Реализация проекта Удалённая Биометрическая Идентификация.

То, что остаётся за скобками Коммерческих предложений.

Генеральный директор SDK Systems **Алексей Александров**

Основание для реализации

479-ФЗ от 29.12.2020

Банки с универсальной лицензией ОБЯЗАНЫ обеспечить возможность клиентам - физическим лицам открывать счета (вклады) в рублях, а также получать кредиты в рублях без личного присутствия после проведения идентификации клиента - физического лица с использованием технологии Удалённой Биометрической Идентификации (далее - УБИ) на основе биометрических данных в Единой Биометрической Системе, такая возможность обеспечивается банком посредством своего официального сайта в сети Интернет, а также мобильного приложения, которое соответствует требованиям, установленным ЦБ РФ.

Перечень требований ИБ

Федеральный закон РФ от 27.07.2006 N 149-ФЗ (ред. от 19.07.2018) «Об информации, информационных технологиях и о защите информации» (далее Федеральный закон № 149-ФЗ);

Федеральный закон РФ от 27.07.2006 № 152-ФЗ «О персональных данных»;

Федеральный закон Российской Федерации от 06.04.2011 № 63-ФЗ «Об электронной подписи»;

Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005);

Указание Банка России и ПАО «Ростелеком» № 4859-У/01/01/782-18 «О перечне угроз безопасности, актуальных при обработке, включая сбор и хранение, биометрических персональных данных, их проверке и передаче информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации в государственных органах, банках и иных организациях, указанных в абзаце первом части 1 статьи 141 Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», в единой биометрической системе»;

Методические рекомендации по нейтрализации банками угроз безопасности, актуальных при обработке, включая сбор и хранение, биометрических персональных данных, их проверке и передаче информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации № 4-МР от 14.02.2019 г;

Методические рекомендации по работе с ЕСИА (https://digital.gov.ru/ru/documents/6186/);

Методические рекомендации по работе с ЕБС (https://bio.rt.ru/business/).

Основная задача УБИ:

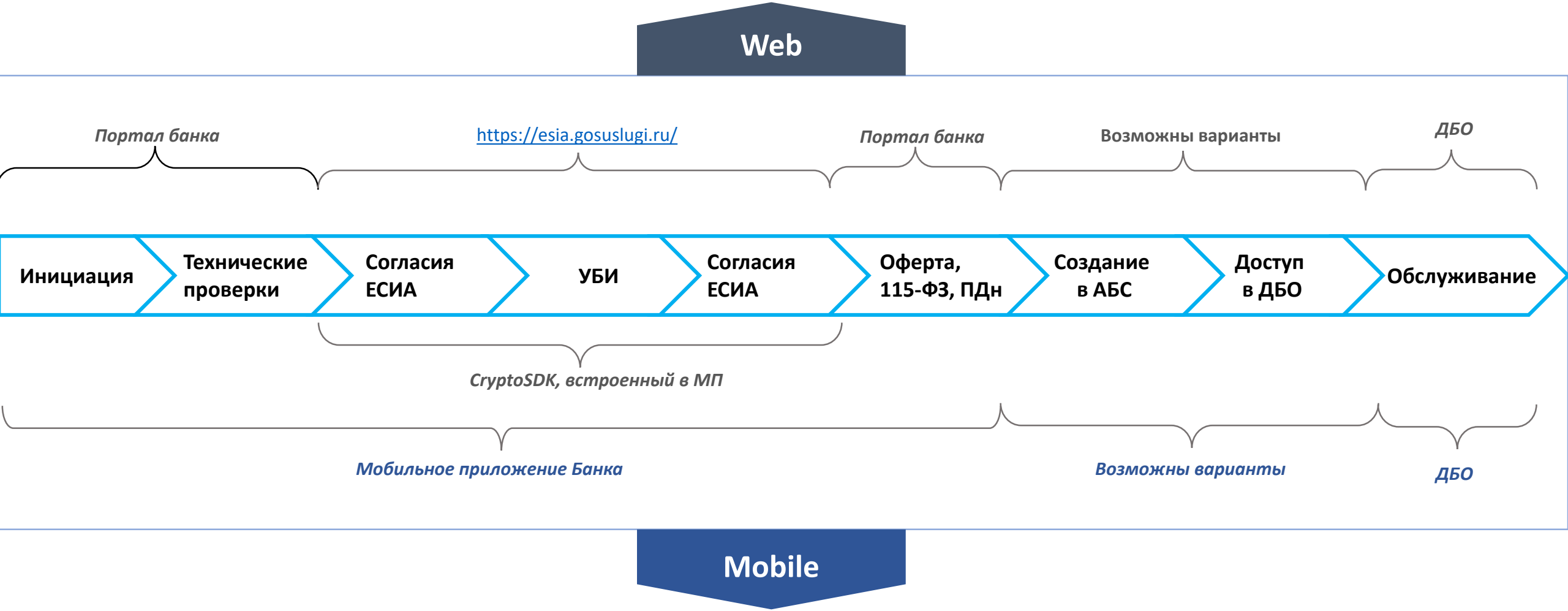
- «опознать» физическое лицо без личного визита в отделение банка и предоставить ему услуги.

