Прикладная криптография наглядно

Арина Эм

ViPNet OSSL

Криптобиблиотека для разработки мобильных и серверных решений

Сертификат ФСБ России: КС1, КС2, КС3

Клиентское и серверное исполнение

Поддержка мобильных ОС

Особенности

- Стандартные интерфейсы OpenSSL и PKCS#11
- Поддержка различных форматов подписи
- Актуальные алгоритмы и протоколы
- Содержит программный токен
- Совместим с токенами и смарт-картами
- Возможность экспортировать ключи с других машин и криптопровайдеров

Характеристики и функциональность

Работа с ЭП

ГОСТ Р 34.10-2012

Хэширование

ГОСТ Р 34.11-2012

Шифрование

- ГОСТ Р 34.12-2015
- ГОСТ Р 34.13-2015

Поддержка ОС

Форматы

- CMS
- PFX
- XMLDsig
- CAdES
- XAdES
- X.509

Протоколы

- TLS 1.2
- TLS 1.3
- TSP
- OCSP

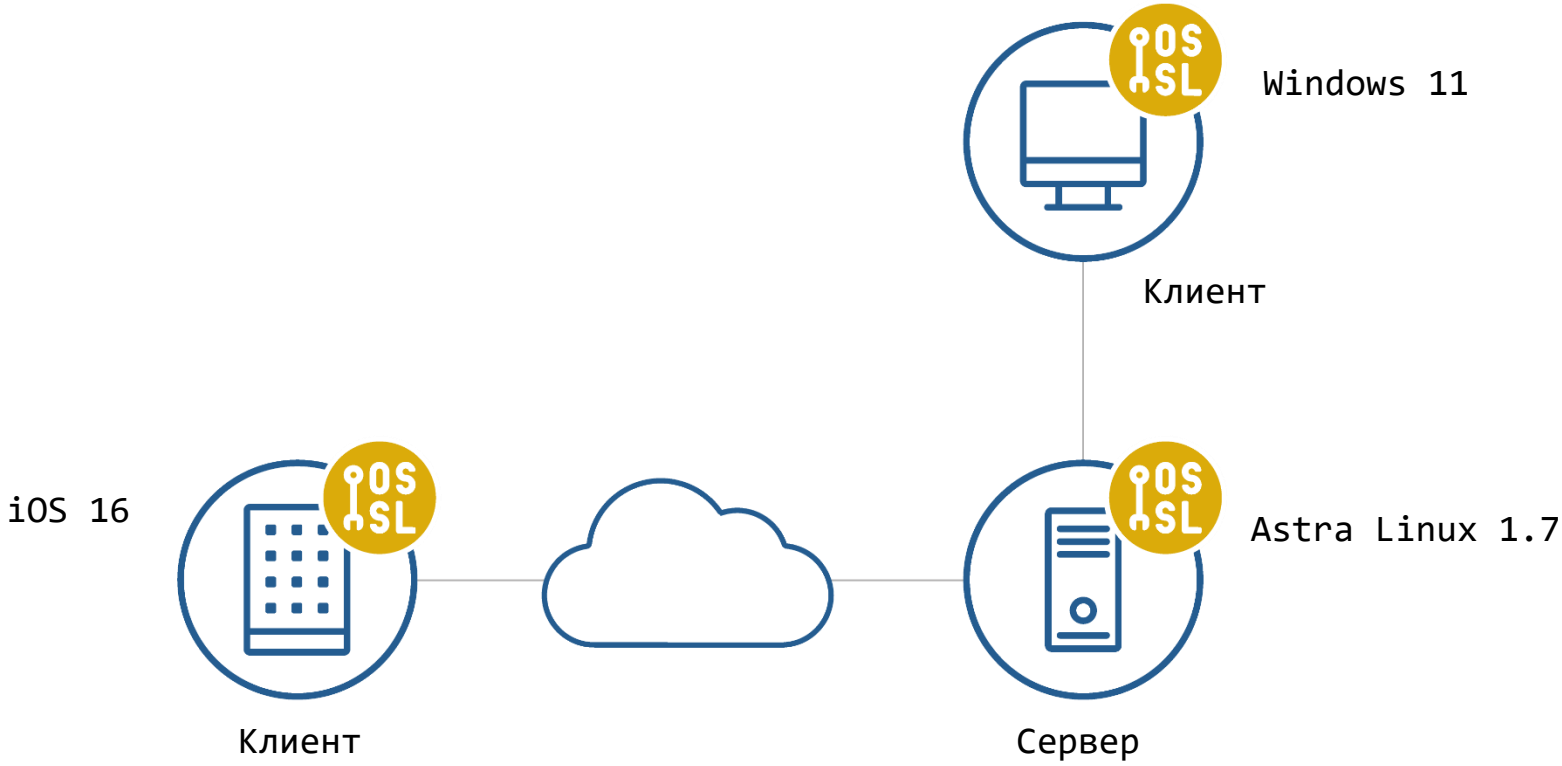
Работа с ключами на токенах

- Rutoken
- JaCarta
- HSM
- и др..

Интерфейсы

- OpenSSL
- PKCS#11

Сценарий



Что сегодня будем смотреть

- Создание и проверка электронной подписи
- Генерация ключей и создание сертификата
- Миграция ключей между устройствами
- Односторонний и двусторонний TLS
- Реализация криптографических функций в мобильном приложении

ТЕХНО 2023 infotecs ФЕСТ

Задавайте вопросы в приложении!

Подписывайтесь на наши соцсети

vk.com/infotecs_news

https://t.me/infotecs_official

rutube.ru/channel/24686363