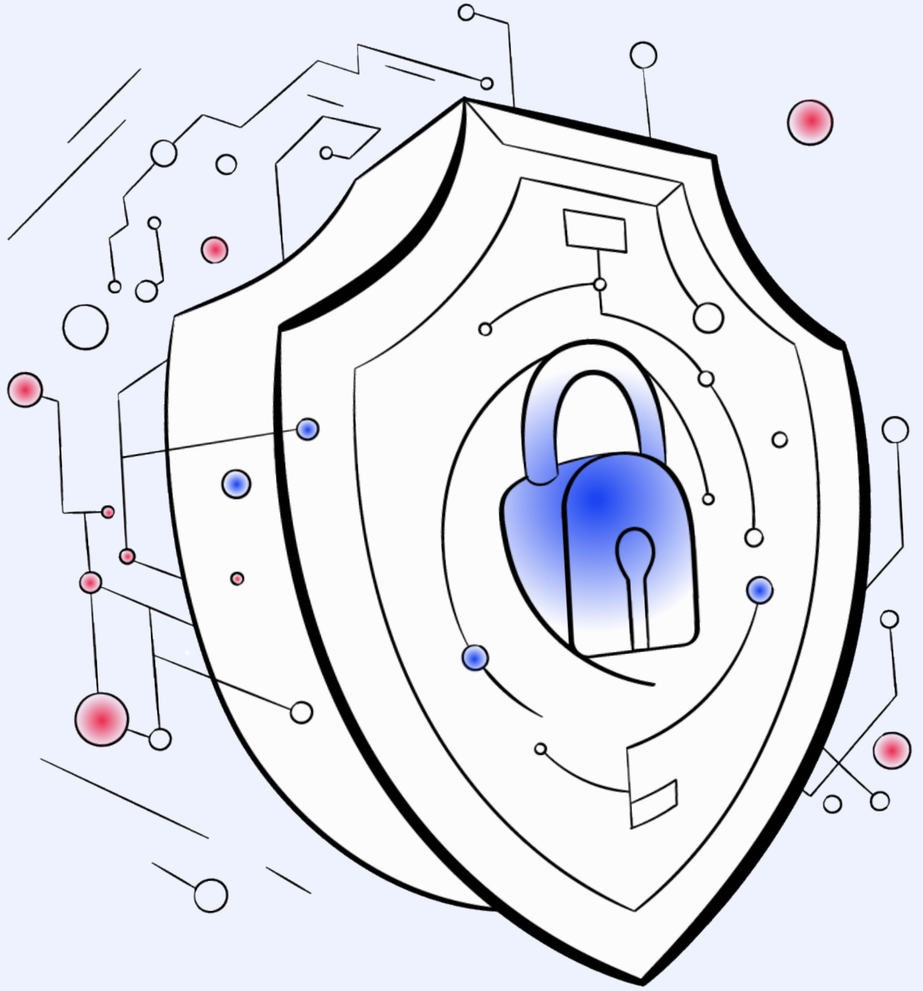
Криптографический модуль КПМ ЕБС

Внедрение российской криптографии в пользовательские продукты на примере клиентского программного модуля ЕБС



АО «Центр Биометрических Технологий»

Единая биометрическая система

Что это?

Цифровая платформа, которая позволяет идентифицировать человека по его биометрическим характеристикам

Биометрические параметры:

