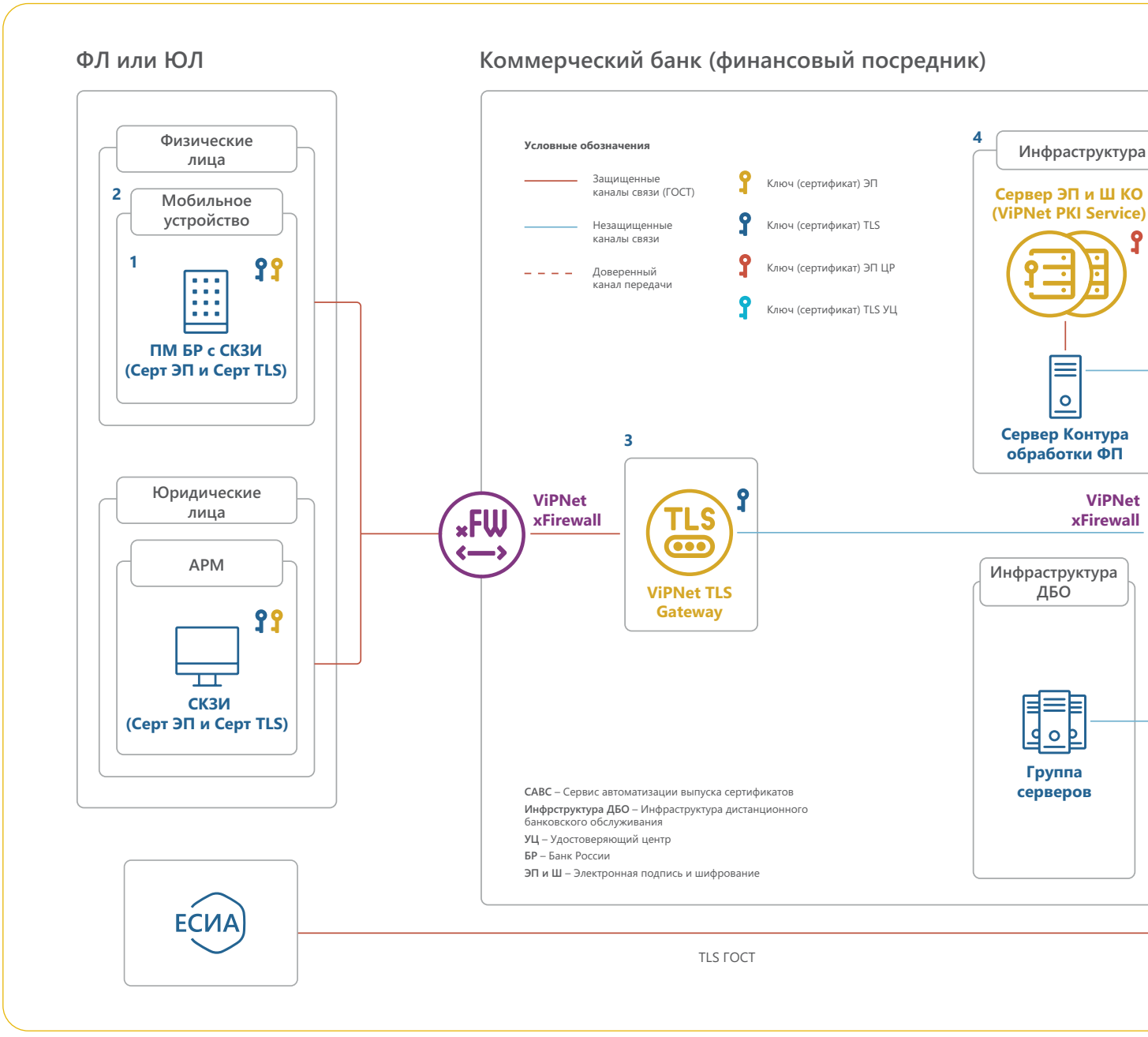
- Комплексное решение, которое может быть предоставлено как целиком, так и в виде отдельных компонентов
- Продукты решения имеют сертификаты ФСТЭК России и ФСБ России
- Возможность организации тестовых и пилотных проектов с использованием продуктов ViPNet на безвозмездной основе
- Компоненты решения соответствуют стандартам PKI и совместимы с PKI-решениями сторонних производителей
- Возможность организации отказоустойчивой системы за счет кластеров
- Возможность проведения работ по оценке влияния в испытательной лаборатории, занимающейся сертификацией предлагаемых к использованию СКЗИ

РЕШЕНИЕ

Рассматривая общую схему инфраструктуры и предлагаемые к использованию соответствующие требованиям средства защиты информации ViPNet, можно начать с сегмента пользователя **(1 и 2 на схеме)**.

