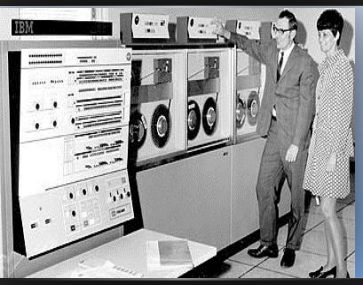
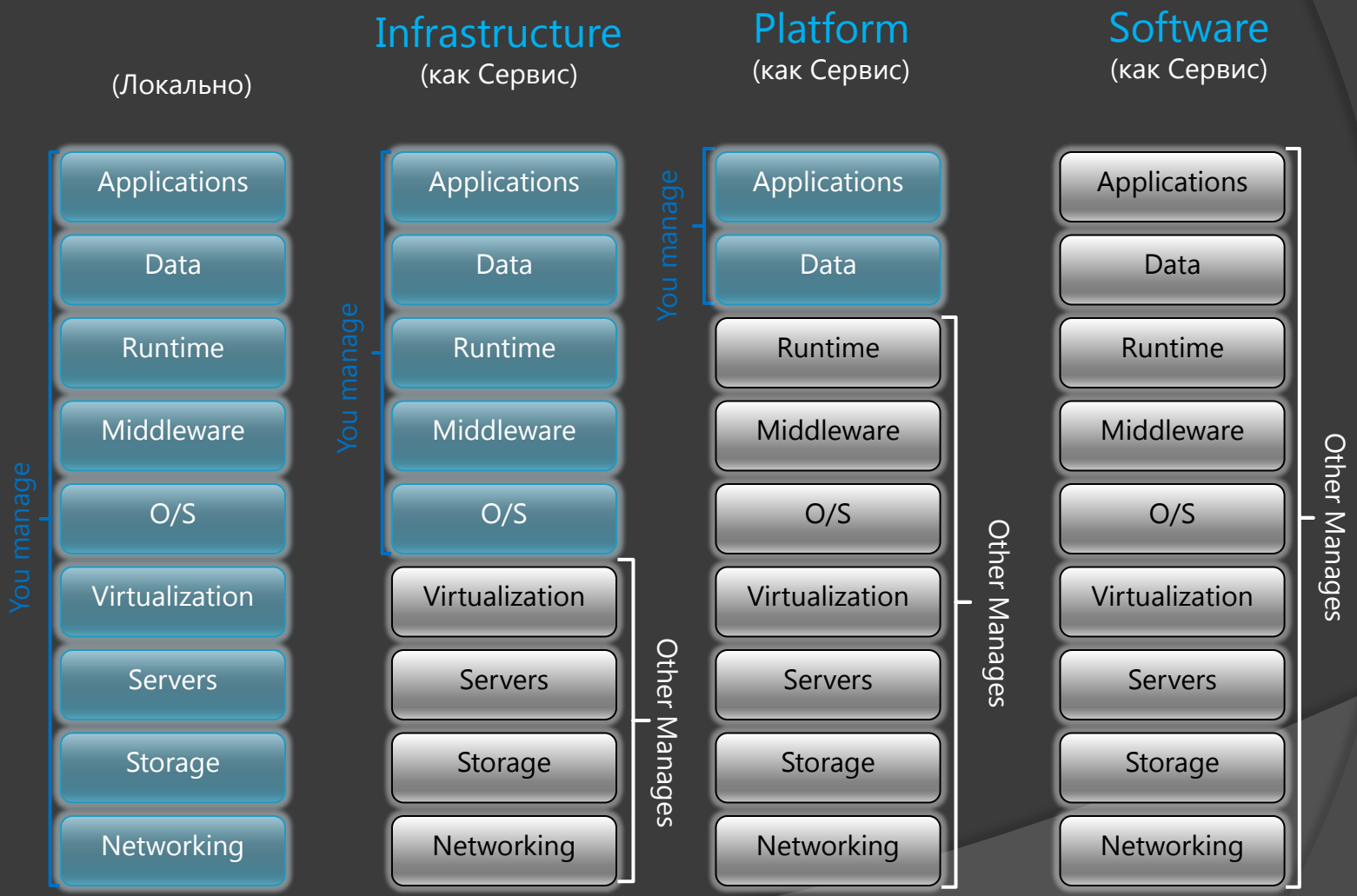
Безопасность облачной платформы

Симаков Сергей
sergesim@microsoft.com
Security Architect, CISSP, CISM
Microsoft Global Security Center of Excellence