Лицо

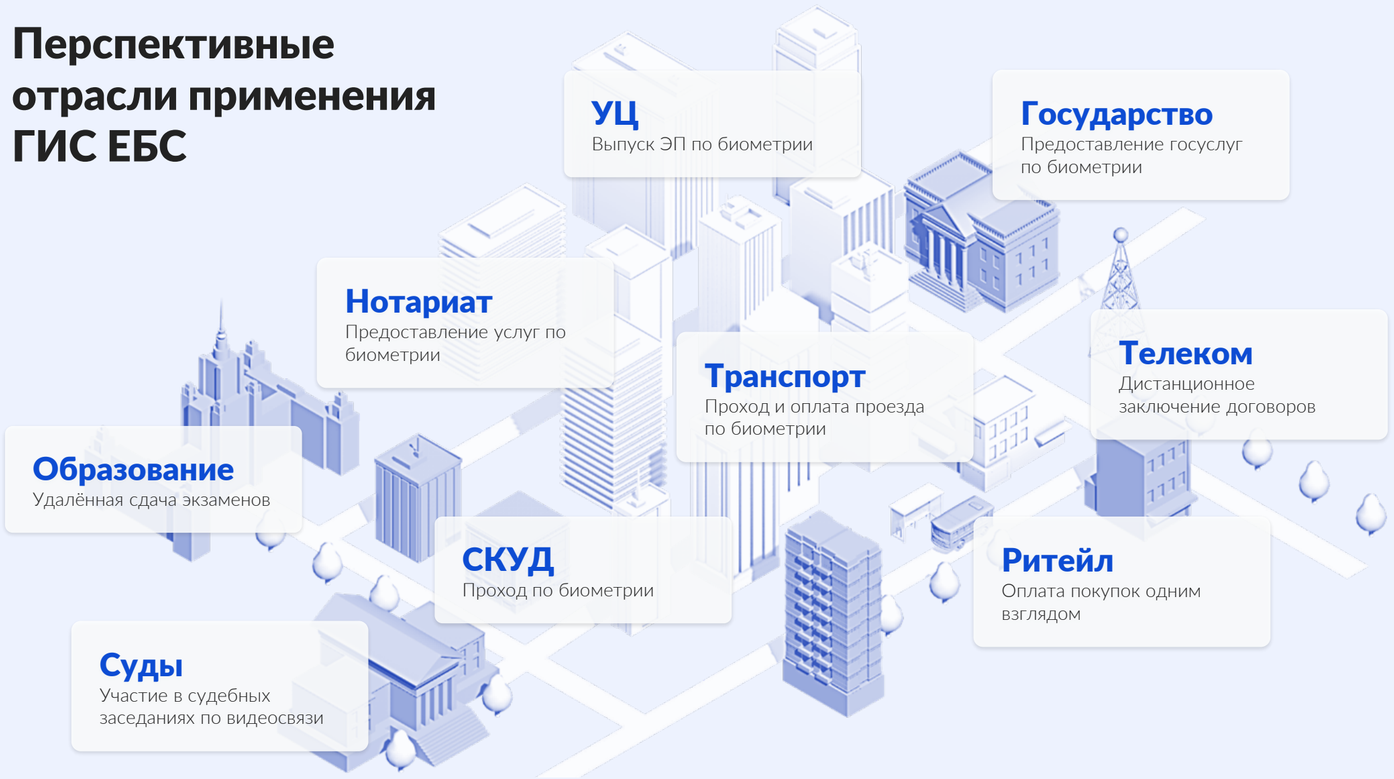
Голос

Государственная система

ЕБС является государственной информационной системой. Оператор ГИС ЕБС — АО «ЦБТ»

Идентификация приравнивается к паспорту

Перспективные отрасли применения ГИС ЕБС



УЦ
Выпуск ЭП по биометрии

Государство
Предоставление госуслуг по биометрии

Нотариат
Предоставление услуг по биометрии

Транспорт
Проход и оплата проезда по биометрии

Телеком
Дистанционное заключение договоров

Образование
Удалённая сдача экзаменов

СКУД
Проход по биометрии

Ритейл
Оплата покупок одним взглядом

Суды
Участие в судебных заседаниях по видеосвязи

Основные функции:

01 Регистрация биометрии

Зарегистрировать биометрию можно в 13 300 отделениях 231 банка в 95% городов России

02 Хранение биометрии

ЕБС — информационная система, защищённость которой подтверждена сертификатом ФСБ

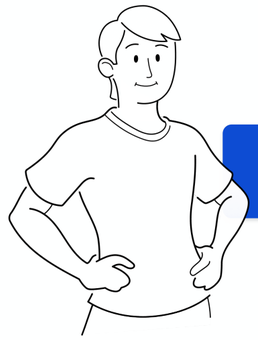
03 Установление личности

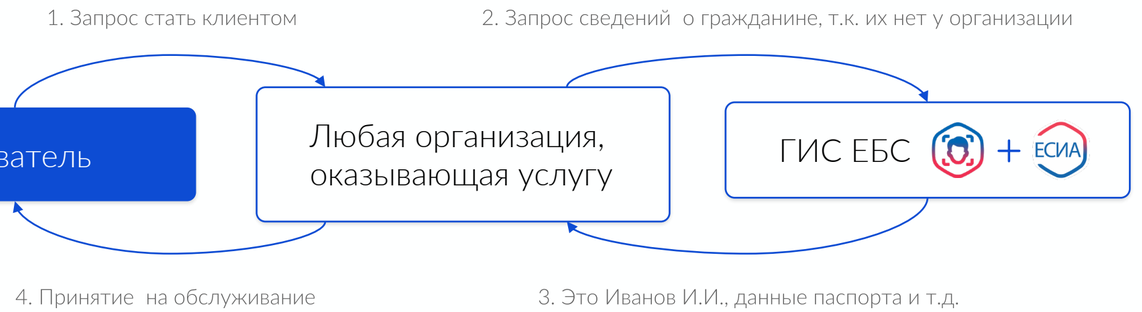
Идентификация и аутентификация граждан по биометрии

Удаленная биометрическая идентификация клиента

Установление личности

01





Требуется обеспечить ГОСТ TLS КС1 между пользователем и информационной системой Организации*

Какие особенности при встраивании СКЗИ?

