

Особенности построения

Облачный сервис ЭЦП

ООО «Сайфер БИС»

Влад Ковтун

Александр Стокипный

Андрей Охрименко

Введение

Цель: Обеспечить безопасное, удобное, легкое и доступное использование ЭЦП для юридически и финансово значимых действий

Области применения:

- Банковские системы
- Системы подачи отчетности
- Электронный документооборот
- Обмен электронной почтой

Использование ЭЦП

ТЕКУЩИЕ ОЖИДАНИЯ

Ожидание

Применение ЭЦП на различных:

- Аппаратных платформах
- Операционных системах
- Технологиях
- Ключевых носителях

Текущее состояние

Различные типы устройств:

- Настольные компьютеры, ноутбуки
 - Windows
 - Linux
 - macOS
- Мобильные устройства (планшеты, телефоны)
 - Android
 - iOS
 - Windows

Текущее состояние

Различные типы технологий и платформ:

- ❑ Приложения (native), например Windows, macOS, Linux и другие
- ❑ Приложения (portable), например Java, Javascript и другие
- ❑ Web-приложения в среде браузеров (FireFox, Chrome Edge, Opera и другие)
 - Javascript (portable)
 - Расширения для браузеров (portable)+библиотеки (native)

Текущее состояние

Мобильные платформы:

- Android (множество версий)
- iOS (множество версии)
- Windows для устройств

Сложность применения ЭЦП:

- Хранение ключей
- Генерация ключей
- Перенос ключей между устройствами (?)

Текущее состояние

Различные ключевые носители:

- Файловые контейнеры
 - PKCS#12 стандартный (p12, pfx)
 - Проприетарные (Key-6/11.dat, JKS, ZS2 и другие)
- Защищенные носители
 - PKCS#11 (Aladdin, SafeNet, Gemalto, Автор, G&D, Avest и другие)
- Защищенные носители, активный режим
 - PKCS#11 (Автор, Avest и другие)
 - Проприетарный (ИИТ)

Проблематика

- Высокая стоимость:
 - Разработки/Изменений
 - Внедрения/Поддержки
- Сложность эксплуатации всей инфраструктуры
- Не всегда ожидаемый результат ...
- Ориентация на ПК под управлением ОС Windows
- Использование Javascript для web-приложений

Что имеем?

Что получается:

- Долго
- Дорого
- Сложно
- Качественно ... (Не факт)

Альтернативный подход

ОБЛАЧНЫЙ СЕРВИС ПОДПИСИ

Существующие сервисы

- ❑ <https://docusign.com> - US
- ❑ <https://hellosign.com> - US
- ❑ <https://www.signinghub.com> - EN
- ❑ <https://aws.amazon.com/cloudhsm> - US
- ❑ <https://www.echosign.adobe.com> - US
- ❑ <https://prime-sign.com> - DE (EU)
- ❑ <https://www.clicksignworld.com> - ES (EU)
- ❑ <https://www.universign.com> - FR (EU)
- ❑ <https://www.time4mind.com> - IT (EU)
- ❑ <https://www.cryptomathic.com> - DN (EU)
- ❑ <https://www.synerdocs.ru> - RU
- ❑ <https://kontur.ru/ca> - RU

Стандартизация

- ❑ CEN/TS 419 241 «Security Requirements for Trustworthy Systems Supporting Server Signing»
- ❑ <http://www.cloudsignatureconsortium.org>

Docapost /
Certinomis (FR)

Adobe – Global
Intesi Group (IT)

SwissSign (SZ)

Graz University of
Technology (AU)

Asseco Data Systems (PL)

InfoCert (IT)

Universign (FR)

Bundesdruckerei / D-
Trust (DE)

Intarsys Consulting (DE)

Safelayer (ES)

Unibridge (NW)

