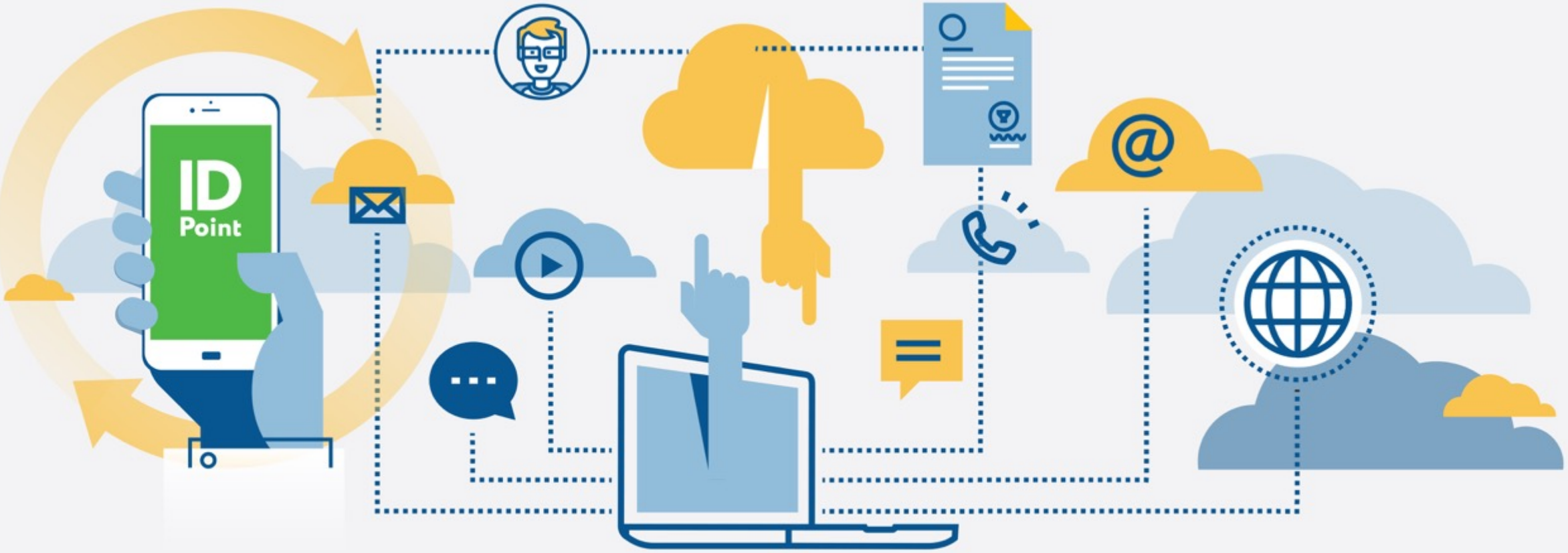
ИНФОТЕКС ТРАСТ

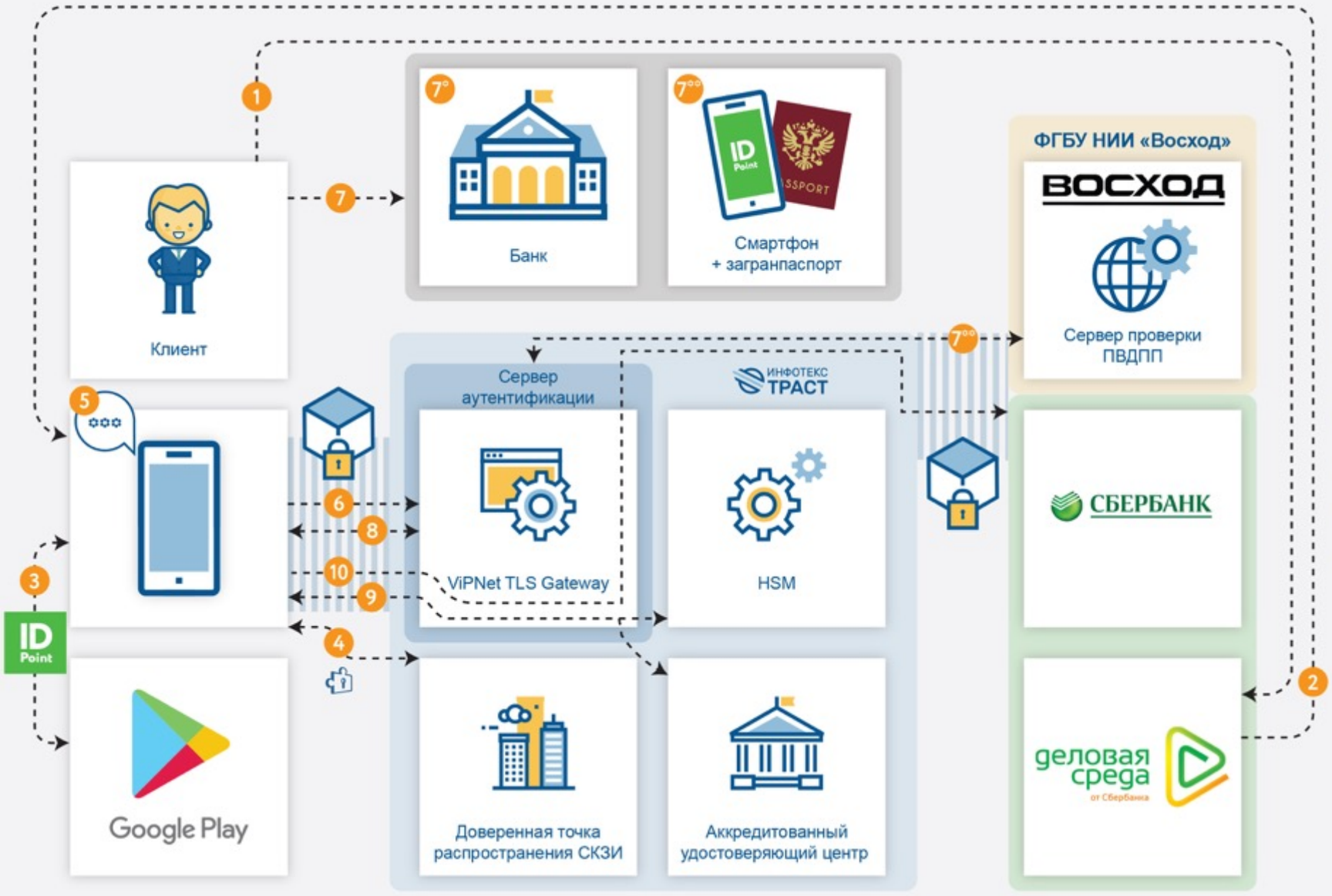
infotecs

Практические решения по обеспечению безопасности при удаленной идентификации пользователей с учетом требований ФСБ России



Докладчик: А. В. Поташников

Порядок работы с IDPoint и СЗАС



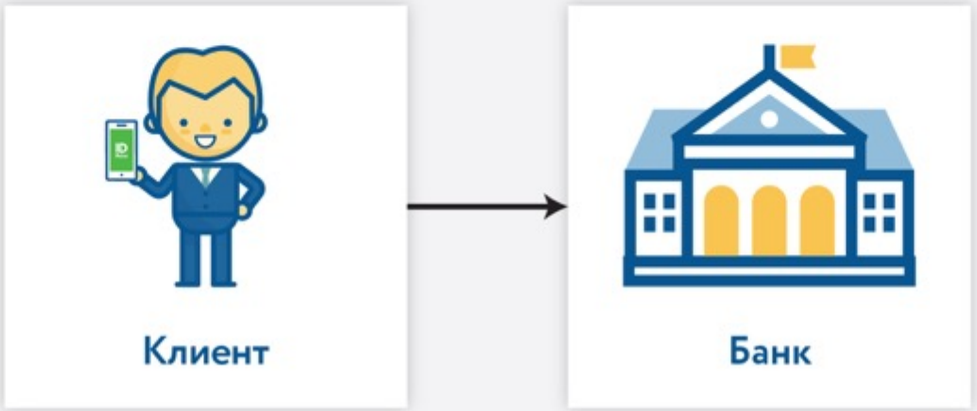
1. Ввод необходимых данных на сайте «Деловой среды»
2. СМС-сообщение со ссылкой на скачивание приложения и идентификацию клиента
3. Скачивание приложения IdPoint
4. Дозагрузка криптобиблиотеки, контроль целостности, учет СКЗИ
5. Формирование стойкого пароля
6. Установление одностороннего TLS, генерация запроса на клиентский TLS-сертификат
7. Аутентификация (7* – очная / 7** – ПВДНП), выпуск TLS-сертификата
8. Установление двухстороннего TLS-канала
9. Формирование запроса и выпуск сертификата КЭП клиента
10. Подпись документов КЭП клиента