Необходимость проведения оценки влияния

Большой релизный срок выпуска МП Организации

*Приказ Минцифры России от 05.05.2023 № 445 «Об утверждении перечня угроз безопасности, актуальных при обработке биометрических персональных данных», Указание Банка России от 25.09.2023 N 6540-У «О перечне угроз безопасности, актуальных при обработке биометрических персональных данных»

Поставленные цели при разработке КПМ ЕБС

- Упрощение интеграции мобильных приложений с ГИС ЕБС
- Бесшовный клиентский путь при работе с ГИС ЕБС
- Упрощение встраивания СКЗИ в МП Организации
- Обеспечение работы ГОСТ TLS КС1 в МП Организации
- Отсутствие необходимости проведения оценки влияния при встраивании
- Работа на платформах Android и iOS

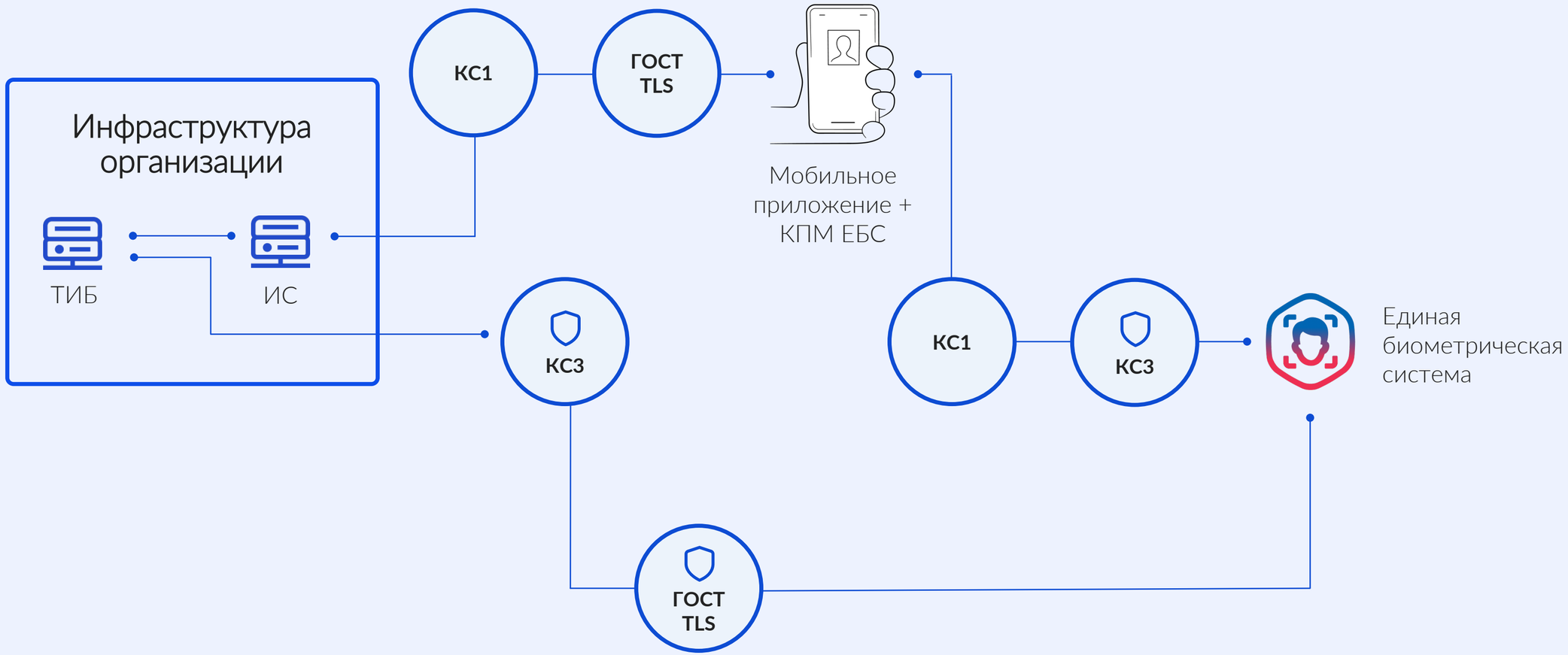
Функции КПМ ЕБС

- установление защищенного соединения по протоколу TLS (протокол TLS предназначен для обеспечения криптографическими средствами аутентификации сервера, контроля целостности и шифрования данных информационного обмена);