Эволюция вычислений

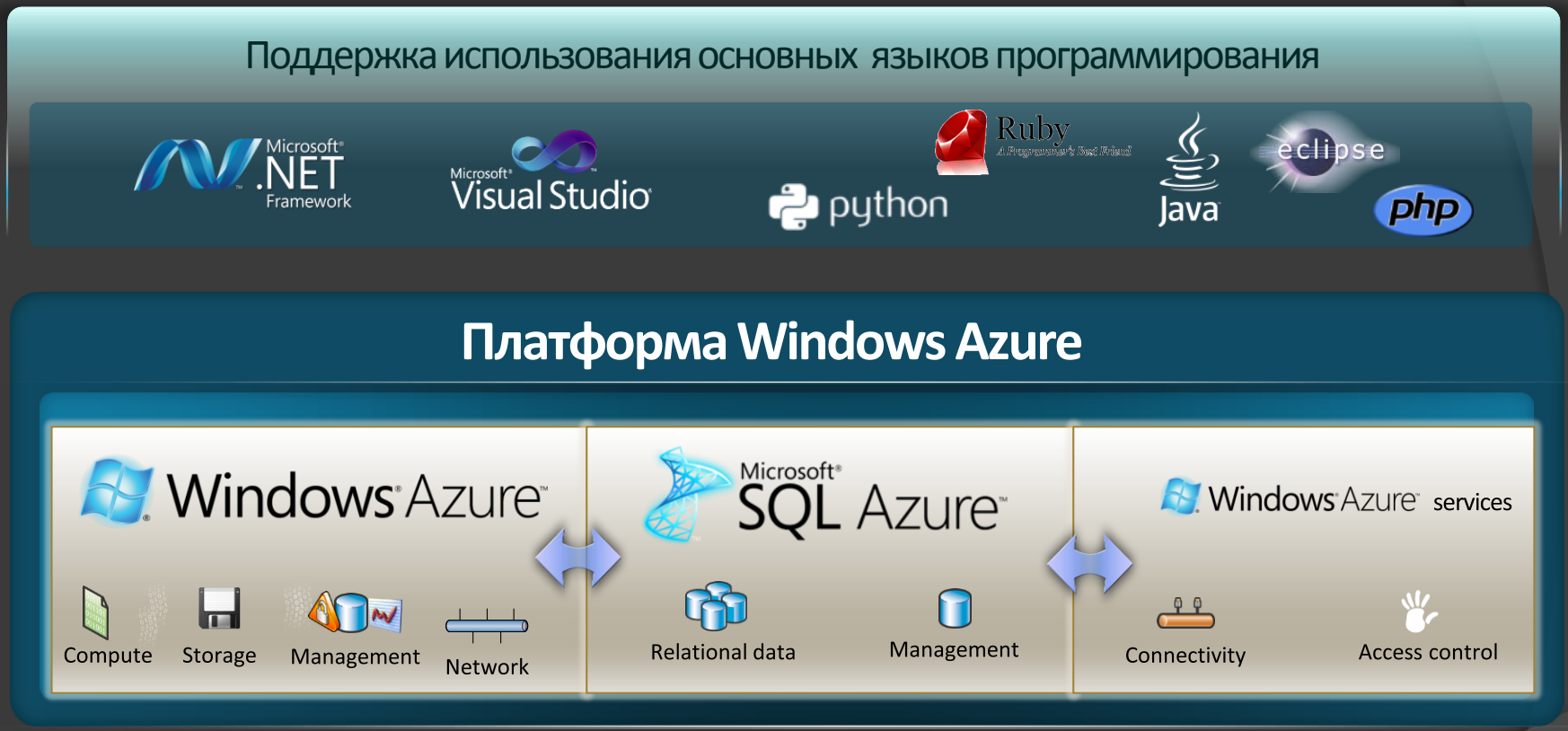
	Технологическая	Экономическая	Бизнес
	Centralized compute & storage, thin clients	Optimized for efficiency due to high cost	High upfront costs for hardware and software
	PCs and servers for distributed compute, storage, etc.	Optimized for agility due to low cost	Perpetual license for OS and application software
	Large DCs, commodity HW, scale-out, devices	Order of magnitude better efficiency and agility	Pay as you go, and only for what you use

Типы облачных сервисов



http://csrc.nist.gov/groups/SNS/cloud-computing/

Платформа Windows Azure



The Windows Azure Platform is an internet-scale cloud services platform hosted in Microsoft data centers around the world, proving a simple, reliable and powerful platform for the creation of web applications and services.