Пользователь платформы цифрового рубля (ПлЦР) осуществляет взаимодействие с коммерческим банком с использованием мобильного приложения банка. Электронные сообщения, передаваемые мобильным приложением и используемые для взаимодействия субъектов платформы, подписываются электронной подписью, шифруются и передаются по защищенному каналу путем организации ГОСТ TLS-соединений.

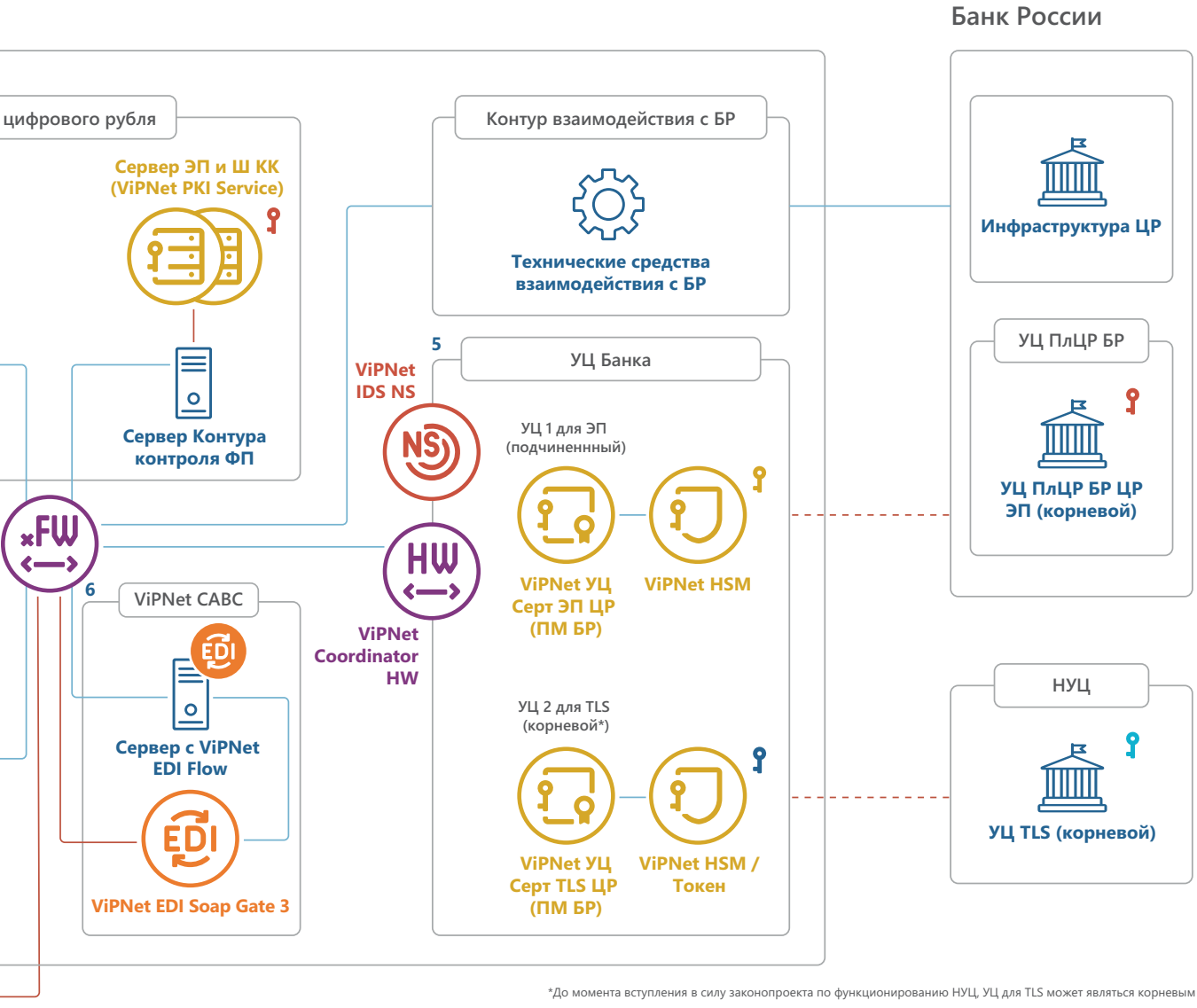
Для этих целей в банковское приложение должен быть встроен программный модуль Банка России с сертифицированным средством криптографической защиты информации (СКЗИ). В настоящее время существует несколько версий программного модуля Банка России, в состав которых входят разные СКЗИ. При этом исключительные права на программный модуль принадлежат Банку России.