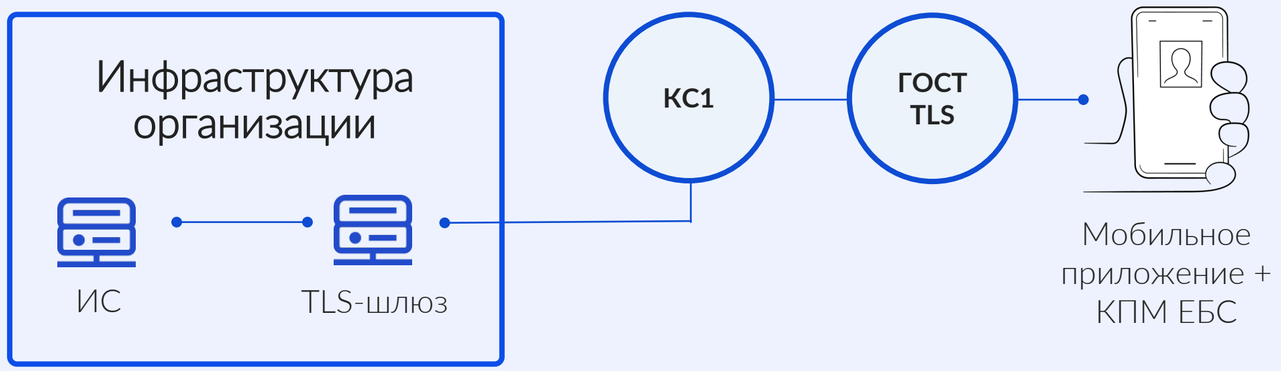
- процесс удаленной идентификации для решения задачи работы в рамках протокола OpenId Connect со стороны пользователя, в том числе возможность произвести запись БО для проведения удаленной идентификации пользователей по биометрическим характеристикам

- обеспечение информационного взаимодействие с Пользователем ЕБС с возможностью изменения стиля отображения визуальных компонентов и экранов.

