

Криптография в КОММЕРЧЕСКИХ СИСТЕМАХ

Симаков Сергей

Security Architect, CISM, CISSP

Microsoft Global Security Center of Excellence

Иванов Андрей

Специалист по технологиям ИБ, MBA-IT, PMP

Russian Technology Office

Microsoft[®]



О каких системах мы говорим?

presentation layer



applications & services



app platform



communications



security



core



Management

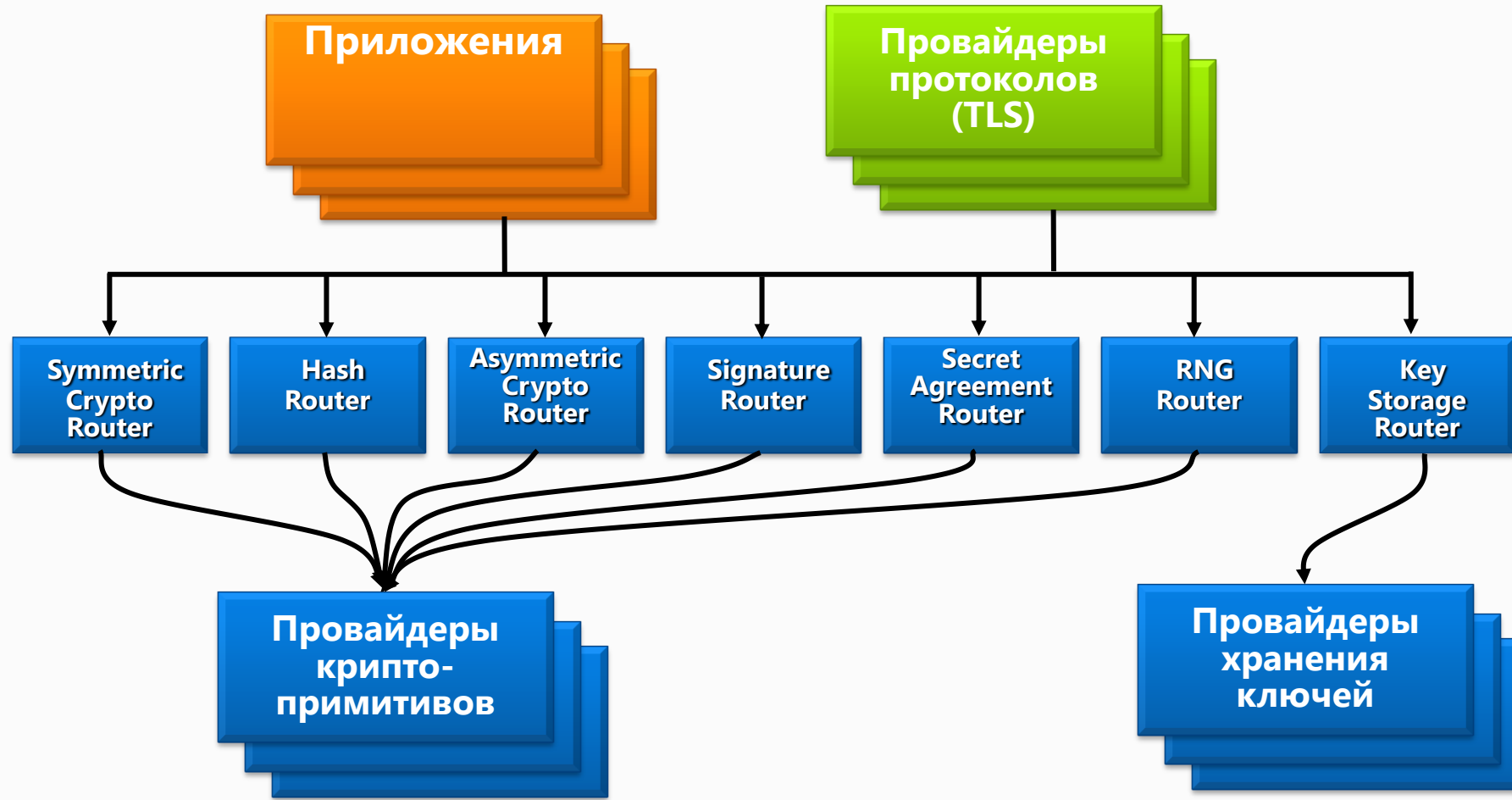


A Microsoft Subsidiary