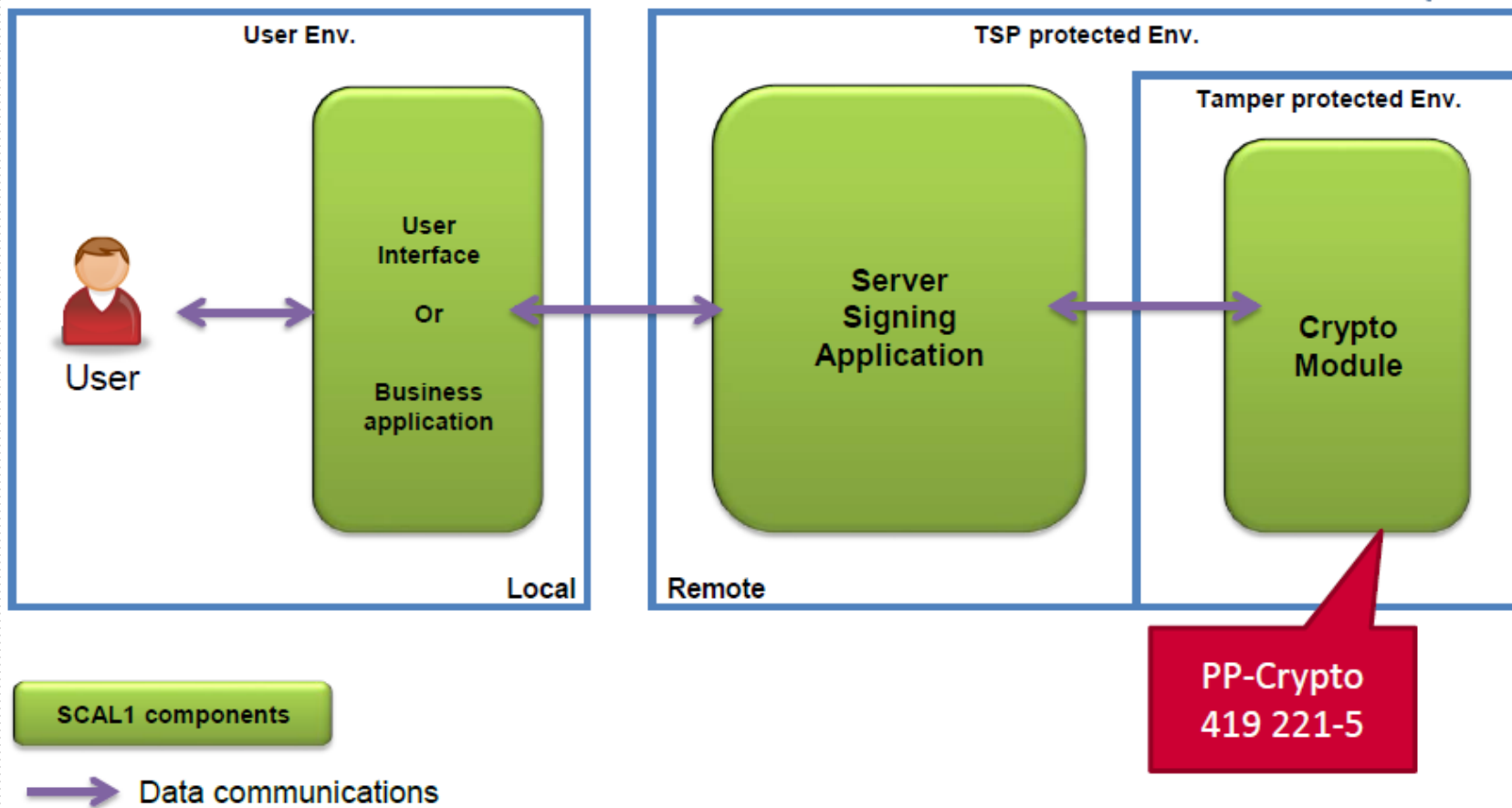
Стандартизация

- CEN 419 241 Part 1: General System Security Requirements
 - Level 1: for electronic signature (or seal)
 - Level 2: for **Advanced** electronic signature (or seal)
- CEN 419 241 Part 2: Protection Profile for QSCD for Server Signing
 - To qualify a signature device necessary for **Qualified** electronic signature (or seal)

Уровни контроля (SCAL1)

- Sole control assurance level 1:
 - The signing keys are used, with a low level of confidence, under the sole control of the signer;
 - The authorized signer's use of its key for signing is enforced by the Server Signing Application (SSA) which authenticates the signer.