В составе версии программного модуля, разработанной компанией «ИнфоТеКС» по запросу Банка России, используется сертифицированное СКЗИ ViPNet OSSL.

ViPNet OSSL – это программное обеспечение на базе библиотеки с открытым исходным кодом OpenSSL, которое позволяет использовать российские криптографические алгоритмы ГОСТ через обращения по интерфейсу OpenSSL, а также:

- создавать защищенное соединение с использованием протокола TLS 1.2 и TLS 1.3
- хэшировать данные
- создавать ключи электронной подписи (ЭП), формировать и проверять ЭП
- шифровать данные



*До момента вступления в силу законопроекта по функционированию НУЦ, УЦ для TLS может являться корневым

Схема 3. Предполагаемая схема защиты инфраструктуры платформы цифрового рубля

Следующий сегмент инфраструктуры цифрового рубля – это сегмент взаимодействия пользователя и финансового посредника **(3 на схеме)**. Программный модуль Банка России со встроенным СКЗИ организует защищенное соединение по протоколу TLS, использующему российскую криптографию.

Для возможности построения двустороннего TLS-соединения на стороне коммерческого банка (финансового посредника) также должен использоваться шлюз безопасности, предназначенный для организаций TLS-соединений. В соответствии с требованием Банка России для этих целей должно использоваться СКЗИ класса КС2. Для реализации данного сценария используется шлюз безопасности ViPNet TLS Gateway.

ViPNet TLS Gateway – это сертифицированный высокопроизводительный TLS-криптошлюз, использующий как российские, так и иностранные криптоалгоритмы.

ViPNet TLS Gateway обеспечивает аутентификацию пользователей и организацию защищенных соединений по протоколу TLS при работе с портальными решениями.

Следующий сегмент – инфраструктура и средства защиты информации в контуре контроля и контуре обработки на стороне финансового посредника **(сегмент 4)**. В соответствии с требованиями Банка России участник платформы должен обеспечивать защиту электронных сообщений при их передаче между пользователем платформы цифрового рубля и участником платформы посредством:

1 Использования усиленной неквалифицированной электронной подписи, реализуемой средствами ЭП не ниже класса КС3 на стороне участника платформы и СКЗИ не ниже класса КС1 на стороне пользователя платформы цифрового рубля

2 Шифрования (расшифрования) электронных сообщений на прикладном уровне с использованием СКЗИ не ниже класса КС3 на стороне участника платформы и СКЗИ не ниже класса КС1 на стороне пользователя платформы цифрового рубля

Для реализации данного сценария могут быть использованы продукты:

ViPNet PKI Service – сервер подписи, разработанный на базе криптографической платформы ViPNet HSM. Он предназначен для выполнения криптографических операций в прикладных сценариях информационных систем: генерации ключей, формирования и проверки ЭП, шифрования данных.

ViPNet OSSL – это программное обеспечение на базе библиотеки с открытым исходным кодом OpenSSL, которое позволяет использовать российские криптографические алгоритмы ГОСТ через обращения по интерфейсу OpenSSL.

Для обеспечения всех участников информационного взаимодействия сертификатами для возможности организации TLS-соединений, формирования и проверки ЭП, шифрования в инфраструктуре цифрового рубля на стороне финансовых посредников должны появиться удостоверяющие центры (УЦ): УЦ для выпуска сертификатов ЭП и УЦ для выпуска сертификатов безопасности **(сегмент 5).** Стоит отметить, что в рамках ПлЦР используется усиленная неквалифицированная подпись, поэтому аккредитация УЦ не требуется.

При этом УЦ финансового посредника для функции ЭП должен быть в подчинении УЦ БР. Транспортный УЦ на текущий момент может выступать в качестве корневого, но после ввода в эксплуатацию национального УЦ данный УЦ должен стать подчиненным. Класс средств УЦ, согласно требованиям Банка России – КС3.

ViPNet Удостоверяющий центр 4 (версия 4.6) – предназначен для построения инфраструктуры открытых ключей. ViPNet Удостоверяющий центр может использоваться для реализации функций удостоверяющего центра в соответствии с Федеральным законом от 6 апреля 2011 г. №63-ФЗ «Об электронной подписи». ViPNet УЦ может хранить ключ в неизвлекаемом виде в ViPNet HSM.