Модель безопасности PaaS

Безопасность в Windows Azure

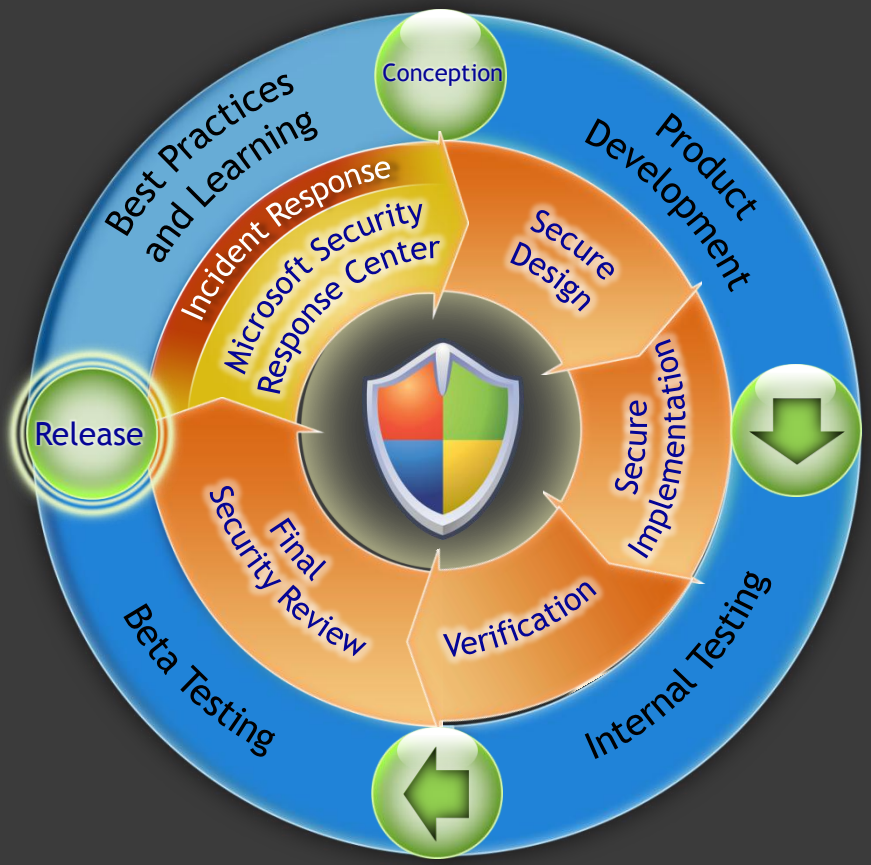
Подход многоуровневой защиты

Уровень	Защита
Data	▪ Ключи контроля доступа к данным ▪ Защита всех передач данных с помощью SSL
Application	▪ Код .Net исполняется с ограниченным доверием ▪ Учётные записи Windows с минимальными привилегиями
Host	▪ Защищенный образ Windows Server 2008 R2 ▪ Границы хоста защищены внешним гипервизором
Network	▪ МЭ хоста ограничивает доступ к вирт. машинам ▪ VLANы и пакетные фильтры в роутерах
Physical	▪ Физическая безопасность мирового класса ▪ Сертификации ISO 27001 и SAS 70 Type II процессов эксплуатации ЦОД

Место криптографии в безопасности облачной платформы

Методология разработки

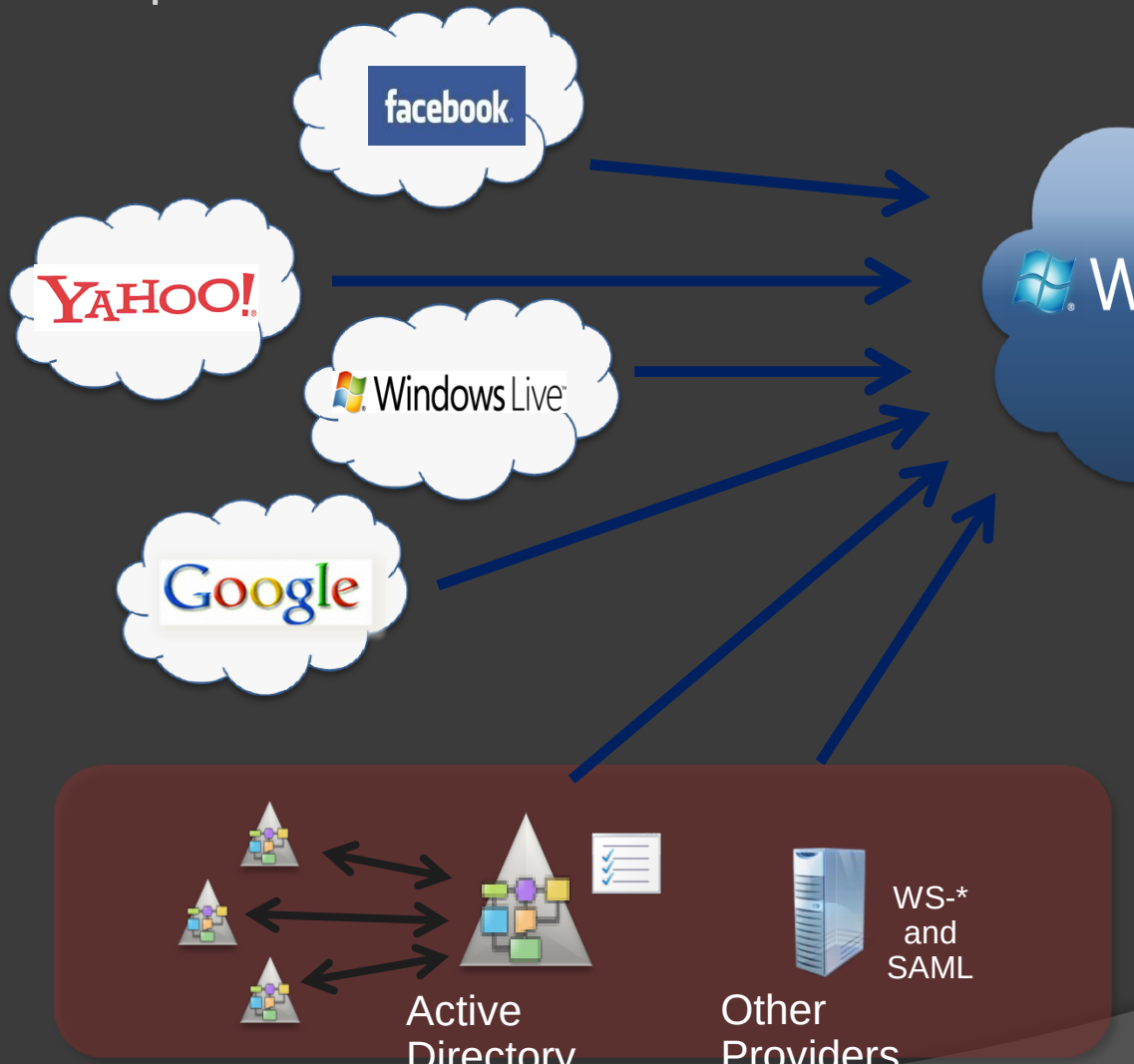
Применение Security Development Lifecycle