ИНФОТЕКС ТРАСТ

infotecs

Варианты верификации клиента

Очная верификация клиента



1. Установка приложения, формирование ключей и запросов
2. Личный визит в банк
3. Верификация личности сотрудником банка и подтверждение корректности запроса на сертификат ЭП
4. Создание сертификата аутентификации
5. Создание квалифицированного сертификата

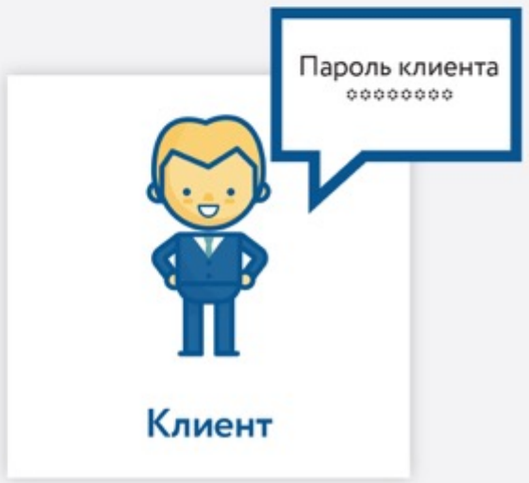
Удаленная верификация клиента

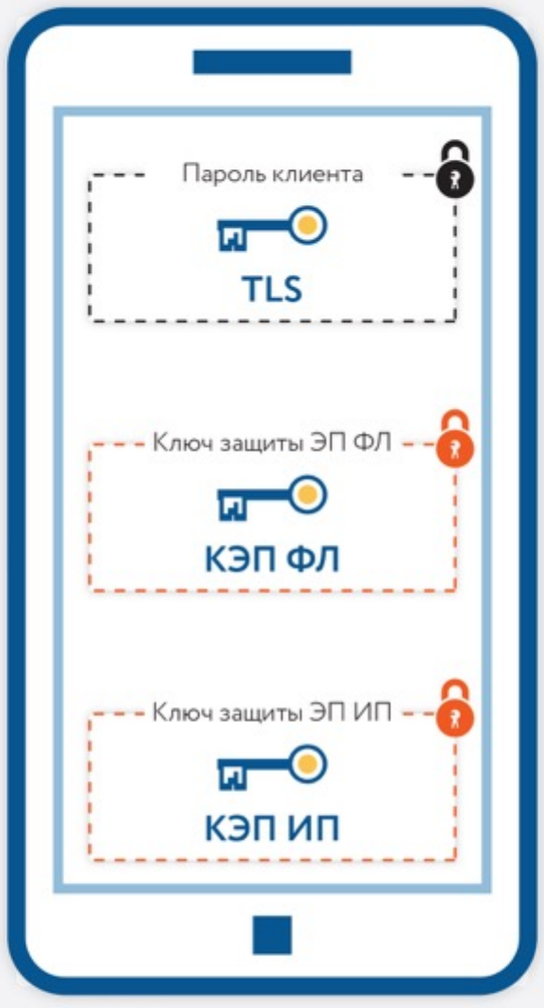
1. Установка приложения, формирование ключей и запросов
2. Считывание информации заграничного паспорта с помощью смартфона
3. Проверка данных клиента
4. Создание сертификата аутентификации
5. Создание квалифицированного сертификата

