ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ
«НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ИНСТИТУТ «ВОСХОД»

Методы и механизмы защиты информации паспорта с электронным носителем гражданина РФ

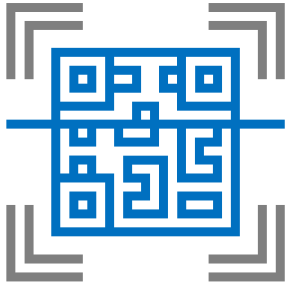
Вдовина Мария Сергеевна

19 марта 2020 года

Микросхема как средство защиты

- Соответствие требованиям приказа ФСБ №796 к средству электронной подписи и требованиям к СКЗИ по классу КВ
- Поддержка квалифицированных сертификатов в соответствии с требованиями приказа ФСБ №795
- Поддержка протокола базового контроля доступа BAC в соответствии с ДОК ИКАО 9303
- Поддержка усовершенствованного протокола базового контроля доступа PACE в соответствии с ДОК ИКАО 9303
- Поддержка аналога PACE на российских алгоритмах – SESPAKE в соответствии с методическими рекомендациями ТК26
- Поддержка сертификатов безопасности для аутентификации по протоколу TLS
- Поддержка протокола расширенного контроля доступа EAC, в том числе на российских криптографических алгоритмах
- Установление защищенного соединения с использованием QR-кода (MRZ-строки)
- Применение КЭП после ввода владельцем PIN-кода
- Поддержка сертификатов специального формата (CV) для санкционирования доступа терминалам к данным
- Сертификация ОС микросхемы по требованиям ФСТЭК России

Механизмы защиты

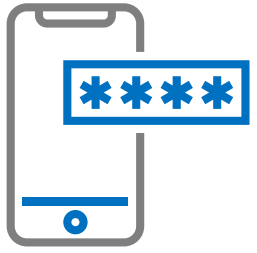


QR-КОД И SESPAKE

- Чтение QR-кода
- Генерация эфемерных сеансовых ключей
- Установление защищенного соединения
- Пассивная аутентификация

EAC И CV-СЕРТИФИКАТЫ

- Аутентификация микросхемы
- Аутентификация терминала
- Чтение CV-сертификата и предоставление доступа



PIN-КОД К КЛЮЧУ АУТЕНТИФИКАЦИИ И ЭП

Использование сертификата безопасности

- Ввод pin-кода
- Установление защищенного соединения

Использование ключа ЭП

- Визуализация документа
- Ввод pin-кода

Методы доступа к данным

№	Данные	SESPAKE (BAC/PACE) и QR-код	EAC и CV-сертификат	PIN
1	Чтение приложения ePassport, за исключением отпечатков пальцев	+	-	-
2	Чтение отпечатков пальцев	+	+	-
3	Чтение неизменяемых и изменяемых метрических, дополнительных данных и фотографии приложений eID и eDL	+	-	-
4	Изменение перезаписываемых метрических и дополнительных данных приложения eID и eDL	+	+	-
5	Применение сертификата безопасности приложения eSign	+	-	+
6	Подпись с помощью ключа КЭП приложения eSign	+	+	+

Терминалы применения

ОБЫЧНЫЙ ТЕРМИНАЛ

- Работа онлайн и офлайн
- Выполнение ограниченного набора функций
- СКЗИ КС1
- Наличие корневых сертификатов УЦ эмиссии и контроля/ИКАО
- Поддержка протокола SESPAKE (BAC/PACE)
- Доступ к сертификату безопасности