Development



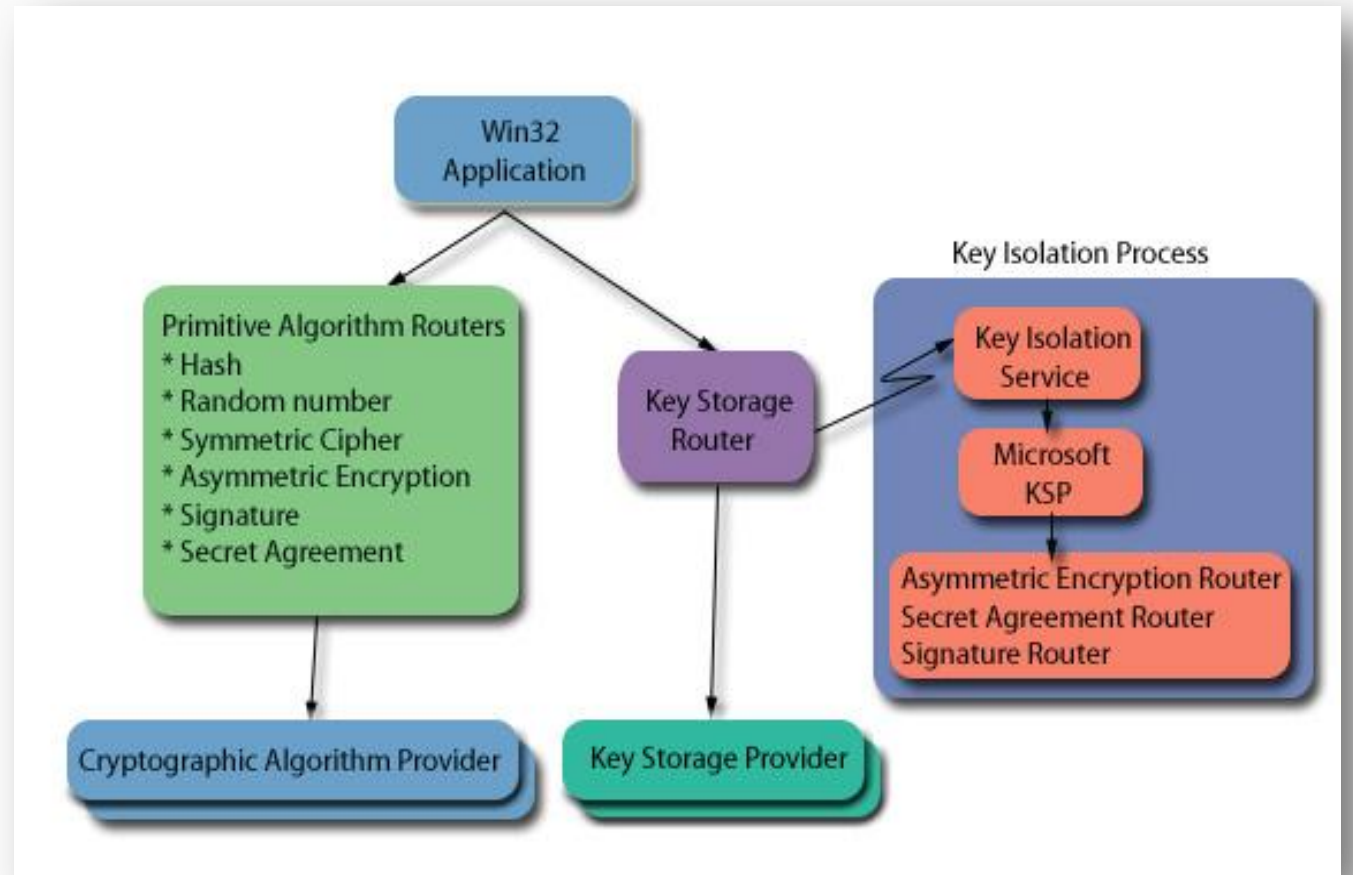
Cryptography Next Generation

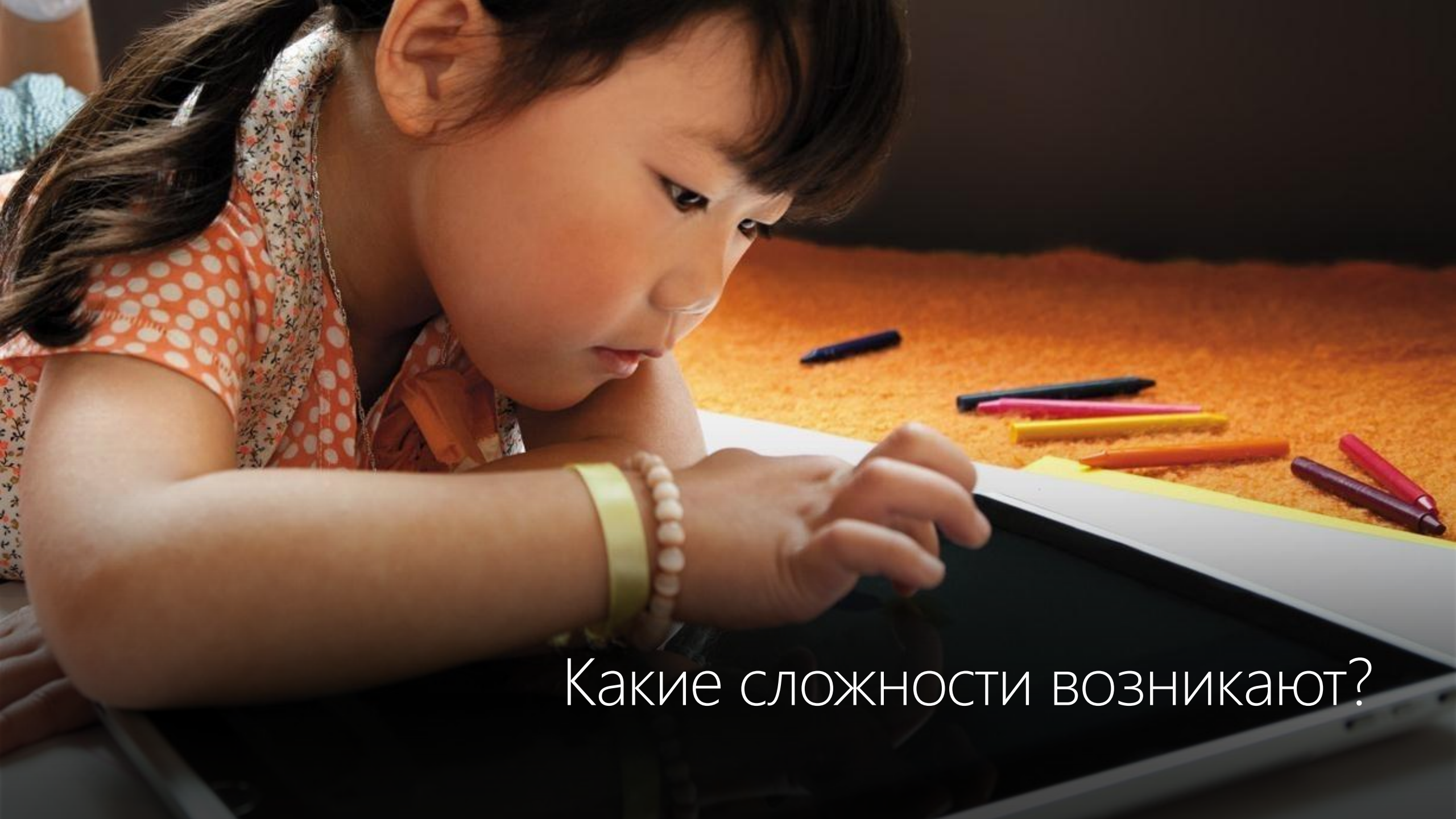


Архитектура CNG

Провайдеры алгоритмов
низкоуровневая реализация
семейства криптографических
алгоритмов