ИНФОТЕКС ТРАСТ

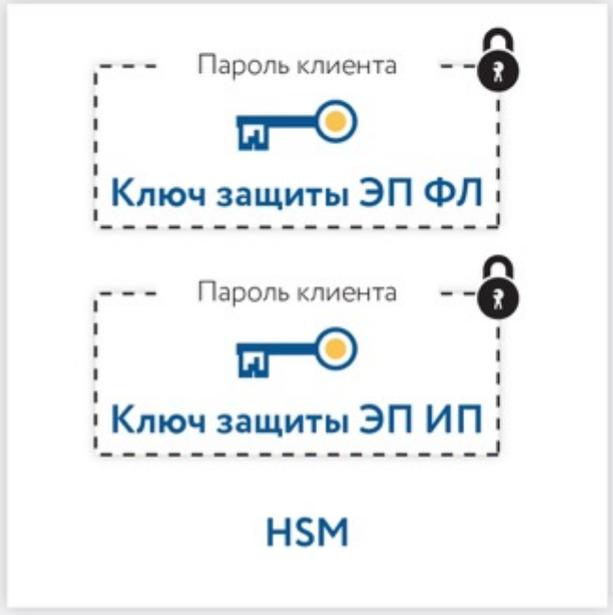
infotecs

Хранение ключей





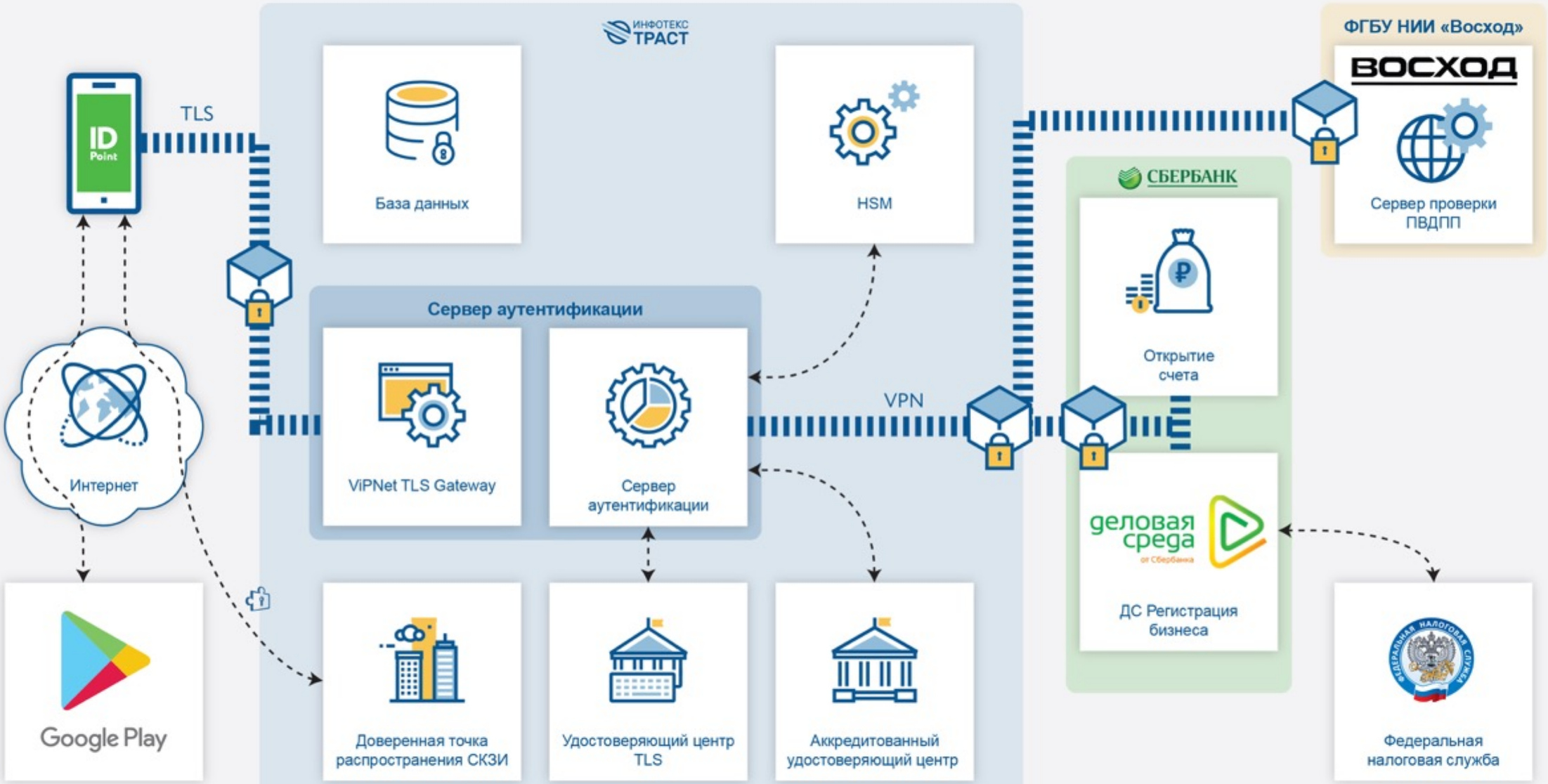
Мобильное приложение



Не допускается хранение ключей ЭП и ключей аутентификации
без их предварительного шифрования (которое должно осуществляться
встроенной функцией ПКК). При этом должно быть реализовано:

- шифрование ключа ЭП на ключе защиты посредством применения алгоритма шифрования в соответствии с ГОСТ 28147-89;
- хранение зашифрованного на пароле ключа защиты ключа ЭП в HSM.

