НИИ ВОСХОД

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

О реализации мероприятий по переходу на отечественную криптографию между государством и обществом

Андрей Пьянченко
Заместитель директора

План М. В. Мишустина

ПЛАН МЕРОПРИЯТИЙ
по формированию Единого цифрового контура идентификации

УТВЕРЖДАЮ
Председатель Правительства
Российской Федерации
М.Мишустин

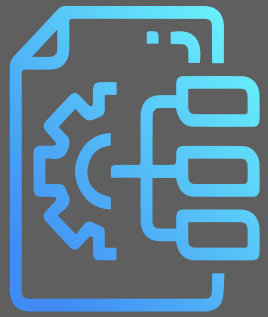
16 декабря 2020 г.
№ 12067п-П10

ПЛАН МЕРОПРИЯТИЙ

по формированию Единого цифрового контура идентификации

№ п/п	Наименование мероприятия	Вид документа и форма реализации	Ожидаемый результат	Срок исполнения	Исполнитель (соисполнитель)
	1. Проектирование единого цифрового контура				
1.1.	Разработка концепции и целевой архитектуры Единого цифрового контура идентификации	Проект распоряжения Правительства Российской Федерации	Утверждена концепция и целевая архитектура единого цифрового контура идентификации, обеспечивающего для граждан удобную и безопасную идентификацию и аутентификацию, подписание электронных документов, а также совершение иных юридически значимых действий в электронном виде	1 марта 2021 г.	Минцифры России, МВД России, ФСБ России при участии Банка России

Структура плана М. В. Мишустина



- Проектирование единого цифрового контура
- Развитие усиленной электронной подписи
- Развитие Единой системы идентификации и аутентификации
- Развитие биометрических технологий идентификации
- Введение новых цифровых решений для идентификации и аутентификации

