



Криптография в массовых банковских продуктах: 851-П, Цифровой рубль, биометрия, подпись

Спикер

Павел Луцик

Эволюция криптографии в банковской сфере

- /// Российская криптография в инфраструктуре банков
- /// Отсутствие регулирования криптографии на массовых клиентских устройствах



- /// Цифровой рубль
- /// 851-П
- /// Биометрия
- /// Мобильная подпись

851-П. Защита безналичных платежей

5.1. Кредитные организации...должны обеспечить целостность электронных сообщений. В целях обеспечения целостности...кредитные организации...должны обеспечивать реализацию мер по использованию любого вида усиленной ЭП, предусмотренной ч.1 ст.5 63-ФЗ, или СКЗИ, реализующих функцию имитозащиты информации с аутентификацией отправителя сообщения.



■ **Использование СКЗИ
КС1**

■ **Использование средств
УЦ КС2**



Электронная подпись

Федеральный закон "Об
электронной подписи" от
06.04.2011 N 63-ФЗ



- /// Распределенно в мобильном приложении и на серверной стороне в ПАКМ КriptoПро HSM.
- /// Локально в мобильном приложении с поддержкой ключевых носителей, подключаемых бесконтактно по NFC или контактно с использованием совместимых носителей.
- /// Локально на рабочем месте пользователя на традиционных ключевых носителях при работе через веб-интерфейс (режим КriptoПро Ключ Lite)

Цифровой рубль

Положения Банка России

▀ «О Платформе Цифрового рубля» № 820-П от 03.08.2023

▀ «О требованиях к обеспечению защиты для участников платформы цифрового рубля» № 833-П от 07.12.2023



▀ СКЗИ КС1 (ПМ БР, веб)

▀ УЦ для ЭП КС3

▀ УЦ для TLS КС3



Биометрия

Федеральный закон 572-ФЗ от 29.12.2022

18-МР к указанию БР №6540-У – для фин. организаций, взаимодействие с ЕБС

19-МР к указанию БР №6541-У – для фин. организаций, взаимодействие с КБС

Угрозы безопасности при идентификации и/или аутентификации с помощью биометрии



Классы криптосредств (СКЗИ)

Биометрия

Целостность и конфиденциальность биометрии при идентификации и/или аутентификации

**КриптоSDK (КПМ ЕБС) со встроенным
СКЗИ КриптоПро CSP 5.0 R2 KC1**

▀ Аутентификация в ЕСИА + ЕБС (OpenID Connect)

▀ Построение ГОСТ-TLS

СКЗИ КриптоПро CSP 5.0 R3 KC1/KC2

▀ Построение ГОСТ-TLS

▀ CMS-шифрование, ЭП (защита на прикладном уровне)



Клиентское устройство



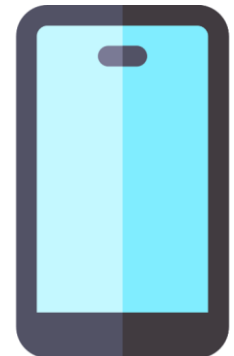
СКЗИ KC1/KC2

Переиспользование СКЗИ



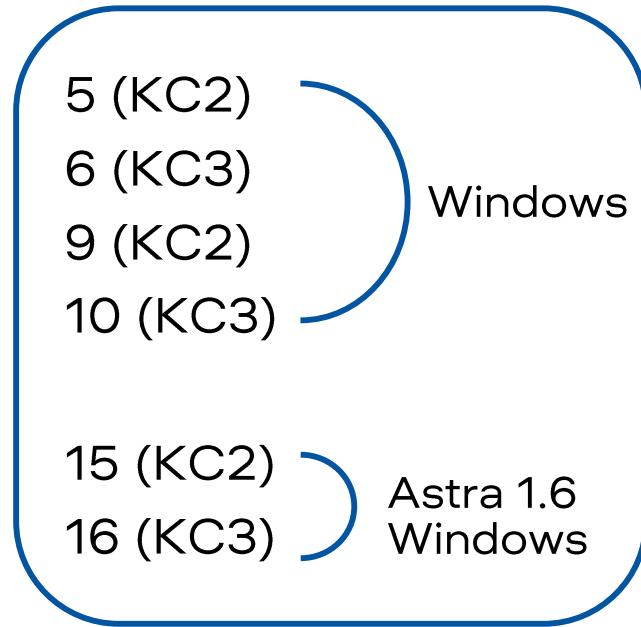
Основные преимущества переиспользования СКЗИ