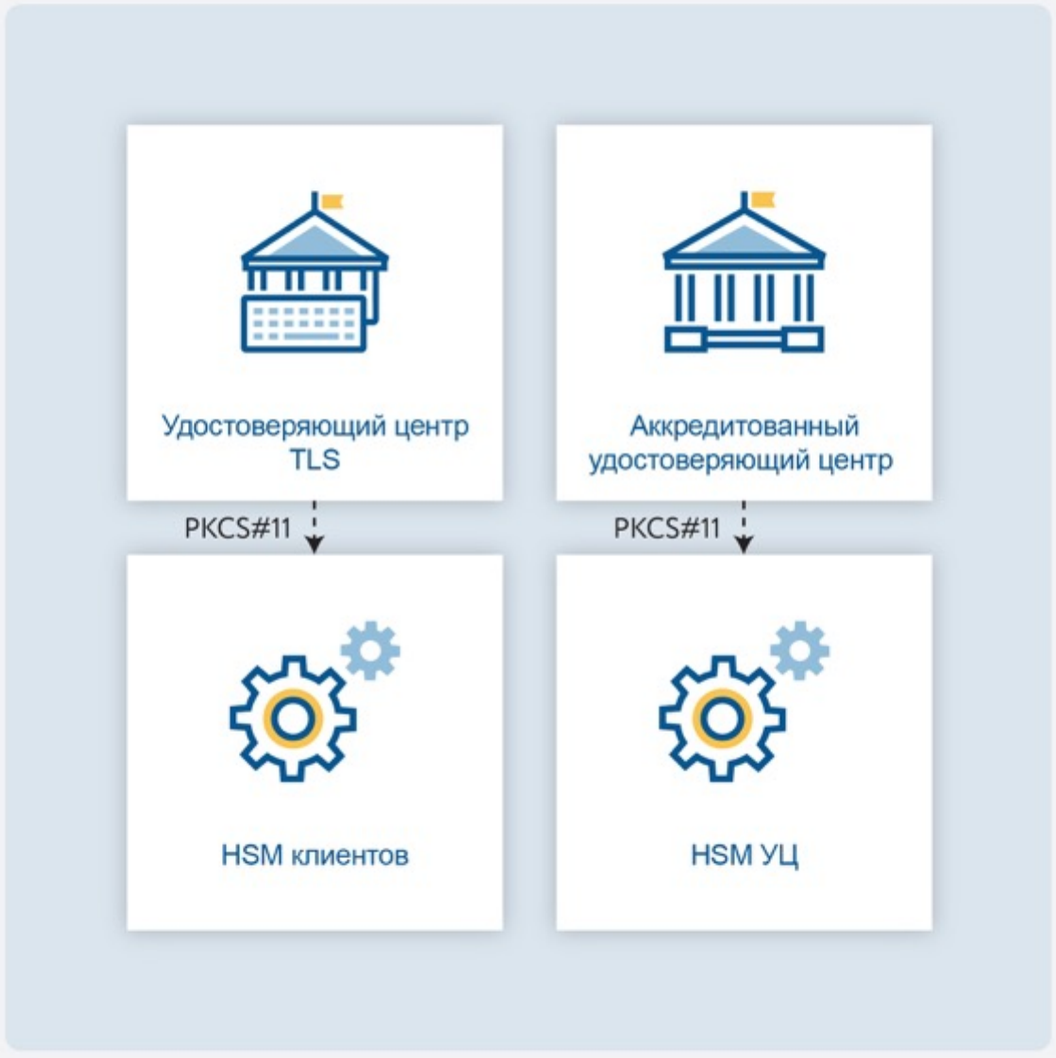
Схема компонентов специализированной защищенной автоматизированной системы



ИНФОТЕКС ТРАСТ

infotecs

Удостоверяющий центр



Средства удостоверяющего центра:

- ViPNet Удостоверяющий центр, сертификат соответствия № СФ/128-2932 (УЦ), класс КС3
- хранение ключей Удостоверяющего центра в ViPNet HSM
- поддержка алгоритмов ГОСТ Р 34.10-2001/2012
- поддержка политик разграничения доступа

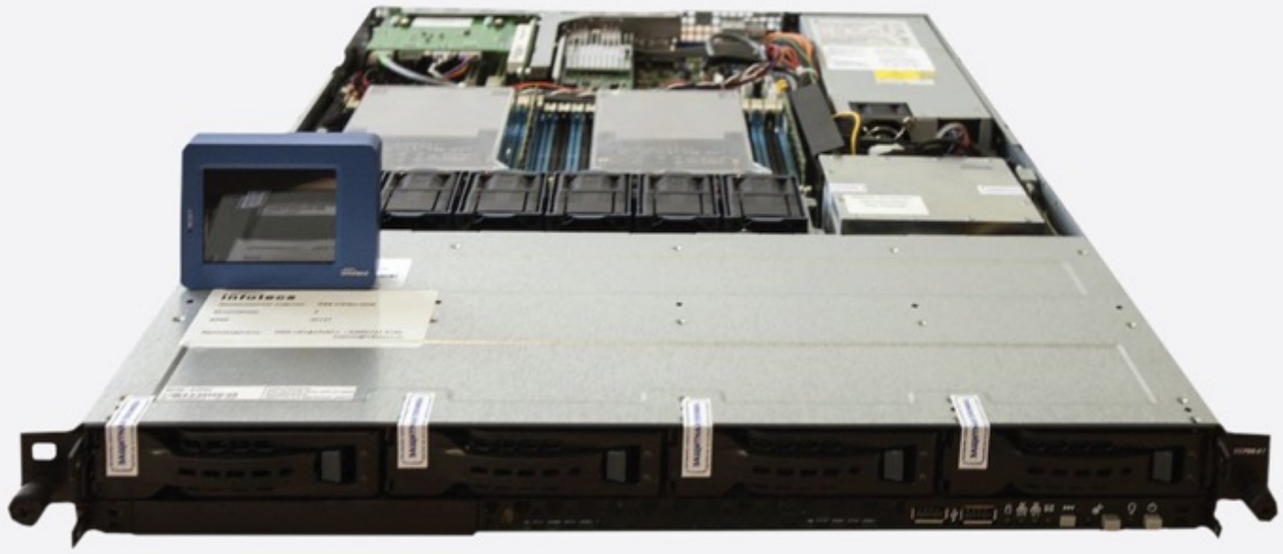
Временные требования:

- Ключи ЭП, используемые для подписи квалифицированных сертификатов и списков уникальных номеров квалифицированных сертификатов, действие которых на определенный момент было прекращено УЦ до истечения срока их действия, должны создаваться и храниться посредством ПАКМ HSM УЦ в зашифрованном на ключе защиты, формируемом по схеме разделения секрета 3 из 5, виде.
- Ключ ЭП, используемый для подписания сертификатов открытых ключей аутентификации, в УЦ должен создаваться и храниться посредством ПАКМ HSM клиентов в зашифрованном секрета 3 из 5, виде.

ИНФОТЕКС ТРАСТ

infotecs

ViPNet HSM



ViPNet HSM — высокопроизводительная и высоконадежная платформа, выполняющая криптооперации по запросам различных сервисов. ViPNet HSM может располагаться в любом окружении, так как все операции выполняются во внутренней защищенной среде: хранимые ключи невозможно извлечь, данные пользователей — изменить.

- поддержание полного жизненного цикла ключей, реализация операций ЭП и шифрования (ГОСТ 28147-89, ГОСТ Р 34.10-2001/2012)
- выполнение криптографических операций по запросам различных сервисов
- надежное хранение ключей и данных пользователя
- развитая ролевая модель, разграничение прав администраторов (кворум) и разделение секрета по схеме Шамира
- СКЗИ и средство ЭП класса КВ (КВ2), сертификат ФСБ СФ № 124-3071

ИНФОТЕКС ТРАСТ

infotecs

ViPNet TLS Gateway

ViPNet TLS Gateway — это шлюз безопасности, предназначенный для установления защищенных соединений по протоколу TLS v. 1.2 с использованием российских криптоалгоритмов ГОСТ.