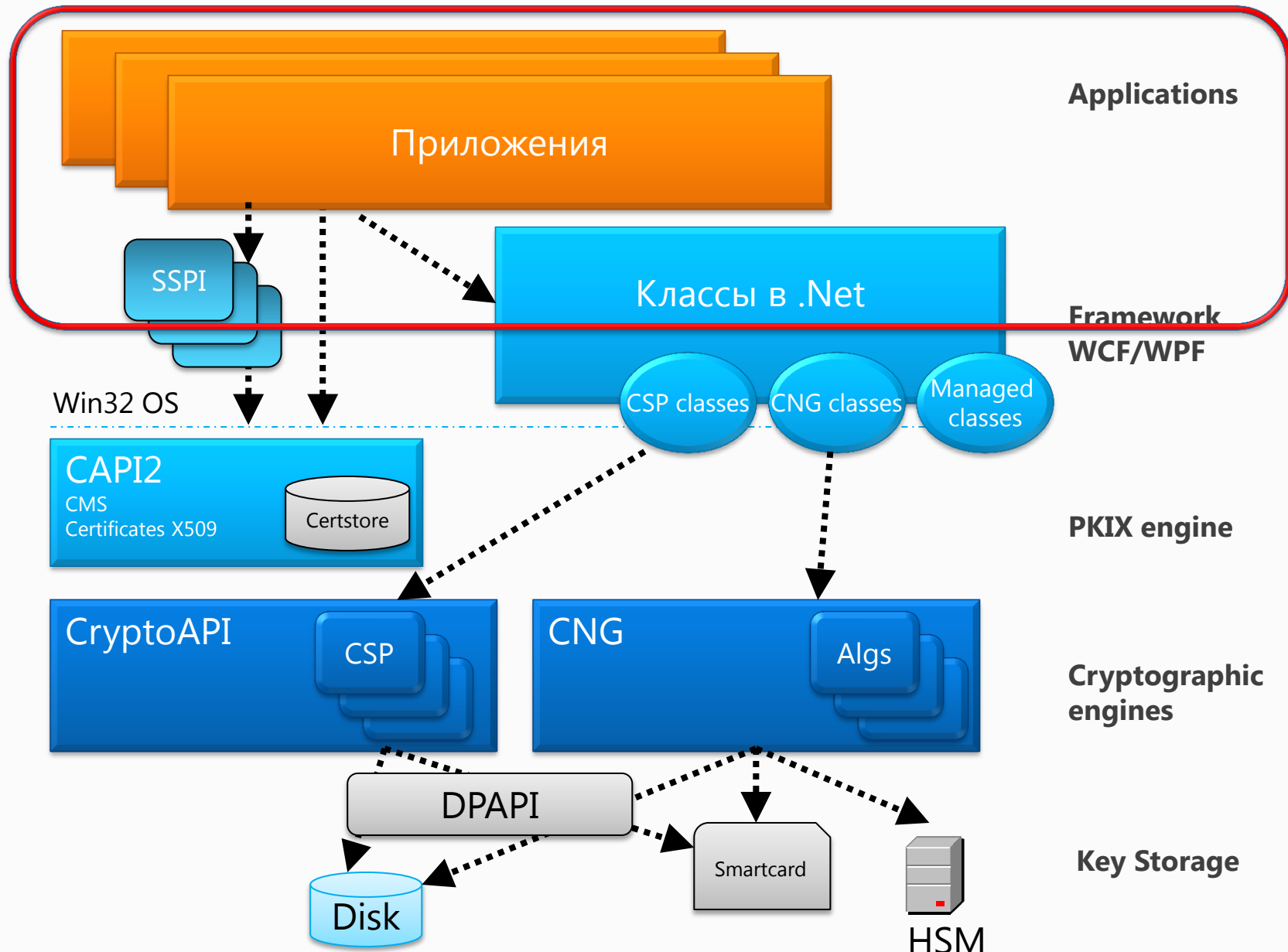
Провайдеры ключевой инф-ии
(или KSP) для управления и
хранения секретных ключей





Какие сложности возникают?

Корректность встраивания



Использование в «облаке»

Обмен ключами?

