ГАЗИНФОРМСЕРВИС

XII международная конференция
по проблематике инфраструктуры открытых ключей
и электронной подписи «PKI-Forum Россия 2014»

Проблемные вопросы встраивания средств ЭП в информационные системы

Петров Сергей
начальник отдела разработки
средств защиты

Функционально законченное криптосредство

РусКрипто'2014

ГАЗИНФОРМСЕРВИС

Ассоциация РусКрипто

КРИПТО ПРО

СКЗИ информационных технологий (СКЗИ ИТ)

Совет директоров конференции РусКрипто
Директор по научной работе ООО Крипто ПРО
Соруководитель группы сопутствующих алгоритмов ТК26 КФМН
Попов Владимир Олегович

Введение

В ноябре 2013 г. от руководства ФСБ поступило указание о пересмотре понятия СКЗИ в процессе их разработки и проведения тематических исследований. В данном документе существующая практика работы с СКЗИ определялась ключевыми словами:

- Криптоядро, встраивание, конечный продукт.

Новое представление о СКЗИ, определяемое указанием:

- функционально законченное криптосредство.

Понятие функциональной законченности в ИТ, строящихся по принципу взаимодействия открытых систем (ВОС), основывается на следующих предположениях:

- Система разбивается на функциональные блоки;
- Функциональных блок определяется интерфейсом;
- Интерфейс стандартизируется и является инвариантом блока;
- Функциональная составляющая блока поддерживает соглашения интерфейса, допустимо расширение функций блока при выполнении требований обратной функциональной совместимости.

Могут быть определены следующие подходы к понятию функционально законченного криптосредства:

- Подход ВОС;
- Подход действующих требований к СКЗИ;
- Подход нормативной базы сертификации СКЗИ;
- ПКЗ 2005;
- Существующая практика построения СКЗИ.

Функционально законченное криптосредство

Уровни криптографической подсистемы ИТ

Сложившаяся практика использования криптографических подсистем позволяет выделить 4 уровня:

1. Уровень хранения ключей (ключевые пары, ключи и неструктурированные данные, механизмы шифрования, MAC, хеширование, ЭЦП), (CSP).
2. Уровень криптографических протоколов (токены доступа, сертификаты, протокольные сообщения), (CSP + сертификаты, revocation provider).
3. Уровень защищенных услуг ИТ пользователя (субъекты доступа и информация субъекта доступа).
4. Уровень распределения ключей (субъекты доступа и ключи субъекта доступа).

Уровни криптографической подсистемы характеризуются:
- функционалом (механизмами) и объектами;
- интерфейсами и SDK.