Два варианта интерфейса:

- Мобильное приложение
  - Защищённый канал до ЕБС и до «типового решения» в Банке
  - Определённый перечень экранных форм-согласий
  - Встраивание КриптоSDK или CSP

- Web-портал
  - Web-браузер с поддержкой ГОСТ TLS
  - Защищённый канал до ЕБС и до «типового решения» в Банке

Отличия процесса при УБИ в Web и Mobile



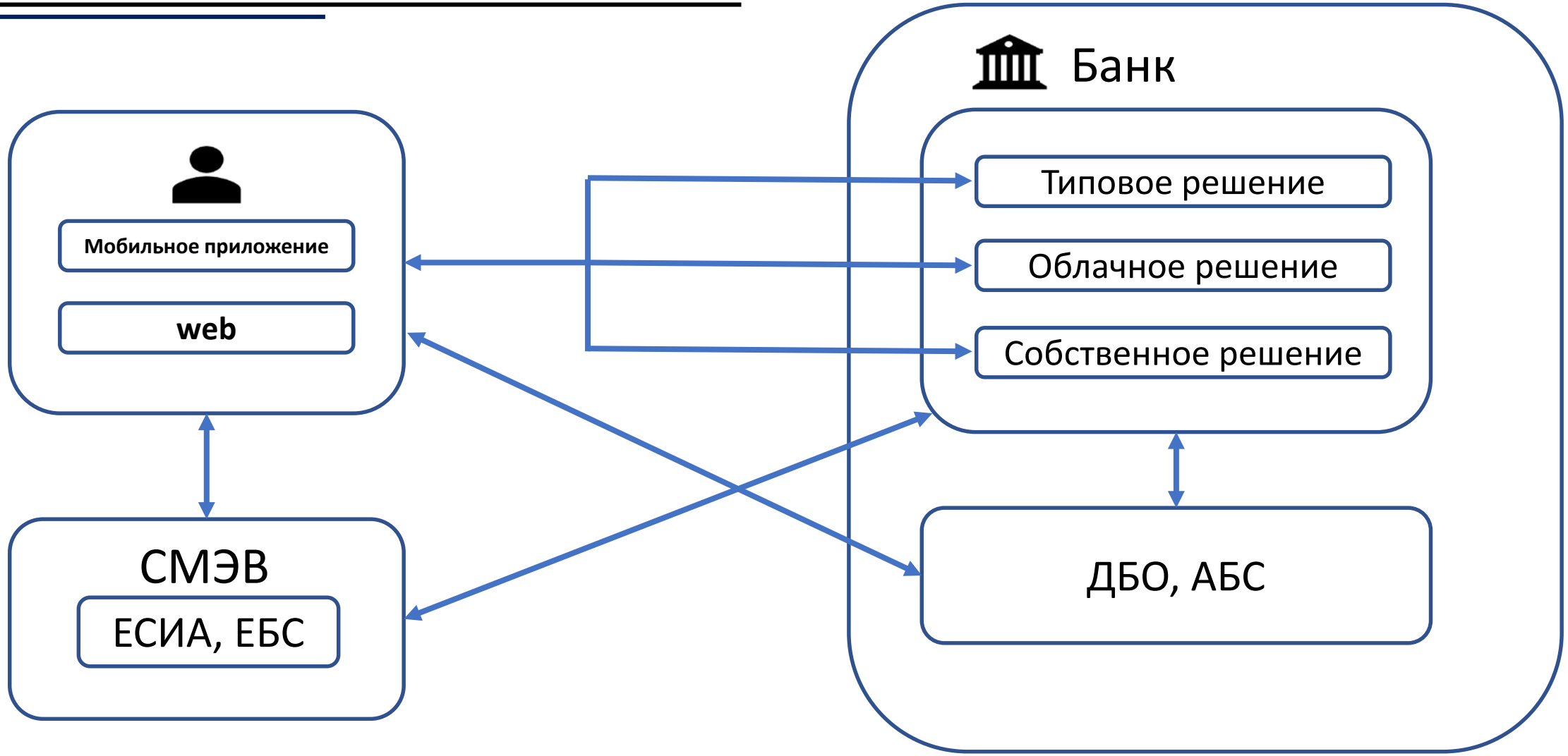
Неудобные вопросы:

- КриптоSDK прошёл Тематические исследования?
- Самостоятельное встраивание CSP (iOS, Android)
- Поэкземплярный учёт СКЗИ?
- Публикация приложений со встроенным СКЗИ на зарубежных серверах приложений (Apple AppStore, Google Play) – экспорт криптографии?

Методические рекомендации ЦБ 4-МР от 14.02.2019:

- Типовое решение
- «Облачное» решение (сервис)
- Собственное решение

Составные части решения для УБИ



Интеграция с внешними системами

1. Подключение к СМЭВ, ЕСИА и ЕБС

2. Интеграция с УЦ, выпустившим сертификат для ключа в HSM
   a) Перевыпуск сертификата по истечении срока действия
   b) Регулярное обновление CRL

3. Интеграция с УЦ, выпустившим сертификаты для операторов (сбор)
   a) Перевыпуск сертификатов по истечении срока действия
   b) Регулярное обновление CRL
   c) Отзыв сертификатов при смене сотрудника

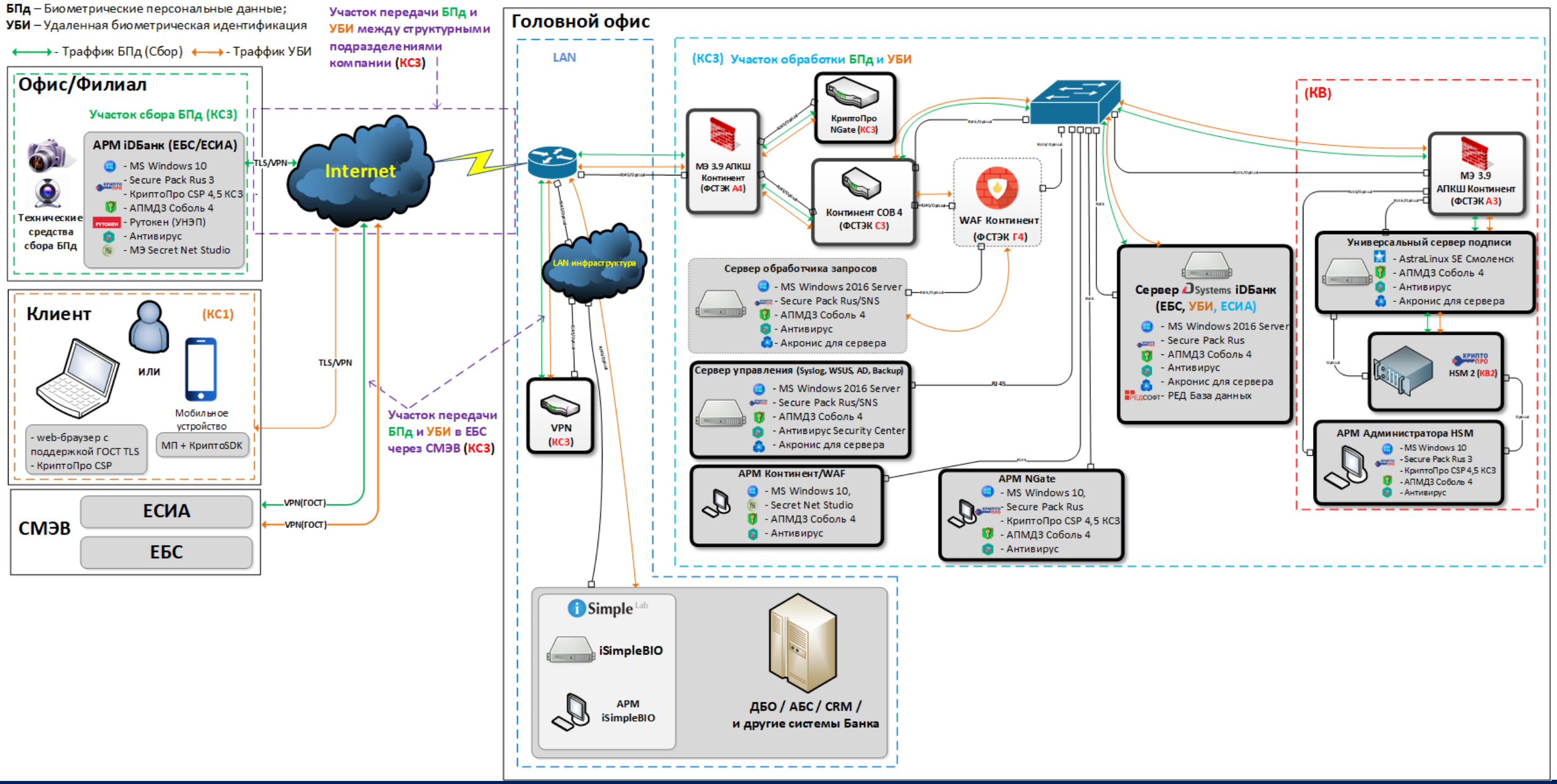
4. Договор на КриптоSDK для мобильного приложения

Протокол OpenIDConnect

- Использование ГОСТ-алгоритмов (использование сертифицированной криптографии)

- Необходимо защищать критические идентификаторы внутри протокола на всем пути:
  - Клиент – ЕСИА, ЕБС
  - Клиент – Типовое решение
  - Типовое решение – ДБО