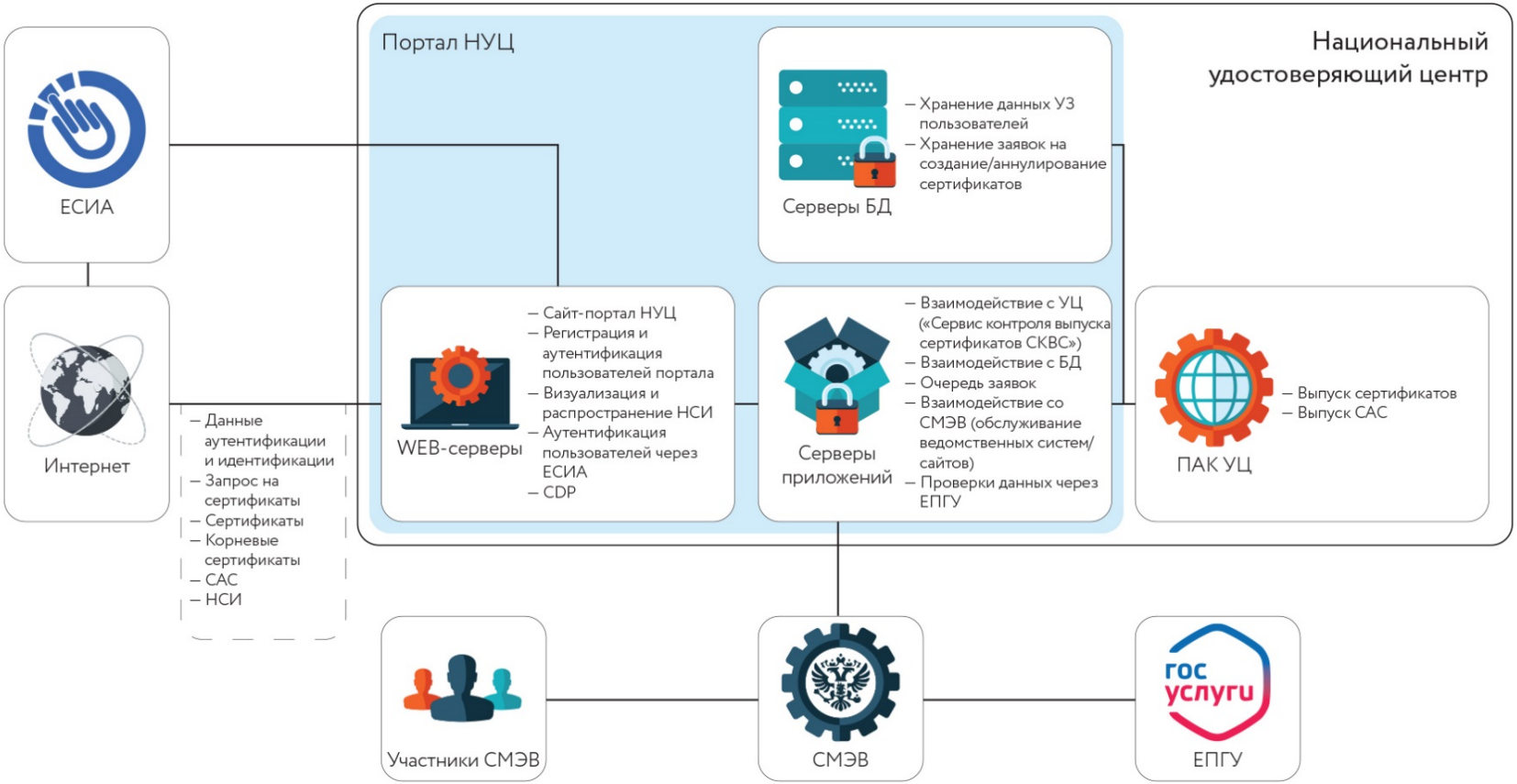
Национальный удостоверяющий центр

Результаты проекта

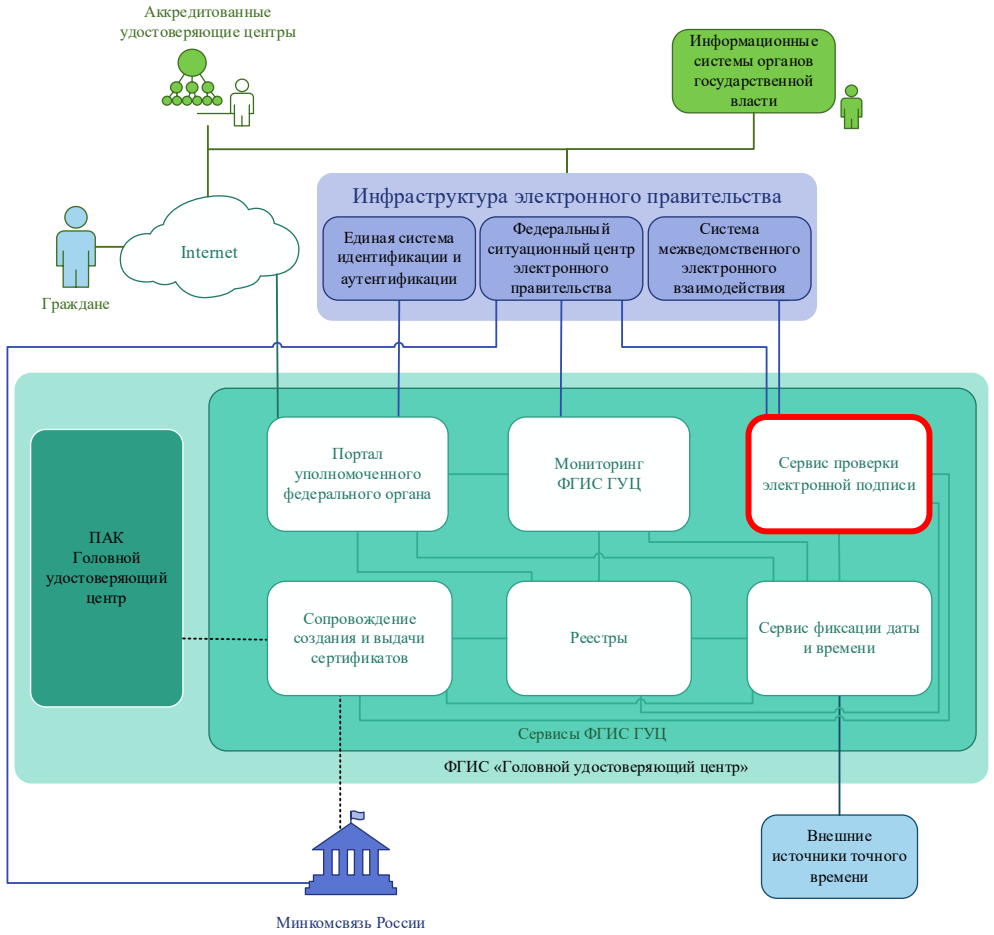
- Владельцы сайтов могут получить отечественный сертификат безопасности
- Гражданин может удостовериться в подлинности сайтов на основе отечественной криптографии
- Канал между гражданином и веб-ресурсом защищен