- Проверенная временм методология
  - Практический подход
  - Не ограничен Windows или Microsoft!
  - Проактивный – не просто «поиск ошибок»
  - Нахождение проблем как можно раньше в цикле разработки (TM)
- Защищает клиентов платформы Windows Azure Platform
- Криптографические рекомендации:
  - Алгоритмы
  - Использование проверенных протоколов
  - Проверка корректности встраивания!

Как выполнять аутентификацию?

Общий Access Control Service



Интеграция с другими системами посредством открытых стандартов WS- и SAML 2.0

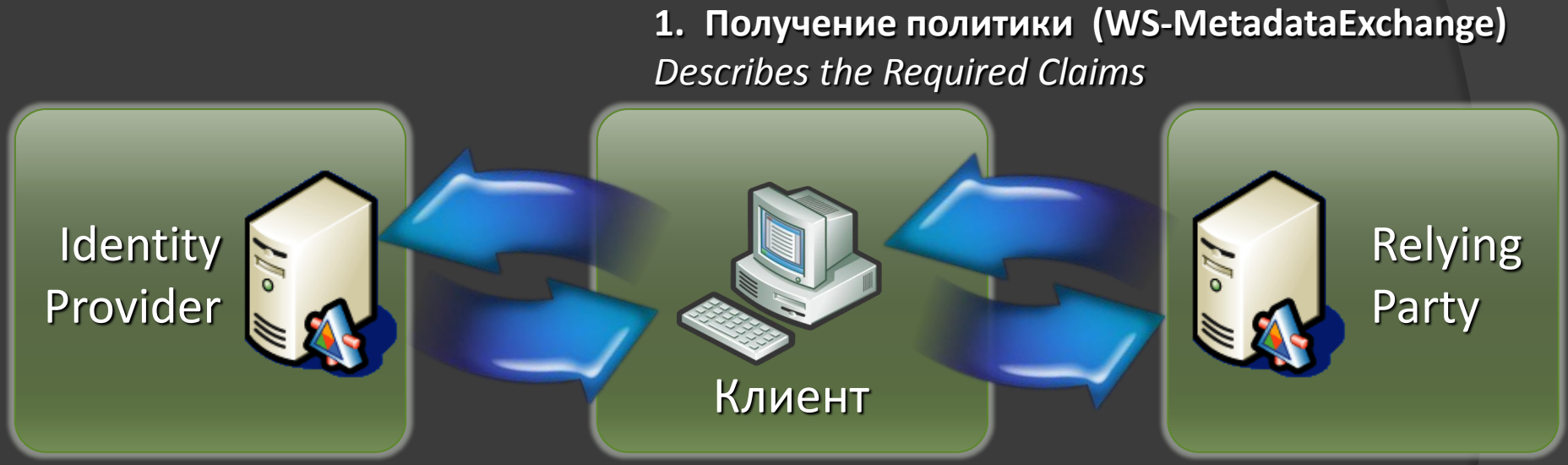
Использование Active Directory и групп (ролей) посредством федерации

