Технологии электронной подписи. Часть 2

Владимир Салыкин
Менеджер по продуктам
Компания «Актив»

https://www.youtube.com/user/AktivCompany

Сегодня мы ответим на вопросы:

- Как работать с подписью на токене из браузера?
- Какие есть совсем высокоуровневые интерфейсы?
- Как работать с токеном из языков отличных от C/C++
- Какой интерфейс выбрать для встраивания?
- Как во всем этом не запутаться и быстро встроить поддержку подписи?

Термины

- Отечественные алгоритмы

  ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012(256 и 512 бит)

  ГОСТ Р 34.11-94 и ГОСТ Р 34.11-2012

  ГОСТ 28147-89

  VKO GOST R 34.10-2001 (RFC 4357)

  VKO GOST R 34.10-2012 (RFC 7836)

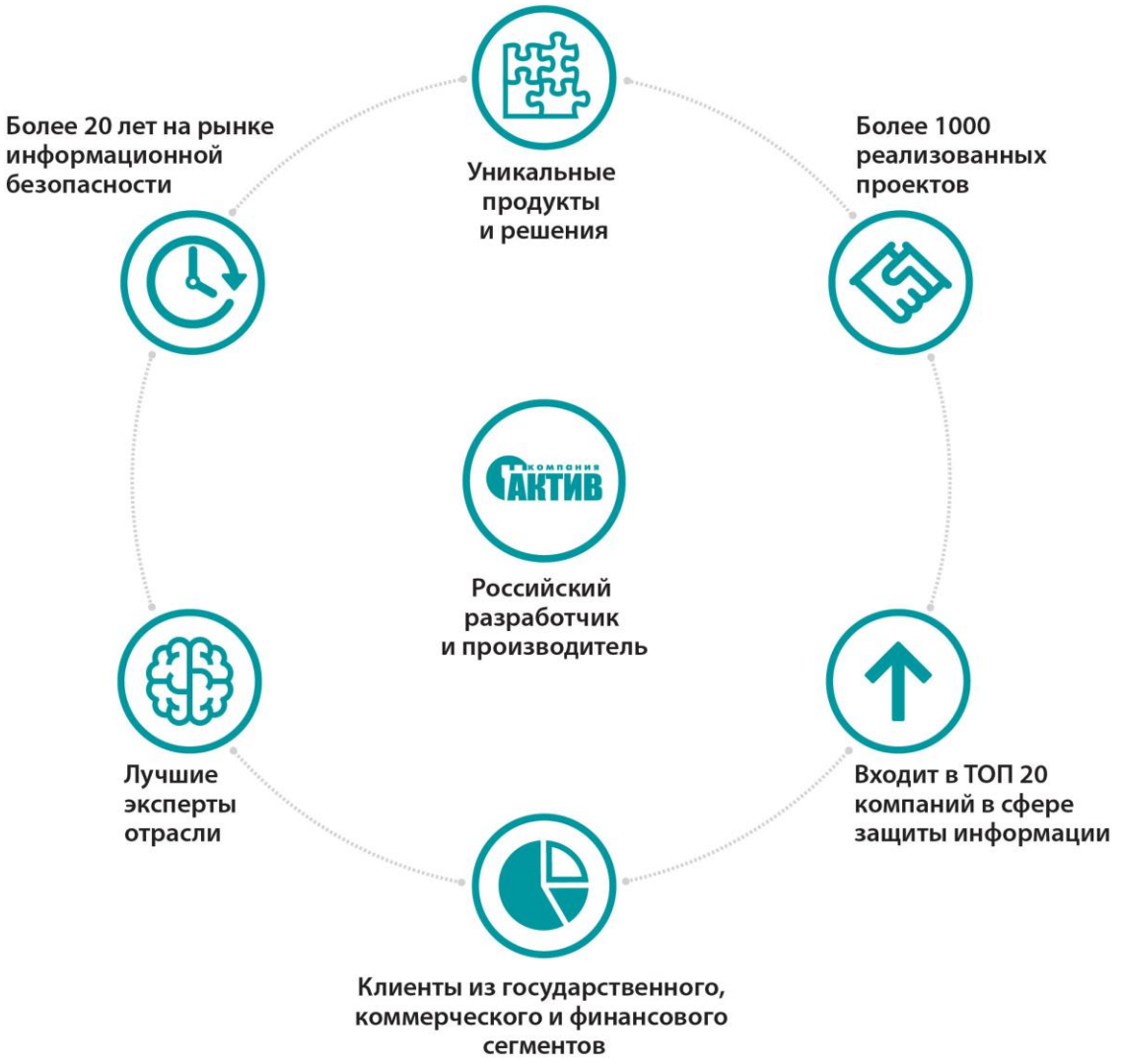
- Иностранные алгоритмы

  RSA

  AES

Компания «Актив»

Крупнейший российский производитель аппаратных средств аутентификации и электронной подписи, разработчик и поставщик комплексных решений в сфере информационной безопасности. Компания основана в 1994 году.



Направления деятельности

РУТОКЕН

Продукты и решения в области аутентификации, защиты информации и электронной подписи.

Guardant

Средства защиты и лицензирования программного обеспечения.

О каких интерфейсах поговорим

- Рутокен Плагин
- pki-core
- RutokenPKCS11Interop
- PyKCS11

Рутокен Плагин

Рутокен Плагин и его особенности

- Интерфейс разработан и поддерживается только для Рутокен
- Только для семейства устройств Рутокен ЭЦП
- Windows + Linux + Mac
- Firefox, Chrome, IE, Safari, Yandex, Sputnik, Opera, Vivaldi, Edge…
- Поддерживает все криптографические возможности устройств
- Поддержка CMS
- Не требует прав администратора для установки
- Доступен абсолютно бесплатно