Национальный удостоверяющий центр

Архитектура



Сервис проверки неквалифицированных сертификатов для платформы Госключ



Текущий проект паспорта с электронным носителем

Паспорт с электронным носителем

- Многослойный пластик
- Визуально читаемые данные
- Полиграфическая защита
- Формат ID1

- Бесконтактная микросхема
- Полностью российская, 1 уровень (согласно постановлению Правительства)
- Криптография по ГОСТ
- Соответствие требованиям ICAO DOC9303

Терминалы применения для ПЭН

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

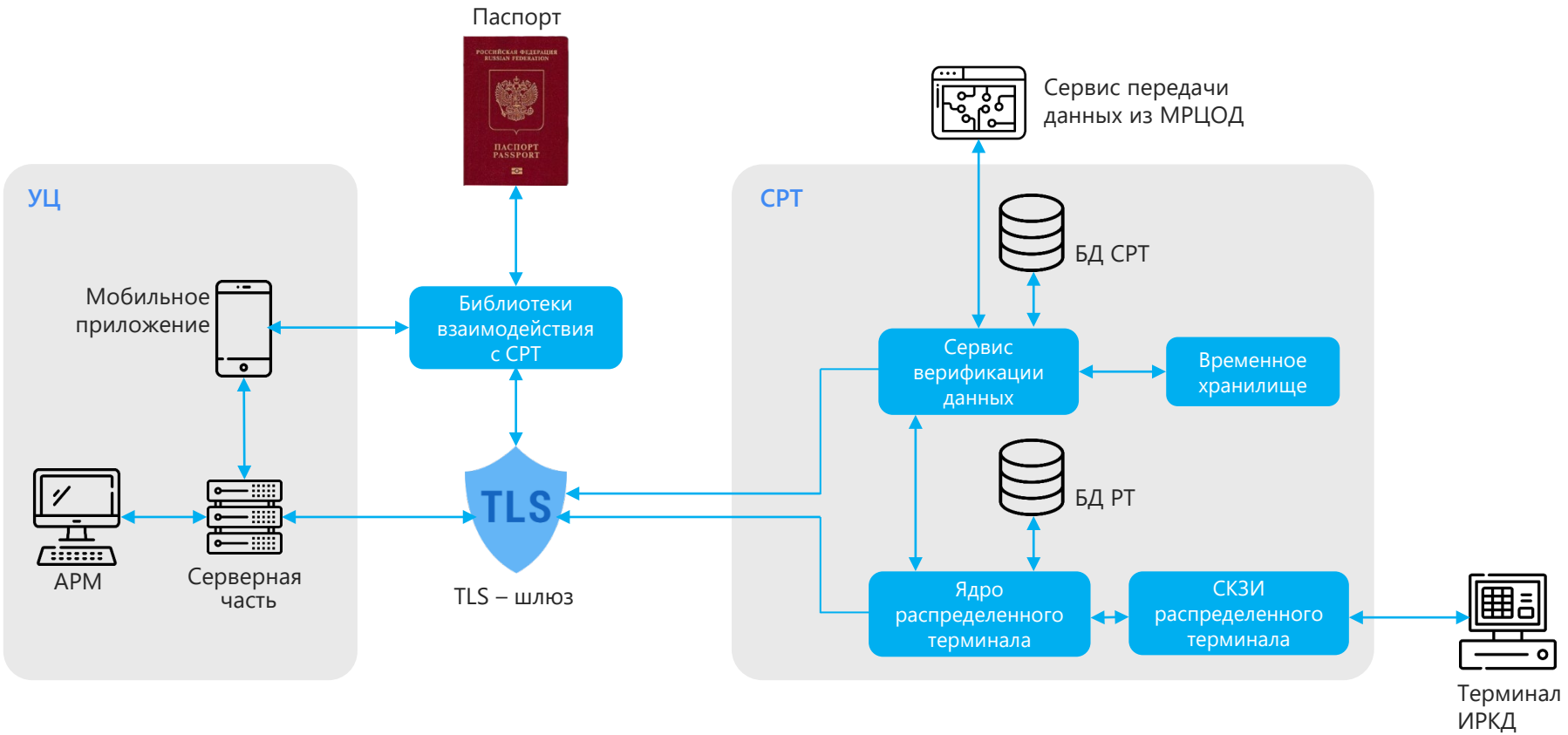
Распределенный терминал (федеральный и локальный)