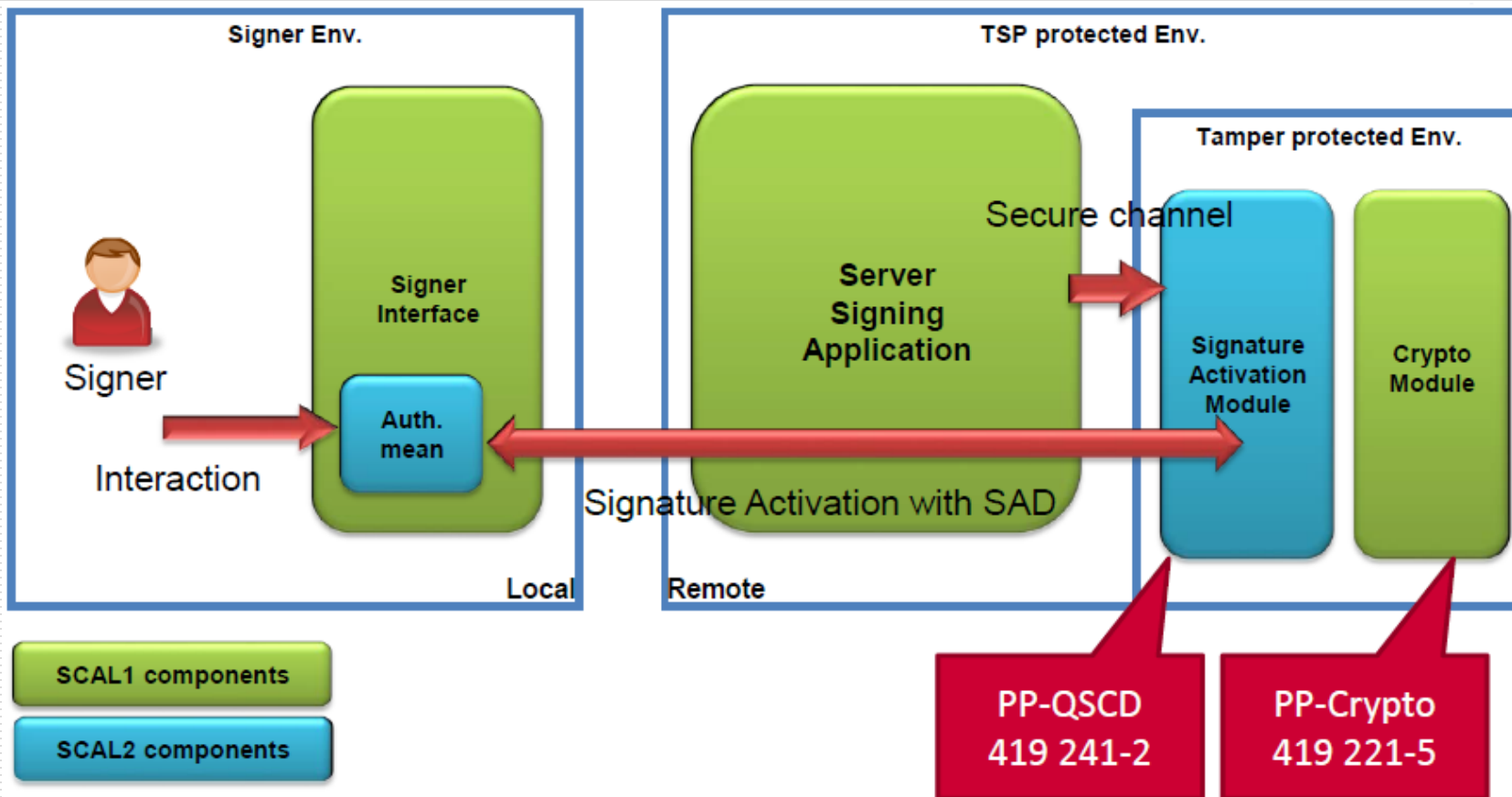
Уровни контроля (SCAL 1)



Уровни контроля (SCAL2)

- Sole control assurance level 2:
 - The signing keys are used, with a high level of confidence, under the sole control of the signer;
 - The authorised signer's use of its key for signing is enforced by the SAM, in order to enable the use of the corresponding signing key

Уровни контроля (SCAL 2)



Механизмы

- **Signature Activation Protocol (SAP):**
 - The set of the necessary steps in order to create a signature;
 - Shall generates an “activation data”.

Механизмы

□ **Signature Activation Data (SAD):**

- Shall be linked to the authenticated signer; (substantial level)
- Shall be linked to the DTBS/R; (to protect from replay attack)
- Shall be generated under sole control of the signer.

Механизмы

- **Signature Activation Module (SAM):**
 - Piece of software protected by an HSM;
 - Checks the validity of the SAD in order to activate the signing key.

Преимущества

- Оператору (банку)
 - API для интеграции с любыми решениями
 - Простота поддержки, обновления
 - Минимизация издержек
 - Прозрачная монетизация