Прозрачный доступ для корпоративных приложений с Active Directory

Single sign-on с популярными интернет-провайдерами

Claims Based Authentication

- Уровень абстракции для управления Identity
- Основанный на стандартах набор технологий



- Токены SAML
- WS-* (WS-Security, WS-Trust, WS-Federation)

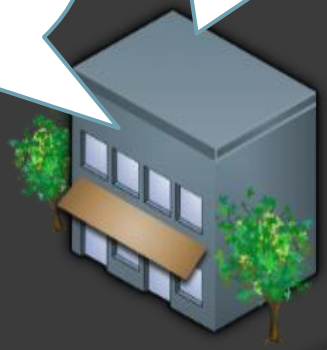
Минимальное раскрытие информации

Offene Kommunikationssysteme OKS Technische Universität Berlin

Пользователь может выборочно раскрыть информацию в токене U-Prove, изданном заранее

Даже в случае сговора издателя (IP) и ресурса (RP) они *не могут* узнать о пользоваетеле больше того, что он решил раскрыть

Кто этот гражданин из Берлина?



http://www.abc4trust.eu/
Европейский проект о минимальном раскрытии

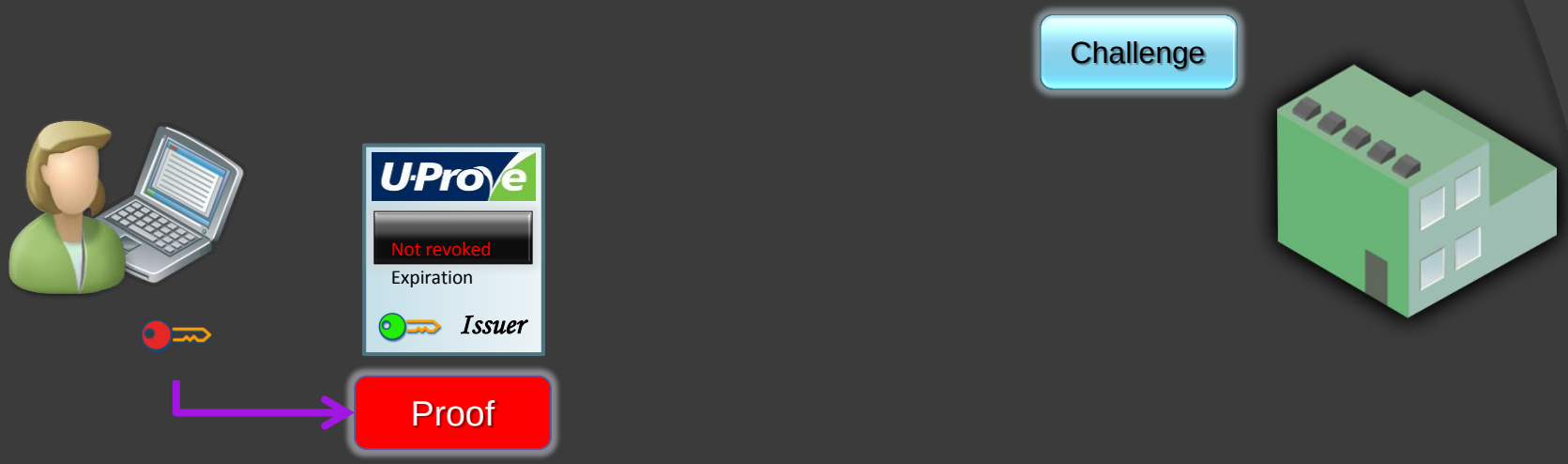
Используемая криптография

- Асимметричная криптография на базе эллиптических кривых
  - Описание, криптографическая спецификация и тестовые вектора доступны http://microsoft.com/u-prove
- При выдаче используется “restrictive blind signature”
  - Издатель знает атрибуты, но не открытый ключ и полпись, полученные в результате
- При предствлении обеспечивается proof of knowledge
  - Доказательство владения без раскрытия секрета
  - Обобщение протокола Schnorr