- 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 (только для локального)
- Применение КЭП в ограниченных случаях

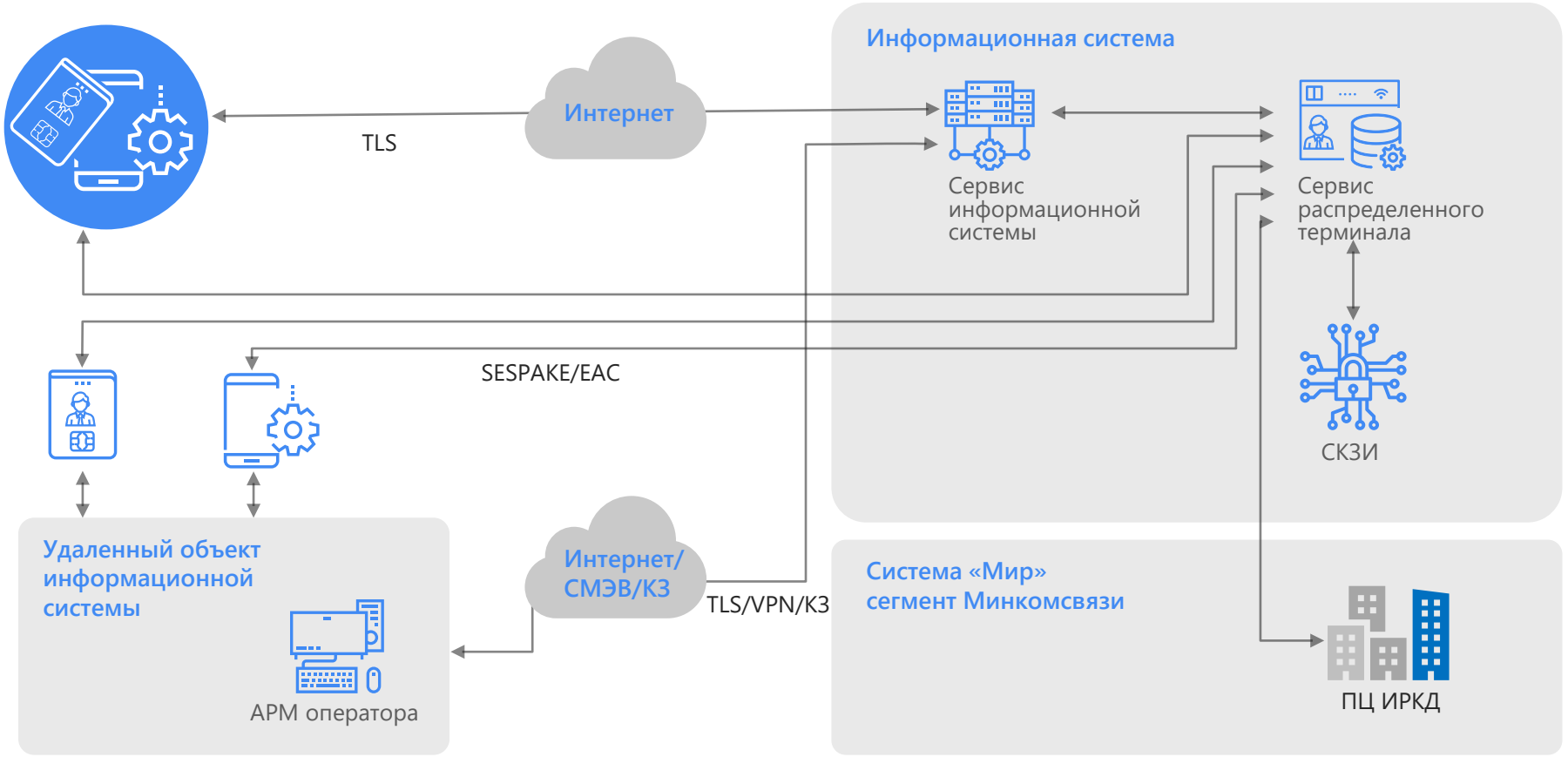
Доверенный терминал

- 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

Система удаленного доступа к микросхеме



Распределенный терминал



СКЗИ «КриптоВС Х»