Компоненты программного комплекса:

- **ViPNet Administrator.** Выступает в роли центра сертификации. ViPNet Administrator реализует все основные функции удостоверяющего центра: издание сертификатов и управление их жизненным циклом
- **ViPNet Registration Point / ViPNet CA Web Service.** Исполняют роль центра регистрации – распределяют нагрузку по выдаче сертификатов в территориально распределенных удостоверяющих центрах
- **ViPNet Publication Service.** Выступает в роли сервиса публикации. ViPNet Publication Service обеспечивает доступ пользователей к выпускаемым сертификатам и CRL, размещая их в общедоступных хранилищах данных
- **ViPNet CA Informing.** Исполняет роль сервиса информирования. ПО ViPNet CA Informing оповещает администраторов и пользователей удостоверяющего центра о критических событиях и формирует отчеты

В качестве дополнительных СЗИ для защиты инфраструктуры цифрового рубля также могут применяться:

- **ViPNet IDS** – СОВ и/или СОА (для УЦ)
- **ViPNet Coordinator HW** – для защиты трафика ЦР в инфраструктуре банка
- **ViPNet xFirewall 5** – межсетевой экран для разделения или выделения сегментов ЦР внутри инфраструктуры банка

Для автоматизации выпуска сертификатов безопасности и сертификатов электронной подписи используется ViPNet CABC **(сегмент 6)**. Пользователь ПлЦР авторизуется через Единую Систему Идентификации и Аутентификации (ЕСИА) для идентификации в ПлЦР, формирует запрос на издание сертификата, который передается в ViPNet CABC. Для выполнения логической и семантической проверки запроса, получения и сверки пользовательских данных компонент ViPNet EDI Flow передает полученные данные в ПАК ViPNet EDI Soap Gate 3, который, в свою очередь, отправляет запрос в ЕСИА для получения маркера доступа и данных о пользователе. ViPNet CABC выполняет сверку данных пользователя, полученных из ЕСИА, с данными из запроса на создание сертификата. При положительном результате сверки ViPNet CABC отправляет запрос на издание сертификата в соответствующий УЦ, который издает сертификат и возвращает его в ViPNet CABC. После семантической проверки полей сертификата ViPNet CABC передает сертификат пользователю ПлЦР.

ViPNet CABC – комплекс технических и программных средств, предназначенный для выпуска сертификатов пользователей ПлЦР. ViPNet CABC обеспечивает автоматизированный процесс выпуска сертификатов безопасности и сертификатов ЭП.

ViPNet CABC включает следующие компоненты:

> программный комплекс ViPNet EDI Flow

> программно-аппаратный комплекс ViPNet EDI Soap Gate 3 (ViPNet ЭДО Шлюз безопасности 3) (далее - ViPNet EDI Soap Gate)

ViPNet EDI Flow – программный комплекс, который обеспечивает взаимодействие с ViPNet EDI Soap Gate и удостоверяющими центрами. ViPNet EDI Flow является управляющим компонентом ViPNet CABC и обеспечивает выполнение всех процессов, связанных с выпуском сертификатов безопасности и сертификатов ЭП пользователя ПлЦР.

ViPNet EDI Soap Gate 3 – программно-аппаратный комплекс, является средством криптографической защиты информации, сертифицированным на соответствие требований ФСБ России по классу КС3, и средством электронной подписи, сертифицированным на соответствие требований ФСБ России по классу КС3. ViPNet EDI Soap Gate осуществляет интеграцию с государственными информационными системами: ЕСИА, СМЭВ, ЦПГ, ЦПО, ГИС ГМП и пр. ViPNet CABC обеспечивает взаимодействие с ЕСИА для авторизации пользователя ПлЦР, проверку ЭП и извлечение данных запросов PKCS#10 пользователей ПлЦР. ViPNet EDI Soap Gate организует соединение с ЕСИА согласно «Методическим рекомендациям по использованию ЕСИА».

Кроме того, для проведения необходимых сертификационных работ по оценке влияния при встраивании программного модуля Банка России в мобильное приложение банка и использовании СКЗИ класса КС3 в контуре контроля и контуре обработки могут быть исполнены услуги испытательной лаборатории «СФБ Лаб», входящей в состав группы компаний «ИнфоТеКС».

инфотекс

+7 495 737-61-92
8 800 250-0-260 (бесплатный звонок по России)

soft@infotecs.ru
hotline@infotecs.ru

www.infotecs.ru

Официальный канал ИнфоТеКС про информационную безопасность современного финтеха

PKI26_DR_00RU