Протокол «слепой» подписи

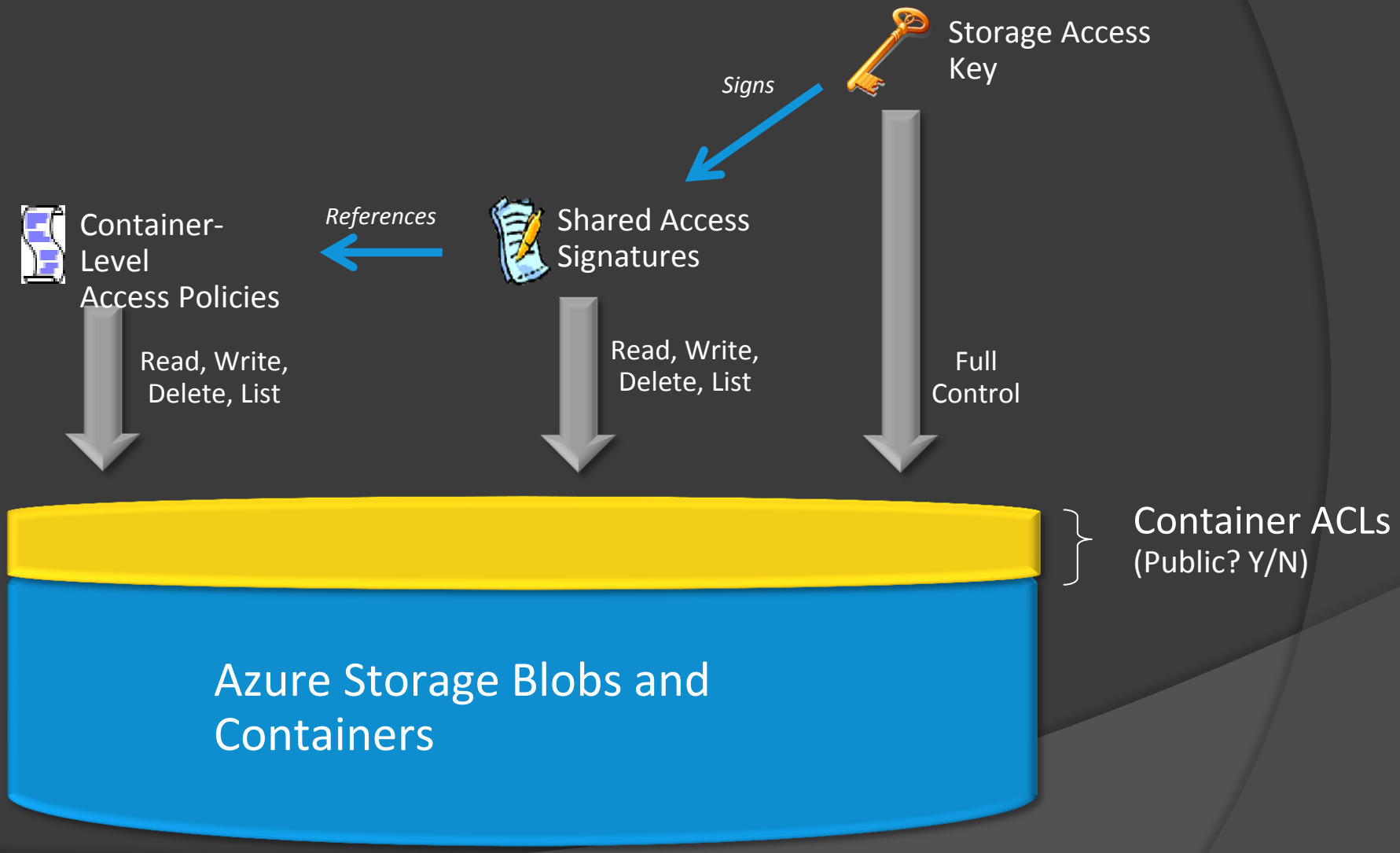
- Первоначальная информация может основываться на существующем X.509 сертификате или смарткарте
- Выпуск токена U-Prove использует “ограниченную” технику слепой подписи
  - Более сложный процесс заверения атрибутов
  - В целом протокол включает 4 обмена

Протокол Proof of Knowledge



- Проверяющая сторона сторона будет знать только раскрытую информацию и уверена, что пользователь знает секретный ключ