Рутокен Плагин демо

pki-core

pki-core и его особенности

- Интерфейс разработан и поддерживается только для Рутокен
- C++ библиотека для работы с устройствами
- Кроссплатформенная библиотека
- Минималистичный интерфейс
- Поддержка отечественных и иностранных алгоритмов
- Поддержка CMS

pki-core vs PKCS11

- Привыкли к классам и объектам? pki-core
- Требуется “сырая” подпись? PKCS11
- Удобный интерфейс с классами? pki-core
- Поддержка стандарта? PKCS11

pki-core демо

Rutoken PKCS11Interop

Rutoken PKCS11Interop и его особенности

- Интерфейс разработан и поддерживается только для Рутокен
- Полноценный C# интерфейс
- По умолчанию для .Net 4.0, но может быть собран для .Net 2.0
- Поддержка всех криптографических возможностей устройства
- Поддержка расширенных функций
- Поддержка CMS
- NuGet
- Windows, Linux, Mac OS X

Rutoken PKCS11Interop демо

PyKCS11

PyKCS11 и его особенности

- PKCS#11 Wrapper для Python
- Open-source проект от создателя PC\SC
- Только для Python3
- Поддержка только иностранных алгоритмов
- Без поддержки CMS

PyKCS11 демо

Где найти больше информации?

- Портал документации Рутокен
  https://dev.rutoken.ru
- Комплект разработчика Рутокен
  https://www.rutoken.ru/developers/sdk/
- Github компании Актив
  https://github.com/AktivCo/
- Стандарт PKCS#11
  http://docs.oasis-open.org/pkcs11/pkcs11-curr/v2.40/
- Пишите на
  sv@rutoken.ru
  mk@rutoken.ru

Контактная информация

Электронная почта:

Личная – sv@rutoken.ru

Отдел продаж – sales@rutoken.ru

Тех. поддержка – hotline@rutoken.ru

Facebook:

facebook.com/vladimir.salykin

Сайты:

www.rutoken.ru

www.aktiv-company.ru

Телефон:

+7 495 925-77-90