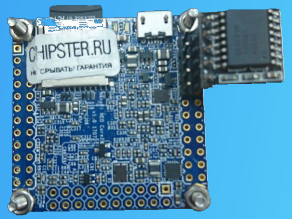
Исполнения СКЗИ «КриптоВС Х»

СКЗИ ПАК «КриптоВС Х» в серверном исполнении

- На базе процессора с архитектурой Эльбрус
- На базе процессора с архитектурой x86-64 (на базе ядра Linux)

СКЗИ ПАК «КриптоВС Х» в настольном исполнении

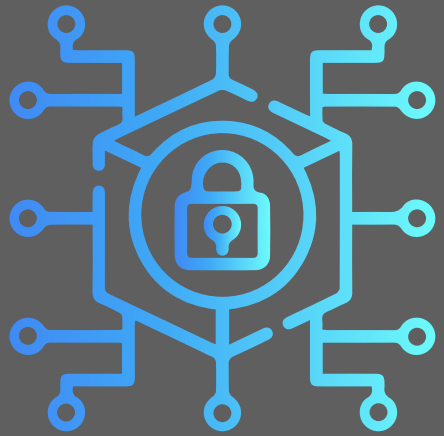
В форм-факторе компактного подключаемого устройства с возможностью взаимодействия с внешними подключаемыми ключевыми носителями



СКЗИ ПАК «КриптоВС Х» в мобильном исполнении

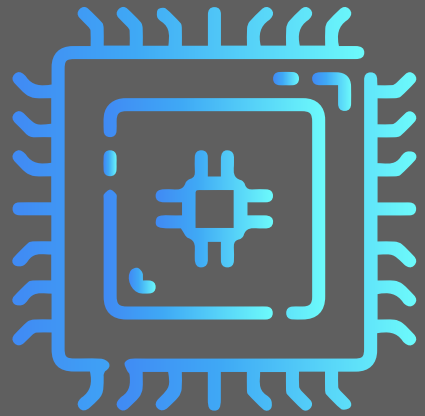
В форм-факторе компактного подключаемого устройства без возможности взаимодействия с внешними подключаемыми ключевыми носителями

Особенности СКЗИ



- Разнообразие аппаратных платформ
- Выполнение всех основных криптографических операций как на отечественных, так и на зарубежных криптоалгоритмах
- Наличие прикладного программного интерфейса (API)
- Наличие web-интерфейса администрирования, позволяющего выполнять настройку и управление ключевым хранилищем СКЗИ
- Возможность использования внешних ключевых носителей, в том числе функциональных (в серверном и настольном исполнениях)
- Использование в серверном исполнении программного интеграционного модуля для обеспечения взаимодействия СКЗИ с ключевыми носителями
- Работа с микросхемой ПВДНП

Возможность работы СКЗИ «КриптоВС X» с новой микросхемой ПВДНП



- Выполнение протокола установления соединения с аутентификацией паролем (PACE) на базе зарубежных криптографических алгоритмов, а также с использованием протокола SESPAKE на основе ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012 и осуществление защищенного обмена с интегральной микросхемой

- Выполнение протокола расширенного контроля доступа (EAC) в соответствии с ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012 и осуществление защищенного обмена с интегральной микросхемой

Особенности КриптоВС М

- СКЗИ класса КС1
- Возможность работы под управлением ОС Android и IOS в различных исполнениях
- СКЗИ является приложением с API для возможности встраивания
- Выполнение всех основных криптографических операций как на отечественных (ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012, ГОСТ 34.10-2018, ГОСТ Р 34.11-94, ГОСТ Р 34.11-2012, ГОСТ 34.11-2018, ГОСТ 28147-89, ГОСТ Р 34.12-2015, ГОСТ Р 34.13-2015, ГОСТ 34.12-2018, ГОСТ Р 34.13-2018), так и на зарубежных (ECDSA, SHA-1, SHA-224, SHA-256, SHA-384 и SHA-512, AES и 3DES) криптоалгоритмах
- Работа с микросхемой ПВДНП (в том числе с выполнением SESPAKE и EAC для функции Chip Authentication)

Что в итоге?

- СКЗИ для применения ПЭН
- Новые инструменты идентификации
- Независимость от западных УЦ
- Защита пользовательских данных
- Новые сервисы для информационных систем и граждан