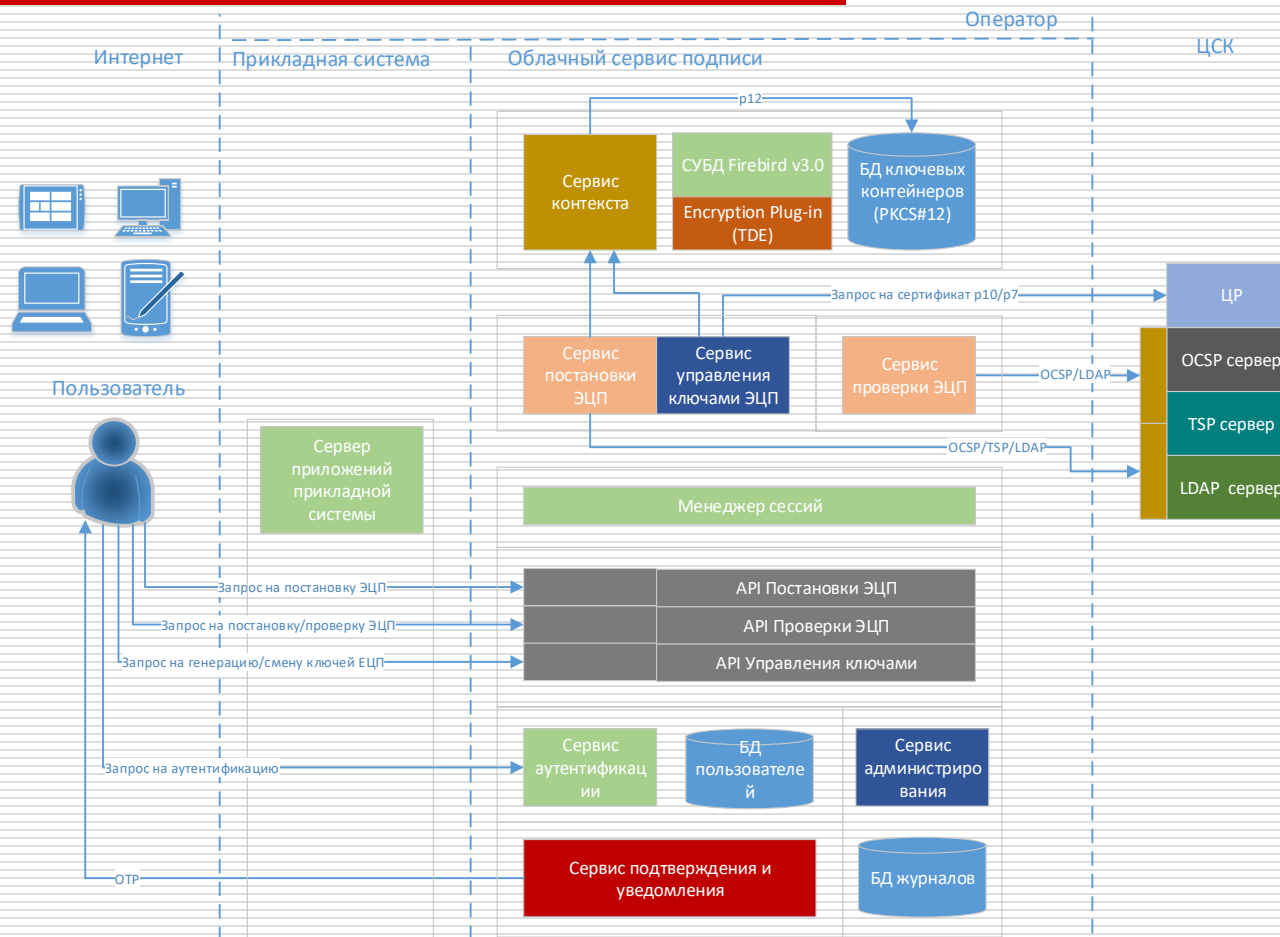
Преимущества

- Пользователю
 - API для интеграции с любыми решениями
 - Поддержка любых платформ
 - Мобильность
 - Минимизация издержек
 - Прозрачная монетизация
 - Контролируемая безопасность ключей

Недостатки

- Оператору (банку)
 - Усложнение инфраструктуры
 - Более жесткий контроль за инфраструктурой
 - Обеспечение прозрачности инфраструктуры
- Пользователю
 - Доверие сервису (через его прозрачность)
 - Контроль за безопасностью ключей осуществляет сервис (не все пользователи могут это позволить)

Архитектура



Архитектура

- Облачный сервис (ядро)
 - Защищенное хранилище (СУБД Firebird+Plugins)
 - Сервис контекста (Java Micro Service - JMS)
 - Сервис подписи (JMS)
 - Сервис управления ключами (JMS)
 - Сервис проверки ЭЦП (JMS)
 - Сервис аутентификации (JMS)
 - Менеджер сессий (JMS)

Архитектура

- Облачный сервис (инфраструктура)
 - Сервис подтверждения и уведомления (JMS)
 - Шлюз API (JMS)
 - Сервис администрирования (JMS)
 - Orchestration Environment для JMS

Архитектура

- ЦСК
 - OCSP
 - TSP
 - LDAP
 - CMP (шлюз в Центр Регистрации)

Услуги

- Генерация ключей ЭЦП
 - Требуется дополнительной аутентификации (ОТР)
- Формирование ЭЦП
 - Требуется дополнительной аутентификации (ОТР)
 - Единожды/Пакетом
- Проверка ЭЦП
 - Единожды/Пакетом
- Смена ключей
 - Требуется дополнительной аутентификации (ОТР)

Вопросы?

Спасибо за внимание!

ООО «Сайфер БИС»

Влад Ковтун

Александр Стокипный

Андрей Охрименко

email: vk@cipher.kiev.ua

as@cipher.kiev.ua

ao@cipher.kiev.ua

www: <https://cipher.kiev.ua>