- /// Сокращение размера мобильного приложения
- /// Сокращение затрат на разработку при встраивании и обновлении СКЗИ
- /// Сокращение затрат на приобретение лицензий на СКЗИ
- /// Упрощение пользовательского пути (пример: однократный вызов БиодСЧ)

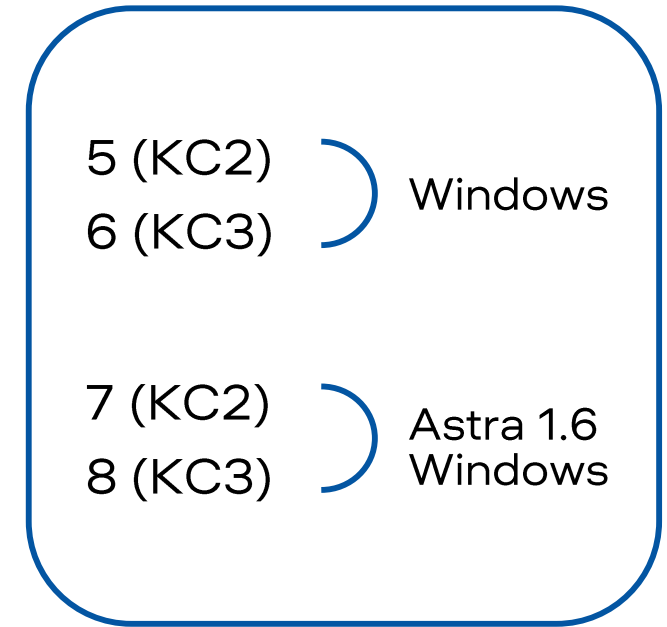


КриптоПро УЦ 2.0 и Службы УЦ 2.0

УЦ 2.0



Службы УЦ 2.0



- КриптоПро УЦ 2.0 (исп. 15 и 16) - текущая версия
- API для интеграции текущей версии отличается от API предыдущих (было SOAP, стало REST)

Поддерживаемые ОС и СУБД КриптоПро УЦ 2.0 (исп. 15, 16)

УЦ допустимо использовать на следующих ОС:

- ОС Astra Linux SE 1.6 (идет согласование с ФСБ возможность использования версии 1.7)
- Семейство Windows Server 2008R2/2012/2012R2/2016/2019

УЦ поддерживает следующие СУБД:

- PostgreSQL 9.6 и выше
- Microsoft SQL Server 2012/2014/2016/2017/2019

КриптоПро УЦ 2.0 (исп. 15, 16) – на текущий момент **единственное** средство УЦ, сертифицированное ФСБ России под российскую ОС

Комплектация ПАК КryptoПро УЦ 2.0 (исп. 15 КС2, 16 КС3)

- Программные компоненты ПАК КryptoПро УЦ 2.0
 - Межсетевой экран не ниже 4 класса защиты ФСБ
 - СКЗИ КryptoПро CSP 5.0 R2 или ПАКМ КryptoПро HSM 2.0
 - Средства защиты от НСД типа «Электронный замок»
 - Сервер точного времени
-
- СЗИ SPR - для ОС Windows (для Astra Linux - не требуется, достаточно встроенного режима ЗПС)

Исп. 15 КС2

Исп. 16 КС3

Исп. 16 КС3

Структурная схема компонент УЦ

Состав компонент:

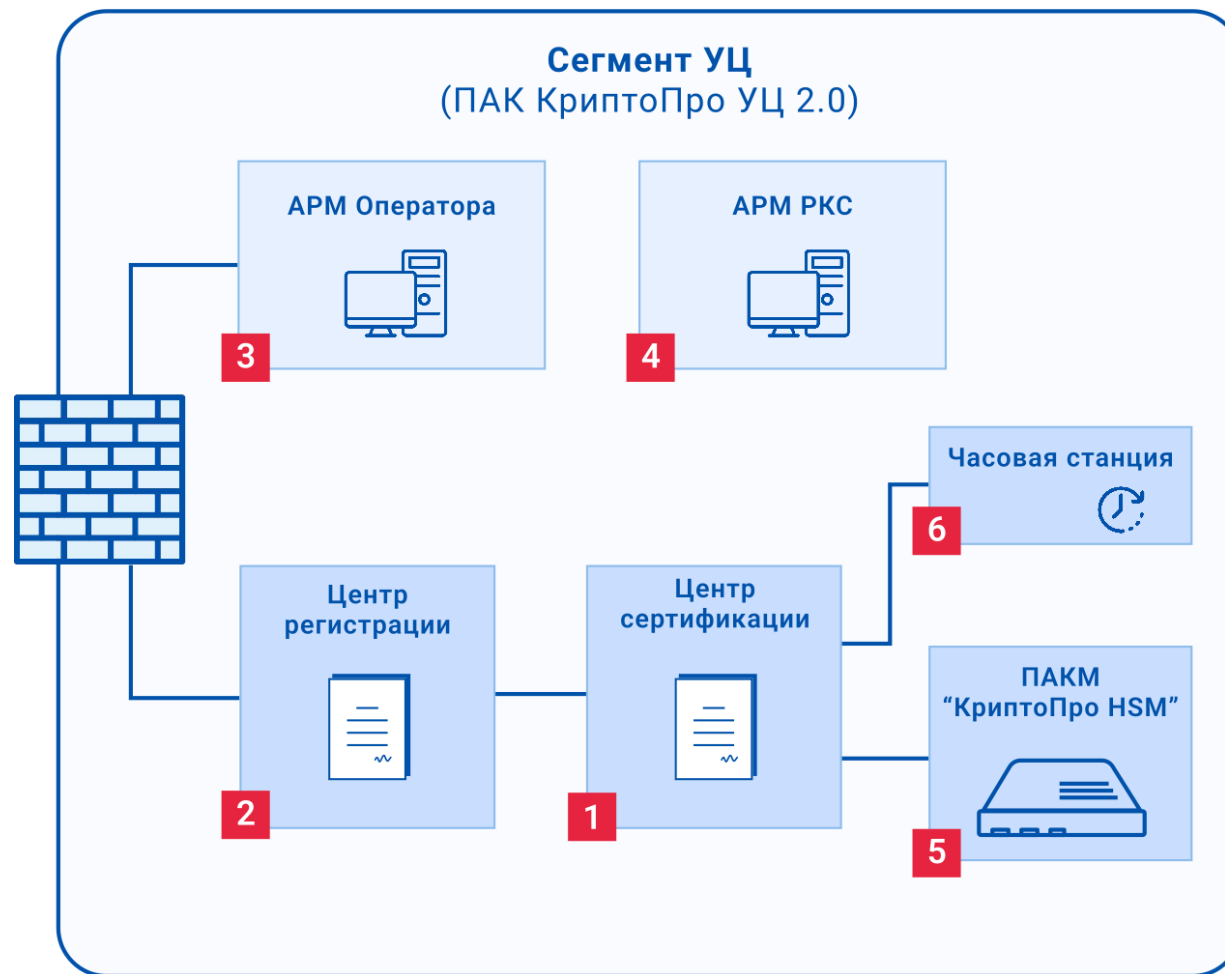
1, 2, 3, 4. ЦС, ЦР, АРМ Оператора, АРМ РКС:

– СЗИ НСД типа ПАК
Соболь/Аккорд

– SPR (требуется для КСЗ для WIN)

5. **HSM** (опционален) позволяет
увеличить срок действия ключа ЦС
до 3-х лет

6. **Часовая станция** типа ИВЧ
1/СП со свидетельством
Росстандарта



Структурная схема компонент УЦ



Состав компонент:

1. OCSP, TSP:

– СЗИ НСД типа ПАК Соболев/Аккорд (серт. ФСБ)

SPR (для Windows для КСЗ)

2. **HSM** для хранения ключей OCSP и TSP Server и выполнения операций (обязателен при подключении Служб УЦ к Интернету)

3. **Часовая станция** типа ИВЧ 1/СП со свидетельством Росстандарта

Лицензирование КриптоПро УЦ 2.0 (исп. 15, 16)

- Для КриптоПро УЦ 2.0 (исп. 15, 16) необходима новая лицензия
- Для обновления до версии КриптоПро УЦ 2.0 (исп. 15, 16) необходимо приобрести лицензию на обновление
- В новой версии УЦ отсутствуют временные лицензии на 3 месяца
- Временные лицензии на УЦ можно запросить на info@cryptopro.ru

Спасибо за внимание



info@cryptopro.ru
cryptopro.ru