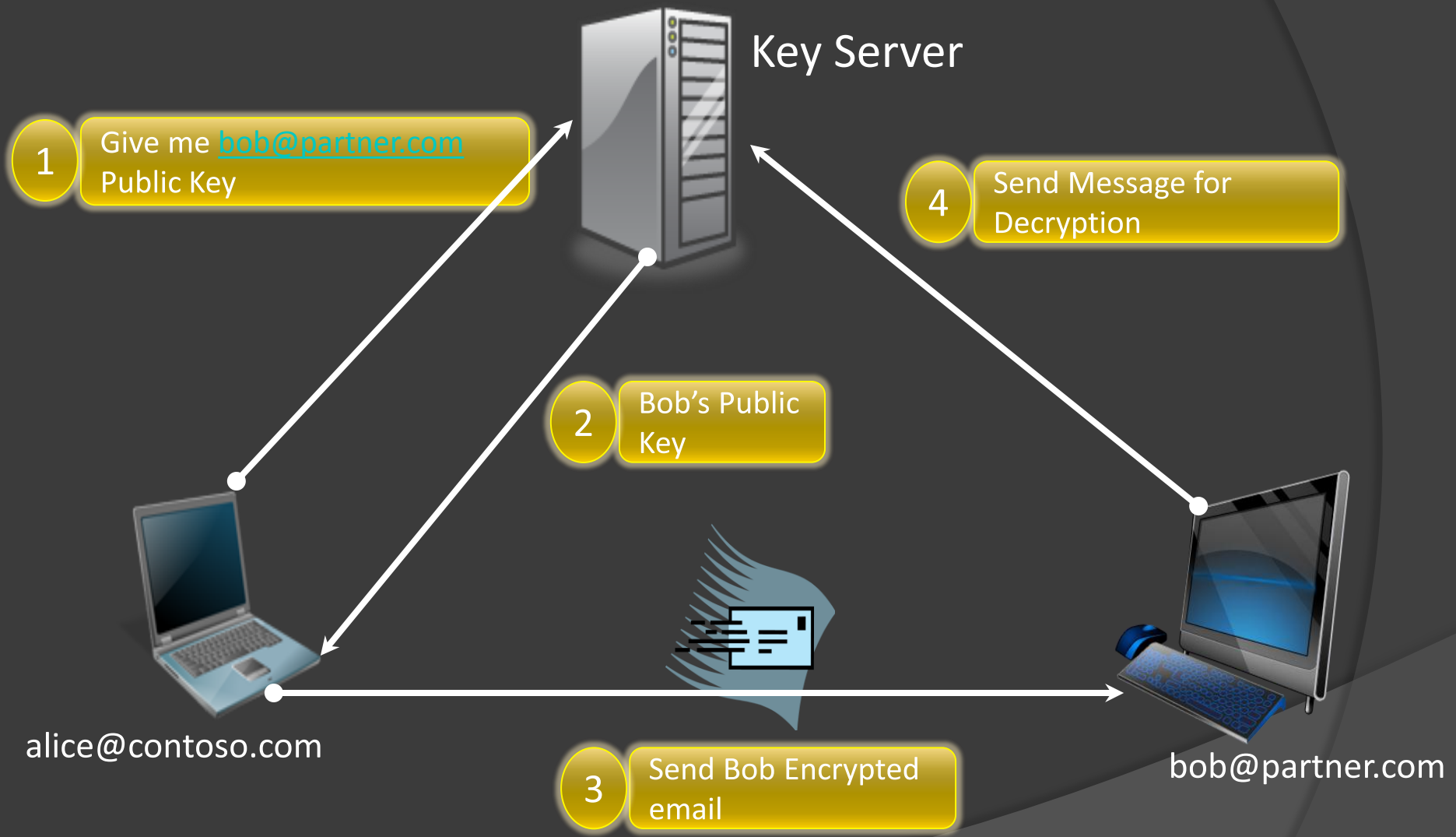
Как контролируется доступ к данным?
Модель безопасности хранения в Windows Azure



Как защищены данные?
Шифрование данных в Windows Azure

- Данные при передаче защищены TLS
  - Как для Azure Storage Services, так и для SQL Azure
- **Сейчас** нет встроенного шифрования данных при хранении в Windows Azure
  - Другая модель защиты секретного ключа для облачного сервиса
  - Данные **должны** шифроваться локально в доверенной среде!
    - Возможно разбивая на части персональные данные, например медицинские (Microsoft HealthVault)
  - .Net Crypto доступно, но возмозможно лучше использовать внешние сервисы партнеров