- Сервера ДБО тоже необходимо* защищать, как часть OpenIDConnect



Общая схема взаимодействия

Сопровождение системы

Сложный проект:

- Использование СКЗИ высокого класса – требования к среде функционирования и персоналу

- Защищённый сегмент с использованием сертифицированных СЗИ (МСЭ, СОВ, WAF и др.)

- Средства защиты должны быть совместимы
  - по формулярам
  - по технике

- Сертификаты на СЗИ истекают и нужно регулярное обновление

Лёгкое решение по УБИ под ключ

Мы видим:

- Мало физических лиц сдали свои БПДн в ЕБС;
- Сжатые сроки реализации УБИ;
- Требование регулятора, а не реальная потребность бизнеса большинства банков;
- Туманные перспективы развития УБИ;
- Нужно перестраивать отлаженные процессы: регистрация клиента, выдача кредита, открытие депозита.

Мы предлагаем:

- ✓ Не тратить время на сложную полноценную автоматизацию процесса;
- ✓ Простую интеграцию с системами ДБО и АБС;
- ✓ Отдельный «front» с повышенными требованиями по ИБ;
- ✓ Переиспользование инфраструктуры для сбора БПДн на 90%;
- ✓ Решение, которое покрывает весь бизнес-процесс и удовлетворяет требованиям информационной безопасности

Вопросы?

Спасибо за внимание!

SDK Systems
ИННОВАЦИИ ЗАЩИТЫ ИНФОРМАЦИИ

+7 (499) 641 2441

post@sdksys.ru