4 уровня

Функционально законченное криптосредство

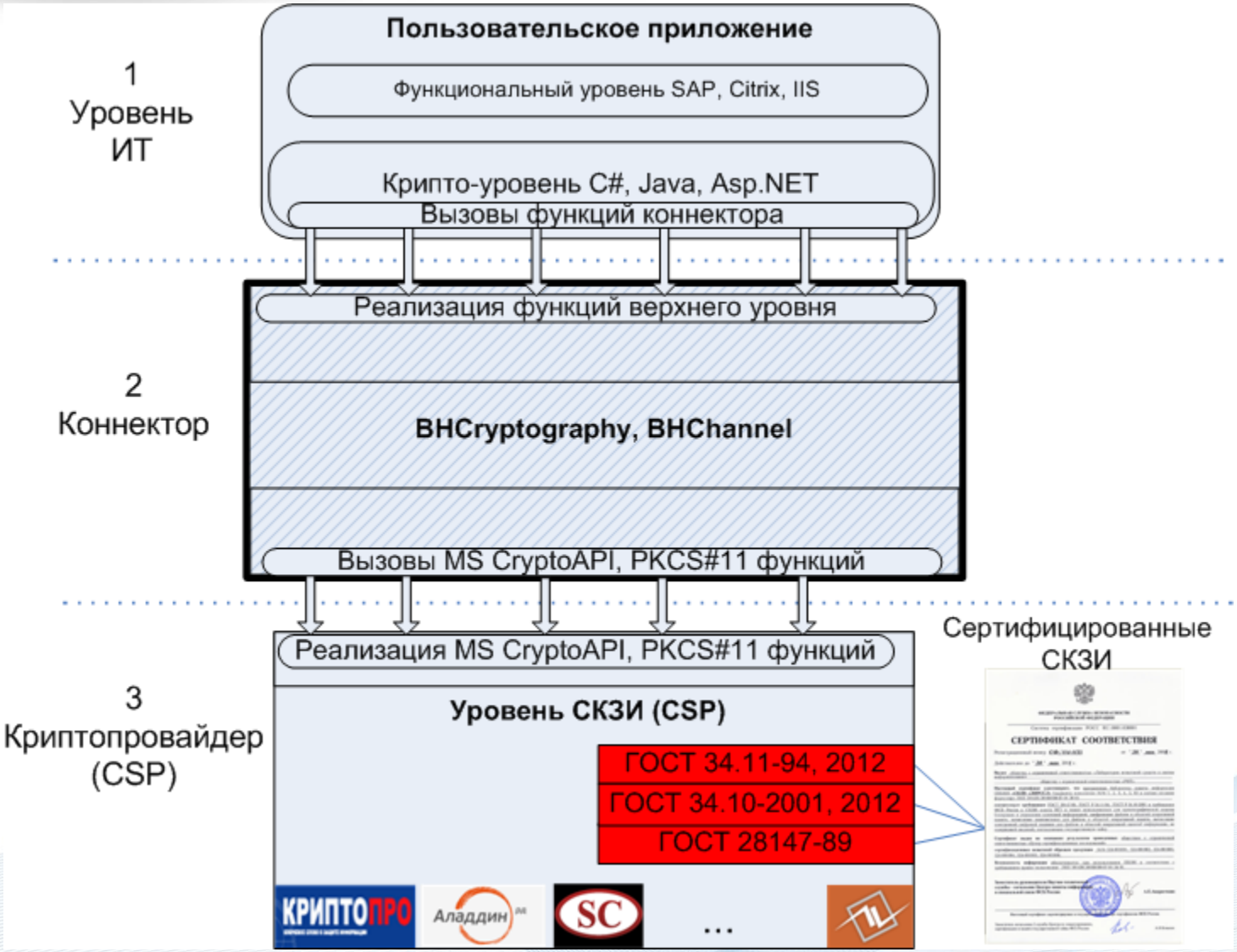
РусКрипто’2014

ГАЗИНФОРМСЕРВИС

- Уровень хранения ключей
- Уровень криптографических протоколов
- Уровень защищенных услуг ИТ пользователя
- Уровень распределения ключей