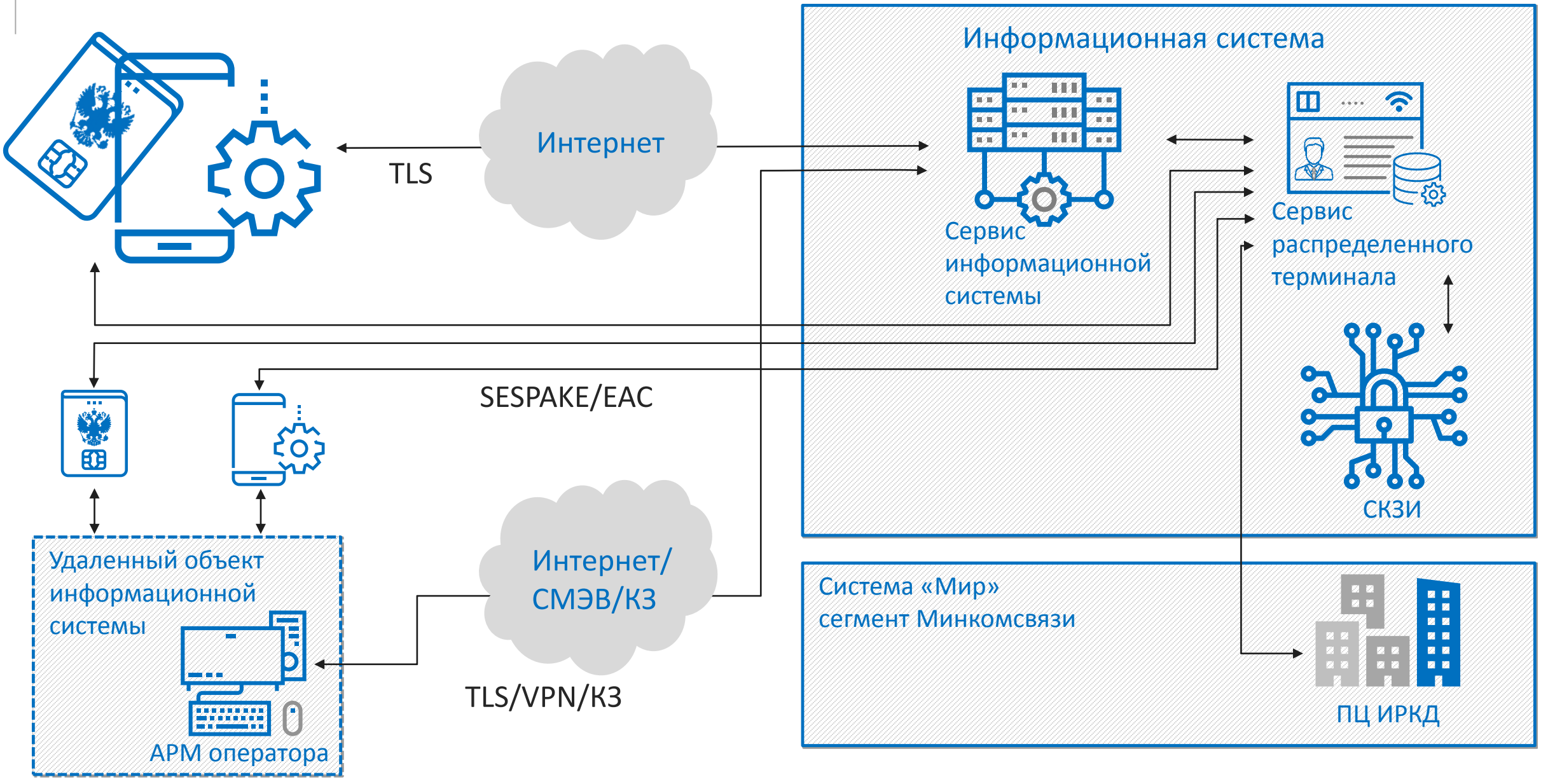
ДОВЕРЕННЫЙ ТЕРМИНАЛ

- Работа онлайн и офлайн
- Полный набор функций
- СКЗИ КС3
- Наличие корневых сертификатов УЦ эмиссии и контроля/ИКАО
- Поддержка протокола SESPAKE (BAC/PACE)+EAC
- Доступ к сертификату безопасности
- Наличие CV-сертификатов
- Верификация отпечатков пальцев
- Применение КЭП

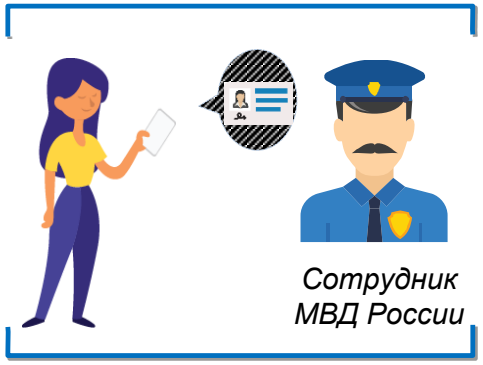
РАСПРЕДЕЛЕННЫЙ ТЕРМИНАЛ (ФЕДЕРАЛЬНЫЙ И ЛОКАЛЬНЫЙ)