Реализация защиты при удаленной биометрической идентификации



Реализация работы по ГОСТ TLS КС1

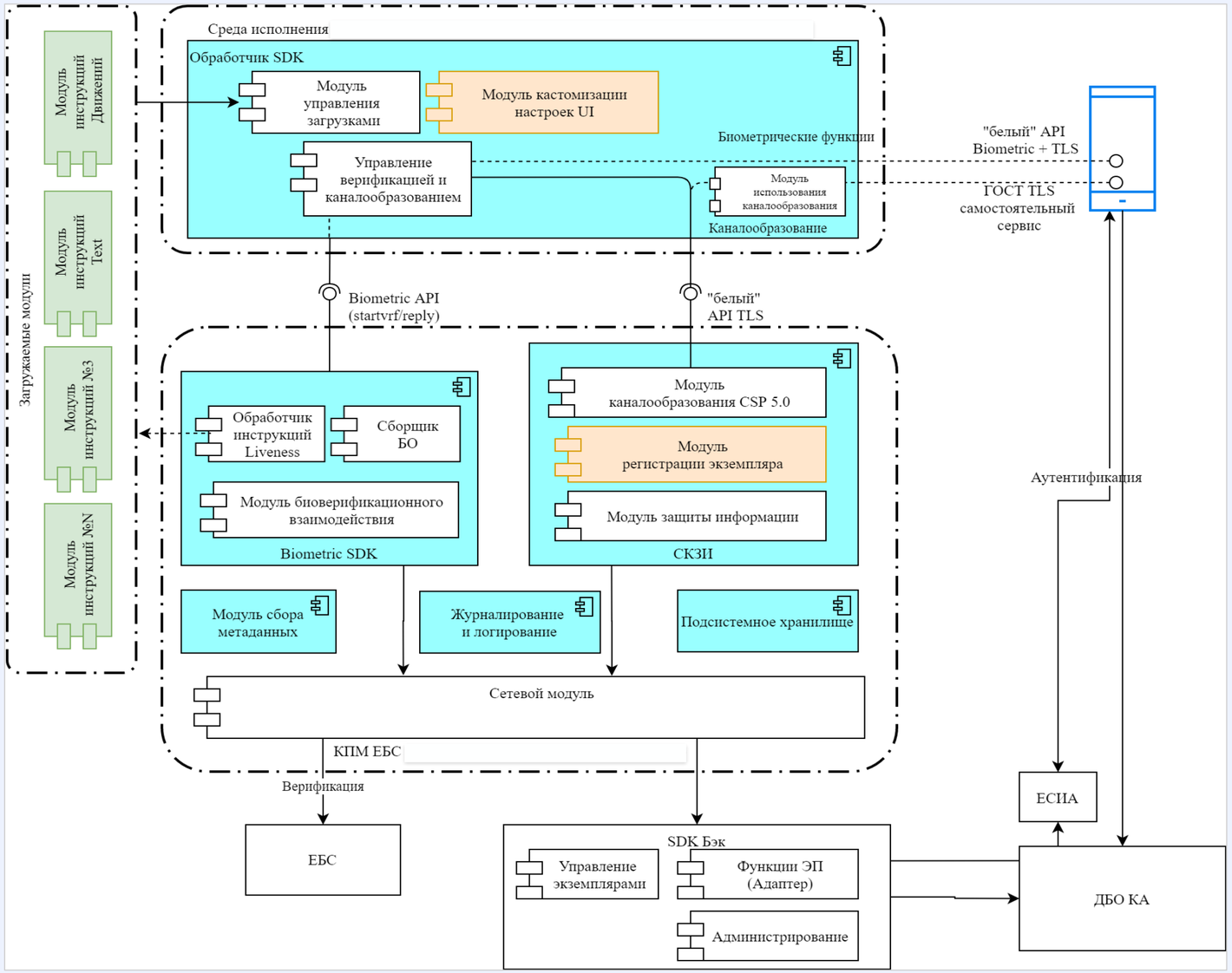


КриптоSDK ГОСТ TLS

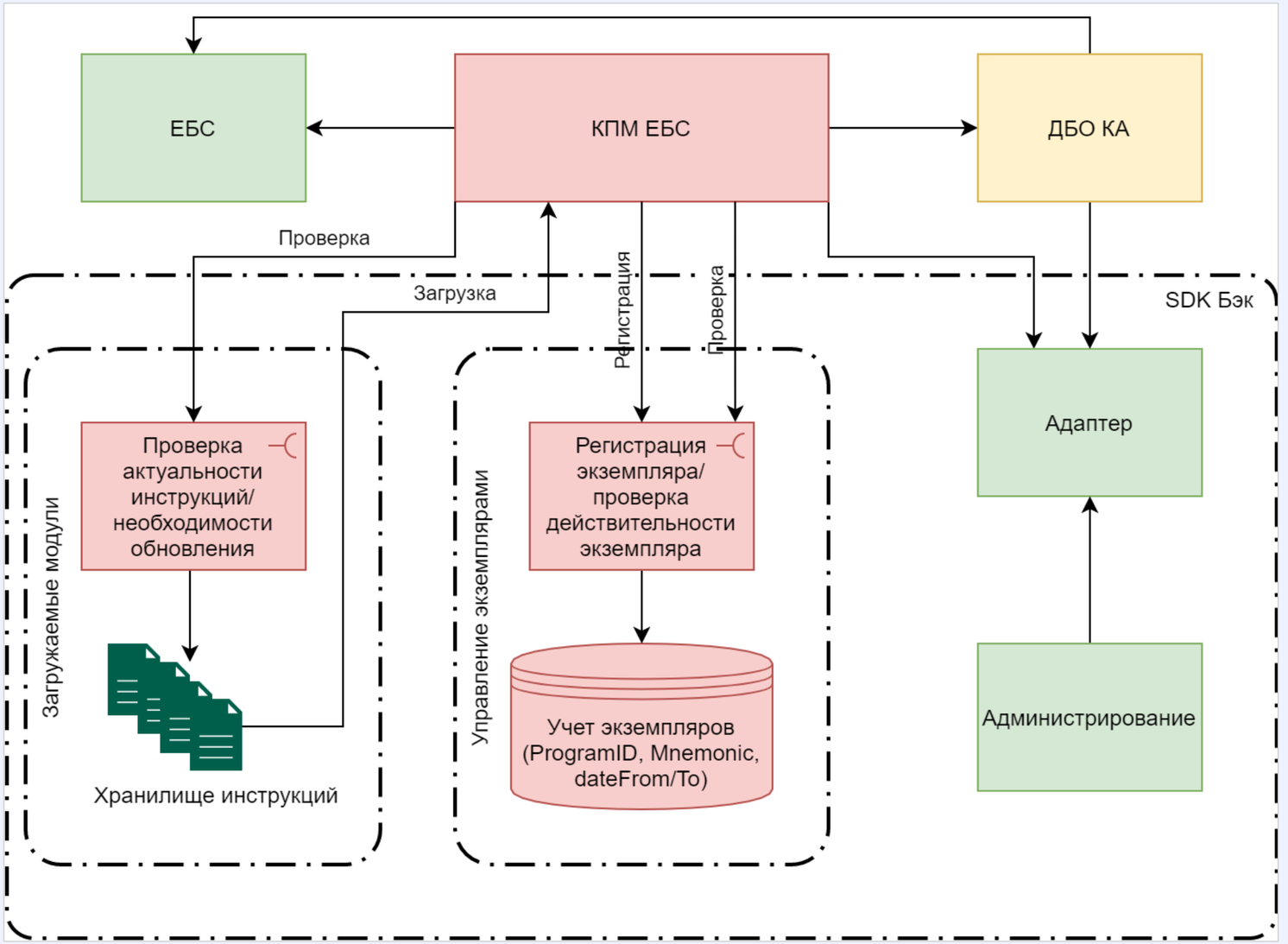
- Встраивается в Apache и Nginx
- Бесшовная работа с ГОСТ TLS
- Работа с TLS-шлюзом NGate или другими
- Не требует тематических исследований при встраивании
- Небольшие аппаратные запросы на функционирование