Identity Based Encryption



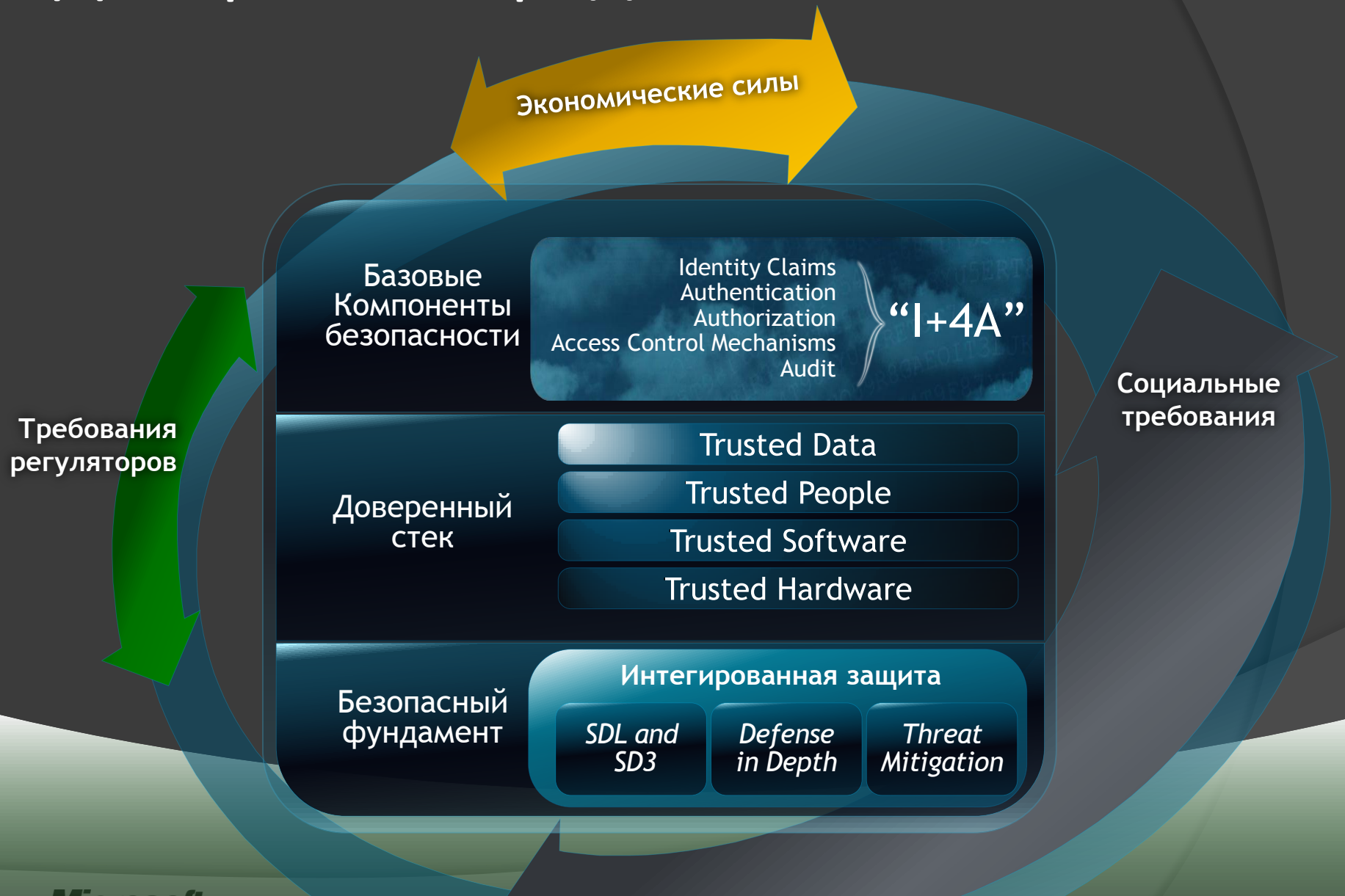
Что такое IBE?

- Асиммметричное шифрование
  - Adi Shamir в 1984, в 2001 Dan Boneh и Matt Franklin решили математическую проблему и создали первую реализацию IBE, http://csrc.nist.gov/groups/ST/IBE
- Все стороны обладают открытым и секретным ключом
  - У Key Server есть Master Key Pair (Mk_{Pub}, Mk_{Priv})
- Алгоритм:
  - Имея Mk_{Pub} и любую строку *S*, *любой* генерирует уникальный S_{pub}
  - Имея Mk_{Priv} и любую строку *S*, *любой* генерирует уникальный S_{priv}
    - В IBE, S является адрес email
- Как это работает:
  1. **Setup**: Create Master Key Pair (Mk_{Pub}, Mk_{Priv})
  2. **Extract**: Use Mk_{Priv} and ACSII string *user@hotmail.com* to generate a unique $user_{priv}$
  3. **Encrypt**: Encrypt message *m*
     - Get $user_{pub}$ using Mk_{Pub} and user@hotmail.com
     - Encrypt message *m* using $user_{pub}$ to generate *c*
  4. **Decrypt**: Decrypt cipher c
     - Get $user_{priv}$ using Mk_{Priv} and user@hotmail.com
     - Decrypt cipher *c* using $user_{priv}$ to generate *m*

Перспективные направления
http://research.microsoft.com/en-us/projects/cryptocloud/

- Multi-Authority Attribute-Based Encryption
  - Шифрование на основе атрибутов данных
- Proofs of storage
  - Обеспечение клиенту уверенности в достоверности данных, хранимых у провайдера сервиса
- Homomorphic encryption
  - Ввыполнение операций над шифрованными данными (fully-homomorphic encryption) или специальные операции (напр голосование)
- Searchable & structured encryption
  - Симметричное шифрование, позволяющее выполнять поиск по зашифрованным данным

Доверенная среда вычислений



Спасибо!

Симаков Сергей,
sergesim@microsoft.com