- защищенный удаленный HTTPS-доступ к ресурсам (обратный прокси-сервер)
- аутентификация по сертификатам ключей проверки электронной подписи
- поддержка работы с пользователями, обладающими сертификатами ключей проверки электронной подписи, изданными различными удостоверяющими центрами
- поддержка режимов односторонней и двусторонней аутентификации
- поддержка политик разграничения доступа
- автоматическое поддержание актуальности списков аннулированных сертификатов (CRL)

Временные требования:

- Взаимодействие ПКК с СА должно осуществляться посредством защищенного протокола TLS в соответствии с рекомендациями ТК 26 «Информационная технология. Криптографическая защита информации. Использование российских криптографических алгоритмов в протоколе безопасности транспортного уровня (TLS 1.2)».

ИНФОТЕКС ТРАСТ

infotecs

Защита каналов

ПАК ViPNet Coordinator KB:

- СКЗИ класса КВ2
- МСЭ 4 класса по требованиям ФСБ

ПАК ViPNet Coordinator HW 1000:

- СКЗИ класса КС3
- МСЭ 4 класса по требованиям ФСБ
- МСЭ типа А4 класса по требованиям ФСТЭК

Временные требования:

- При организации сетевого взаимодействия СК СЗАС между собой в случае их размещения в разных контролируемых зонах, каналы связи (сети связи) между этими компонентами должны быть защищены с использованием СКЗИ, сертифицированных ФСБ России по классу не ниже КВ, либо быть выделенными в соответствии с Федеральным законом от 07.07.2003 № 126-ФЗ «О связи».

ИНФОТЕКС ТРАСТ

infotecs

Временные требования

- Для ограничения возможностей по построению каналов атак на СА, сервер БД, сервер передачи электронных документов участников эксперимента, сервер проверки электронной подписи и ДТР ПКК (далее – серверные компоненты СЗАС, СК СЗАС) с использованием каналов связи должны применяться межсетевые экраны уровня веб-сервера (тип «Г»), сертифицированные на соответствие Требованиям к межсетевым экранам, утвержденным приказом ФСТЭК России от 9 февраля 2016 г. № 9, по 1, 2, 3 или 4 классу защиты.

- Для обеспечения обнаружения компьютерных программ или иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования защищаемой информации или нейтрализации средств защиты информации, а также реагирования на обнаружение этих программ и информации должны применяться средства антивирусной защиты, сертифицированные на соответствие Требованиям к средствам антивирусной защиты, утвержденным приказом ФСТЭК России от 20 марта 2012 г. № 28, по 1, 2, 3 или 4 классу защиты.

- Для обнаружения вторжений, направленных на преднамеренный несанкционированный доступ к информации, специальные воздействия на средства защиты информации и (или) информацию в целях ее добывания, уничтожения, искажения и блокирования доступа к информации, а также для реагирования на эти действия (предотвращение этих действий) должны применяться системы обнаружения вторжений, сертифицированные на соответствие Требованиям к системам обнаружения вторжений, утвержденным приказом ФСТЭК России от 6 декабря 2011 г. № 638, по 1, 2, 3 или 4 классу защиты.

ViPNet IDS

ViPNet IDS — это программно-аппаратный комплекс, предназначенный для обнаружения компьютерных атак (вторжений) в информационные системы за счет динамического анализа сетевого трафика всех уровней модели взаимодействия открытых систем ISO/OSI, начиная с канального и заканчивая прикладным.

- возможность обнаружения компьютерных атак (вторжений) на основе сигнатурного и эвристического метода выявления аномалий в сетевом трафике
- регистрация информации об обнаруженных событях и атаках для последующего анализа
- регистрация географического положения источника атаки
- база сигнатур атак российского производства — содержит более 20 000 правил, поставляется и обновляется ЗАО «Перспективный мониторинг»
- ролевая модель доступа к системе управления
- расследование инцидентов ИБ
- подключение к «Корпоративному центру обнаружения, предупреждения и ликвидации последствий компьютерных атак ИнфоТеКС» или к «Центру мониторинга ИнфоТеКС» с целью повышения уровня защищенности информационных систем

ИНФОТЕКС ТРАСТ

infotecs

Спасибо за внимание!

Вопросы?

ОАО «ИнфоТеКС»
ОАО «Инфотекс Интернет Траст»

Александр Поташников
Potashnikov@infotecs.ru

Москва, Старый Петровско-
Разумовский проезд, 1/23, стр. 1

8 800 250-0-260
iitrust.ru