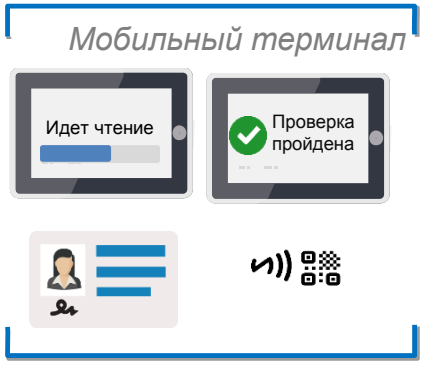
- Работа онлайн
- Централизованное выполнение функций, терминал как сервис
- СКЗИ класса от КС1 до КС3
- Наличие корневых сертификатов УЦ эмиссии и контроля/ИКАО
- Поддержка протокола SESPAKE (BAC/PACE)+EAC
- Доступ к сертификату безопасности
- Наличие CV-сертификатов
- Верификация отпечатков пальцев
- Применение КЭП в ограниченных случаях

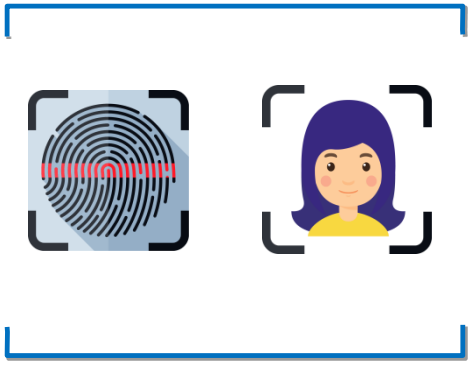
Распределенный терминал

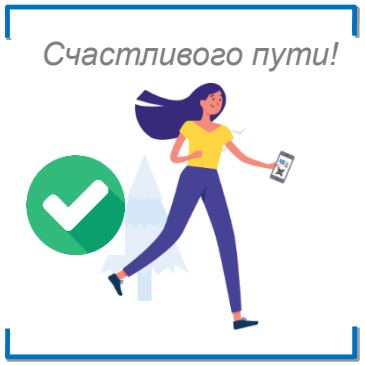


Доверенный терминал и паспорт







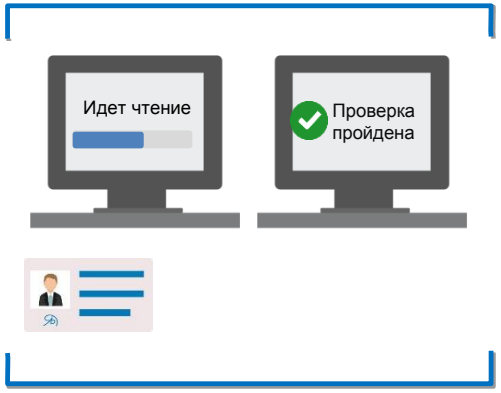


1 Предъявление паспорта с электронным носителем

2 Чтение данных и проверка подлинности

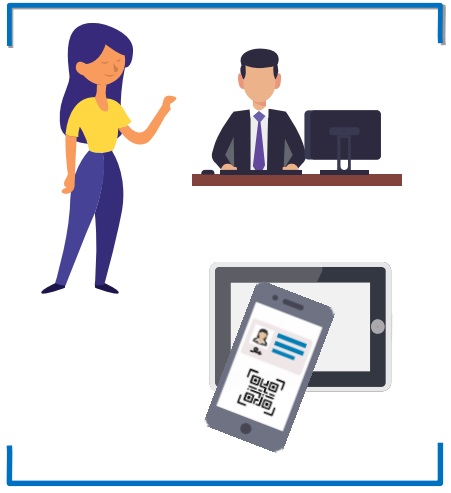
3 Биометрическая верификация гражданина

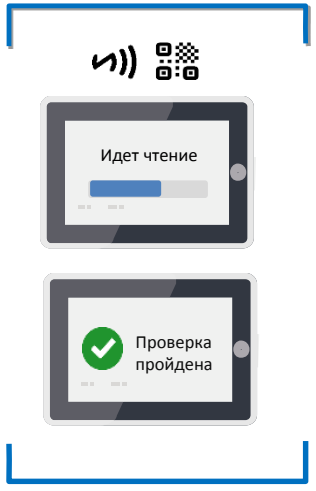
4 Удостоверение личности и проверка документа успешны

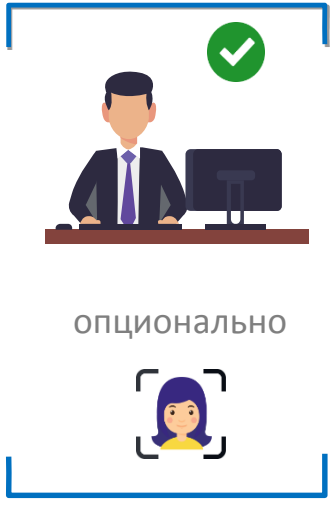


Доверенный терминал и мобильное приложение

Сфера применения: в МФЦ при получении услуг, не требующих применения КЭП для юридически значимых действий