Уровни встраивания ЭП

ГАЗИНФОРМСЕРВИС



Задачи встраивания

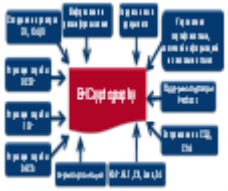
ГАЗИНФОРМСЕРВИС

SAP

documentum

CITRIX

Сервисы ДТС

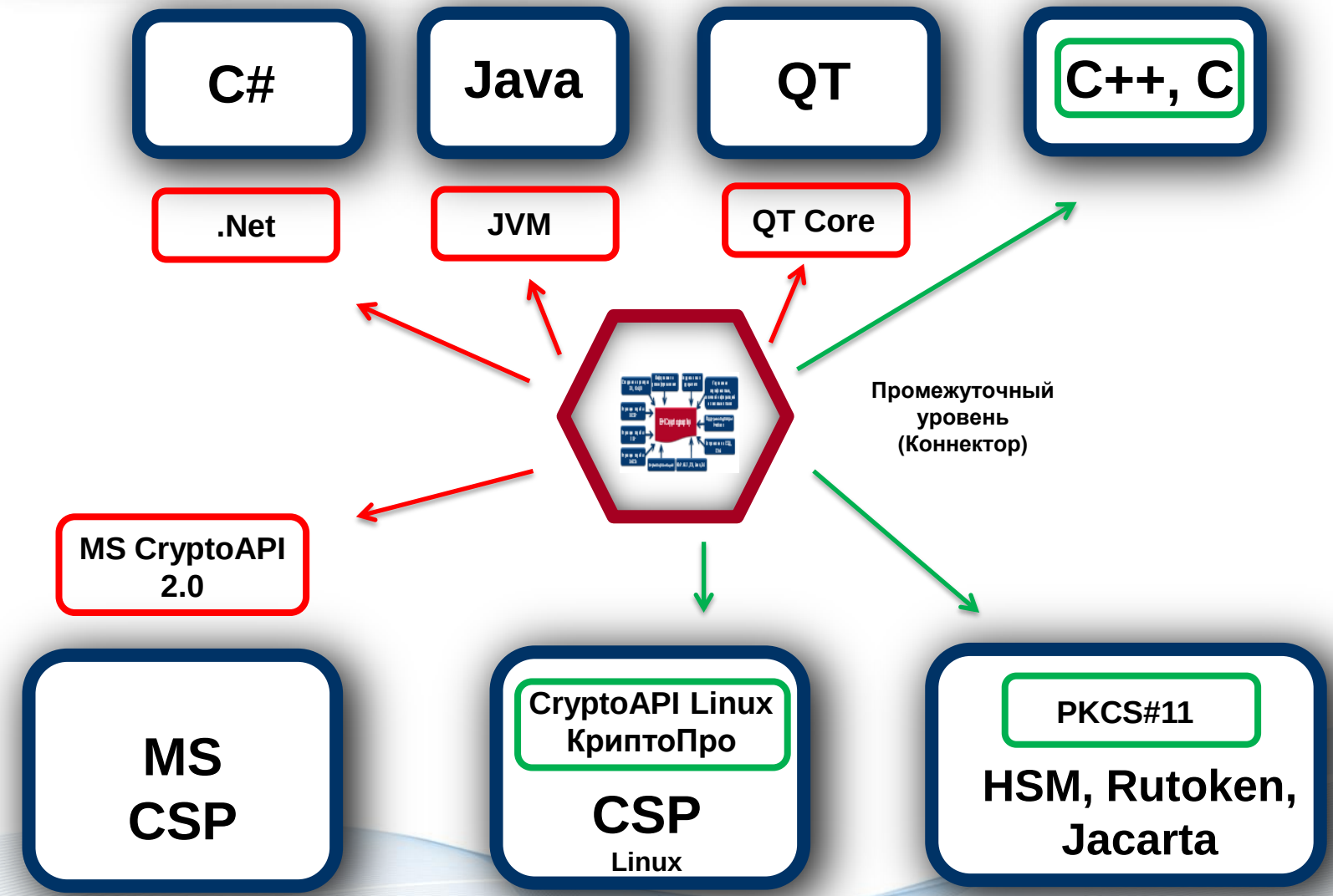


КРИПТОПРО

Аладдин

Недоверенные интерфейсы

ГАЗИНФОРМСЕРВИС



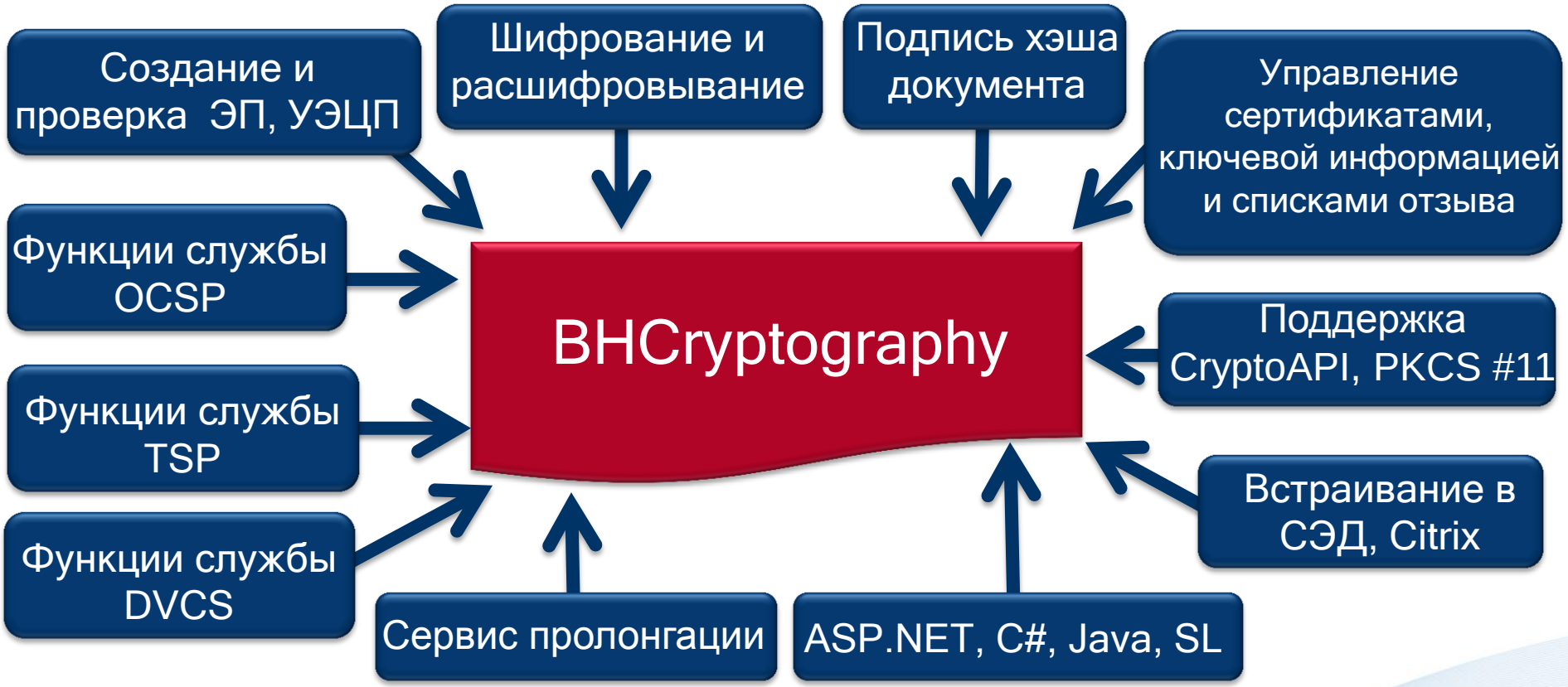
Функционально законченное криптосредство