Что под капотом?

СКЗИ «КриптоПро CSP» 5.0 R2 КС1 (исполнение 1-Base)



Что под капотом?



Заключение ФСБ России

Письмом от 17.01.2024 N 149/3/2/1-137 получена выписка из заключения 149/3/2/1/4034 от 27.12.2023 по результатам оценки влияния типового клиентского программного модуля Единой биометрической системы на СКЗИ «КриптоПро CSP» версии 5.0 R2 КС1 (исполнение 1-Base)

В соответствии с заключением:

01 СКЗИ «КриптоПро CSP» версии 5.0 R2 КС1 (исполнение 1-Base) встроено в КПМ ЕБС в соответствии с требования и рекомендациями формуляра на СКЗИ

02 КПМ ЕБС не оказывает негативного влияния на выполнение предъявленных к СКЗИ «КриптоПро CSP» версии 5.0 R2 КС1 (исполнение 1-Base) требований

03 КПМ ЕБС разрешается эксплуатировать при условии:

- Наличия действующего сертификата соответствия на СКЗИ СКЗИ «КриптоПро CSP» версии 5.0 R2 КС1 (исполнение 1-Base)
- Выполнения требований согласно формуляра на СКЗИ «КриптоПро CSP» версии 5.0 R2 КС1 (исполнение 1-Base)
- Выполнения положения Методических рекомендаций по использованию КПМ ЕБС

* КриптоSDK – коммерческое название КПМ ЕБС

Требования к контролю использования КриптоSDK и построенных на его основе МП Организации

01 Наличие у разработчика МП Организации лицензии ФСБ России на осуществление разработки, производства, распространения шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, п. 2, 3 Перечня выполняемых работ и оказываемых услуг, составляющих лицензируемую деятельность, в отношении шифровальных (криптографических) средств, являющегося приложением к Положению, утвержденному постановлением Правительства Российской Федерации от 16 апреля 2012 г. № 313

02 Передача в АО «ЦБТ» (для последующего хранения) следующих данных:

- название разработчика МП Организации
- название МП Организации
- назначение МП Организации
- актуальные контрольные суммы разработанного МП Организации

Преимущества использования КриптоSDK

Отсутствие требований по проведению оценки влияния МП Организации

Взаимодействие с ЕСИА и ЕБС по защищённым каналам связи в процессе биометрической идентификации

Построение произвольных каналов связи, защищённых с помощью отечественной криптографии

Работа на платформах Android и iOS

Включен в Единый реестр российских программ для электронных вычислительных машин и баз данных

Портал ebs.ru

Презентация КриптоSDK

Канал «Биометрия РФ»

Остались вопросы?
Напишите нам на business@ebs.ru

АО «Центр Биометрических Технологий»