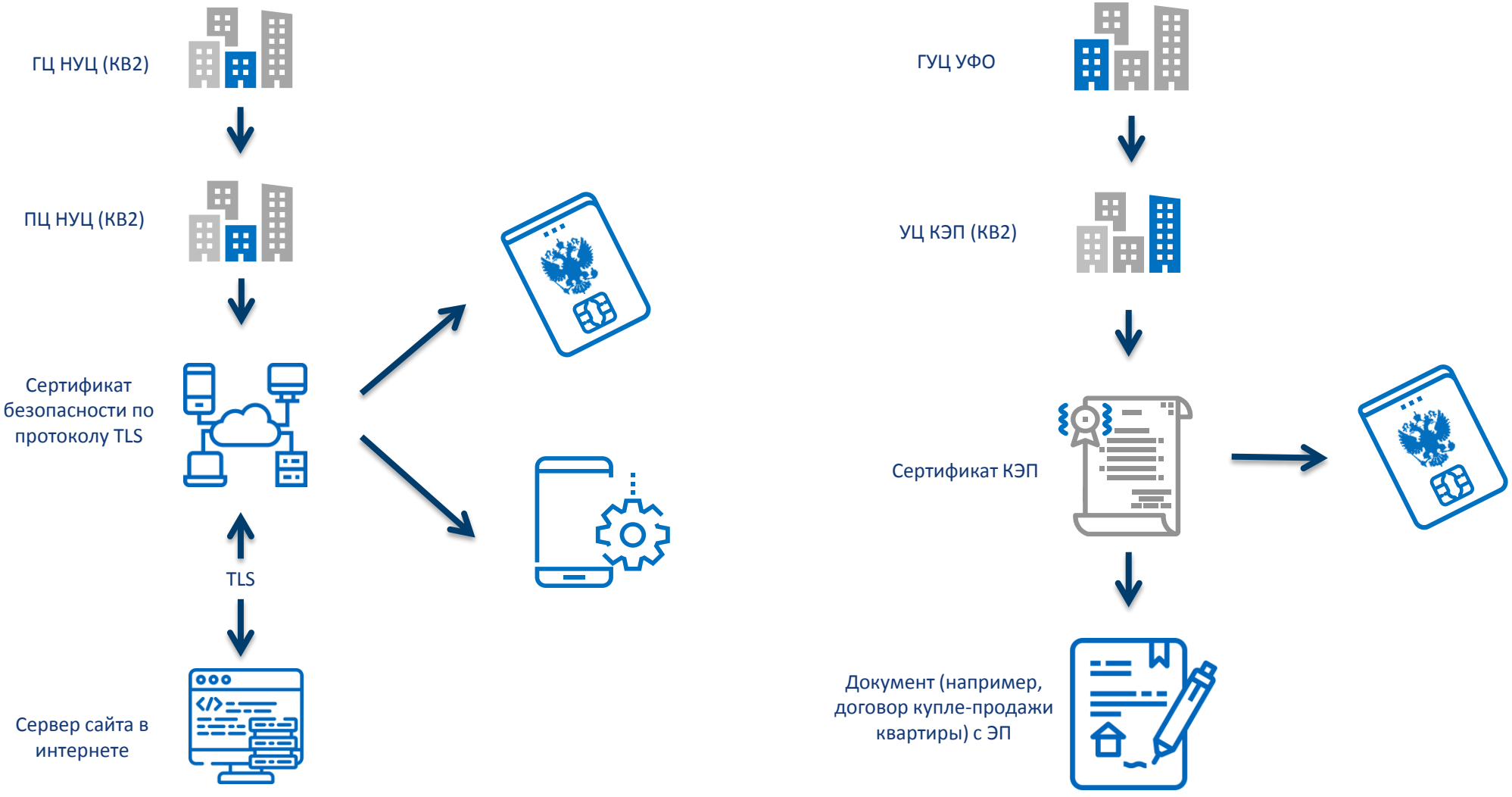






1. Предъявление мобильного приложения
2. Чтение данных и проверка подлинности
3. Автозаполнение форм
4. Верификация гражданина
5. Применение сертификата безопасности

Состав и применение приложения электронной подписи паспорта и мобильного приложения



План мероприятий