ГАЗИНФОРМСЕРВИС

Единый промежуточный уровень

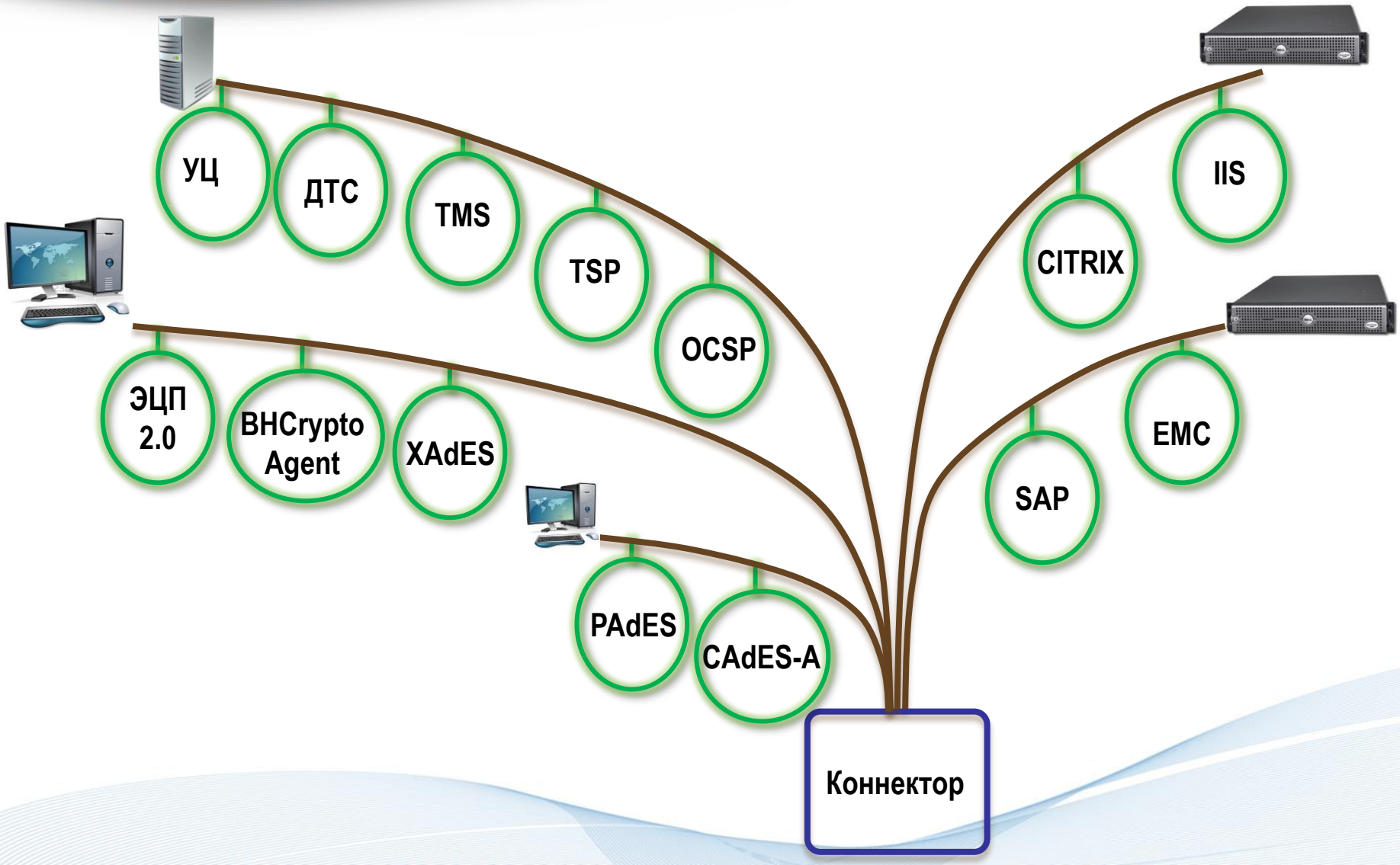
ГАЗИНФОРМСЕРВИС

Sign (Cert, Data),
Verify (Data, Result)



Применение коннектора

ГАЗИНФОРМСЕРВИС



ГАЗИНФОРМСЕРВИС

Спасибо за внимание!

Петров Сергей
начальник отдела разработки
средств защиты