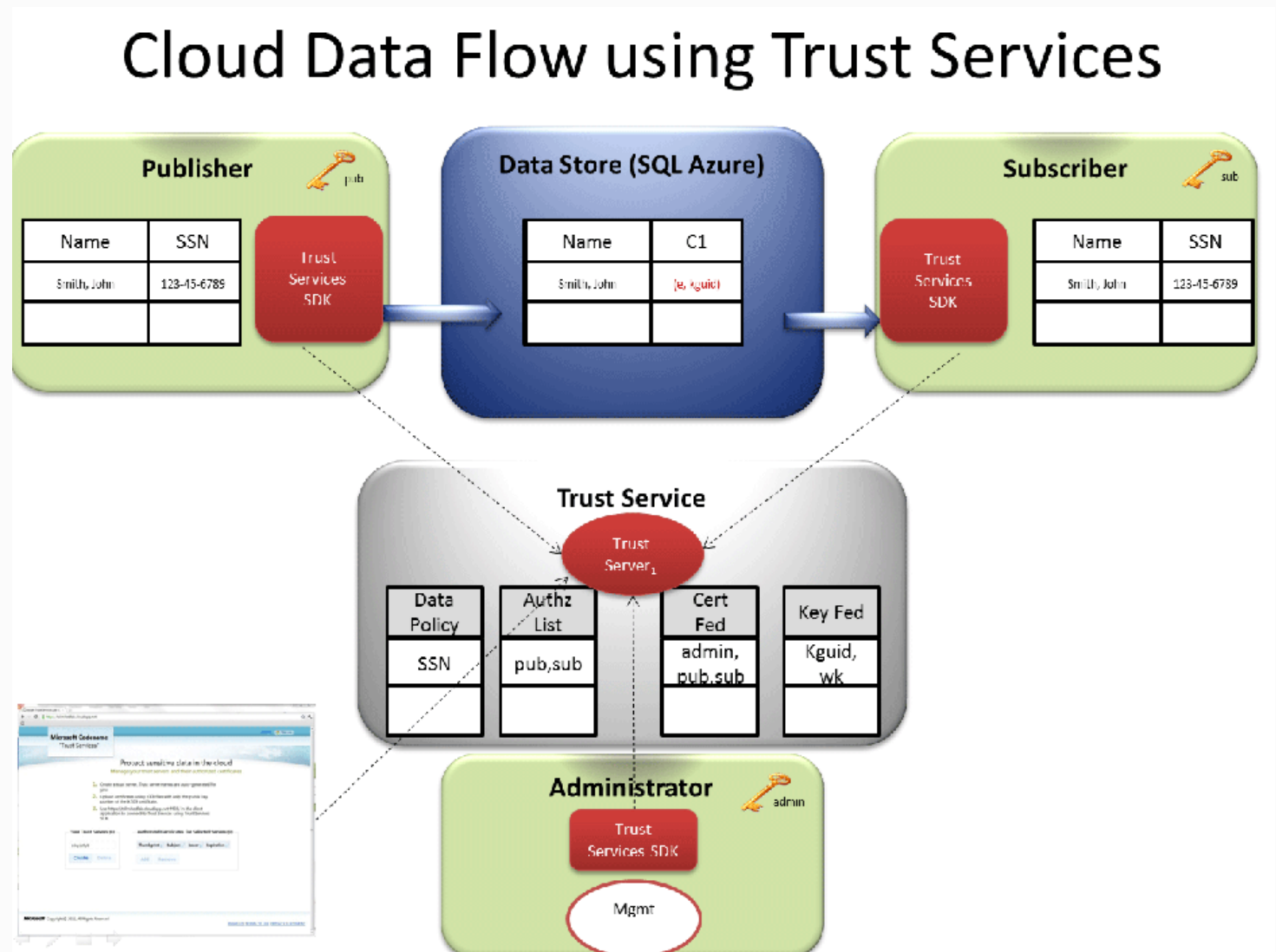
Федерация ключей
Управление и хранение
ключевой информации

Сертификаты?

Федерация и
синхронизация
сертификатов

Контроль доступа?

Управление политиками
Разделение ключей



Russian Security, Interoperability and Compliance Competence Center (RSIC³)

Соответствие требованиям законодательства

Поддержка и развитие связей с российским сообществом ИБ

Взаимодействие с разработчиками решений

Адаптация инициатив штаб-квартиры в России

Поддержка бизнес-подразделений

Давайте работать
вместе!

Андрей Иванов, andreyi@microsoft.com

Сергей Симаков, sergesim@microsoft.com

Microsoft[®]

Microsoft[®]