Стратегическая задача IT-индустрии Украины – межнациональный оператор цифровой подписи

Григорий А. Кравцов

Digitally signed by Григорий А. Кравцов
DN: cn=Григорий А. Кравцов, ou=SMTP, dc=org
Reason: I am the author of this document
Date: 2006.01.19 10:19:03 +02'00'

Автор идеи: Кравцов Григорий Алексеевич

Научный консультант: Мартыненко Сергей Васильевич

Sergii V. Martynenko

Digitally signed by Sergii V. Martynenko
DN: cn=Sergii V. Martynenko, ou=Staff, email=martyn@bkp.liga-net.org, dc=org
Reason: I am approving this document
Location: Kiev, Ukraine
Date: 2006.01.19 10:24:56 +02'00'

От составителей

- В данной презентации компания Huawei Technologies выбрана как возможный партнер при реализации проекта международного оператора цифровой подписи. Однако, это не исключает, что реальный выбор может пасть на любую другую телекоммуникационную копанию, такую как Cisco System, Lucent Technologies и другие…

Введение

В этой презентации показывается:

- Актуальность и необходимость интеграции решения PKI (Public Key Infrastructure) в системах телекоммуникации Huawei Technologies
- Задача и миссия проекта
- Бизнес-модель проекта

Актуальность

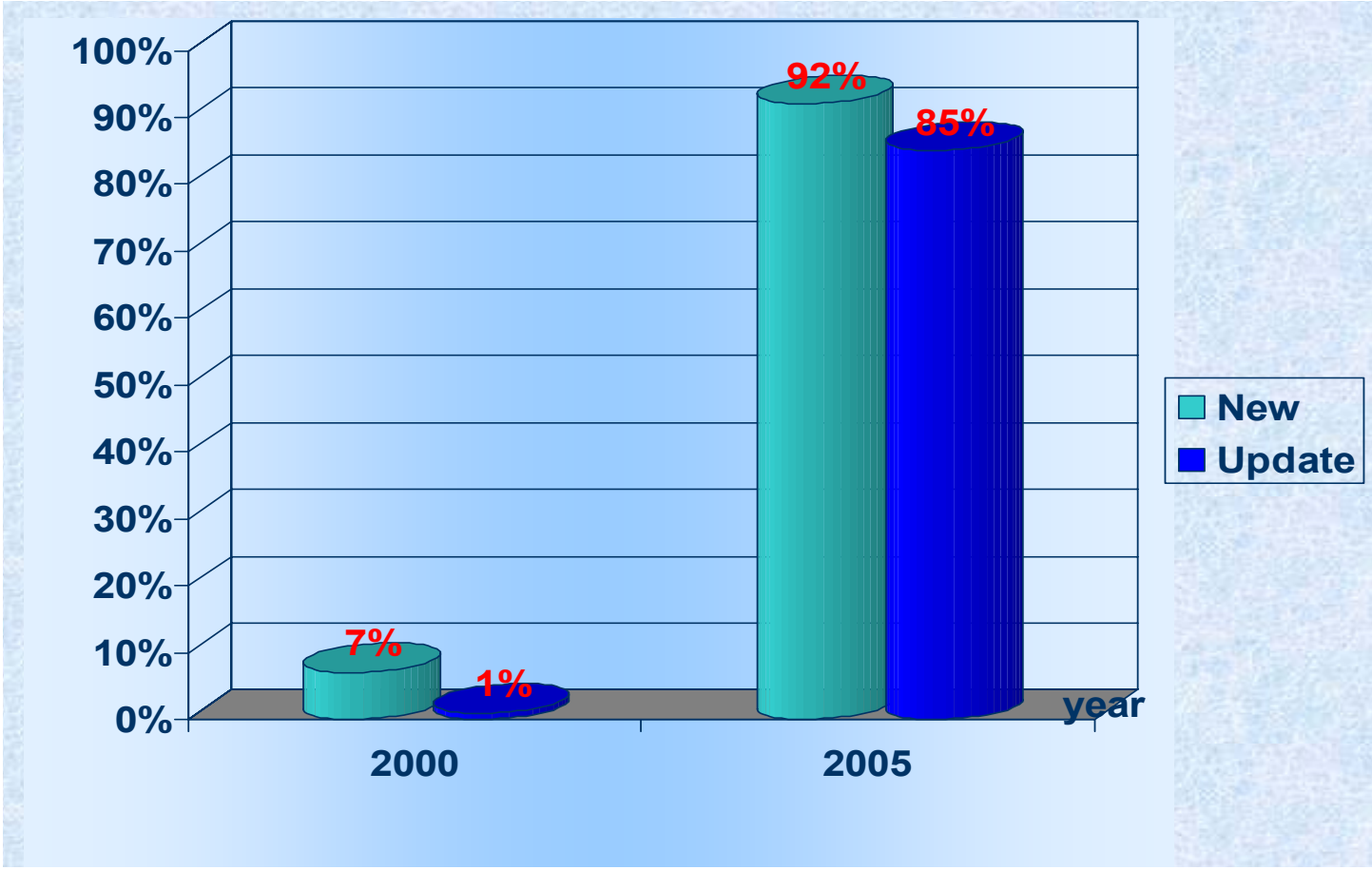
Внедрение общего стандарта архитектуры PKI (Public Key Infrastructure) необходимо для:

- электронного документооборота (B2B, B2C, C2C, eGovernment, eCustoms)
- eCommerce
- построения безопасной архитектуры End-to-End в телекоммуникациях (VPN, IPSec, …)
- и т.д

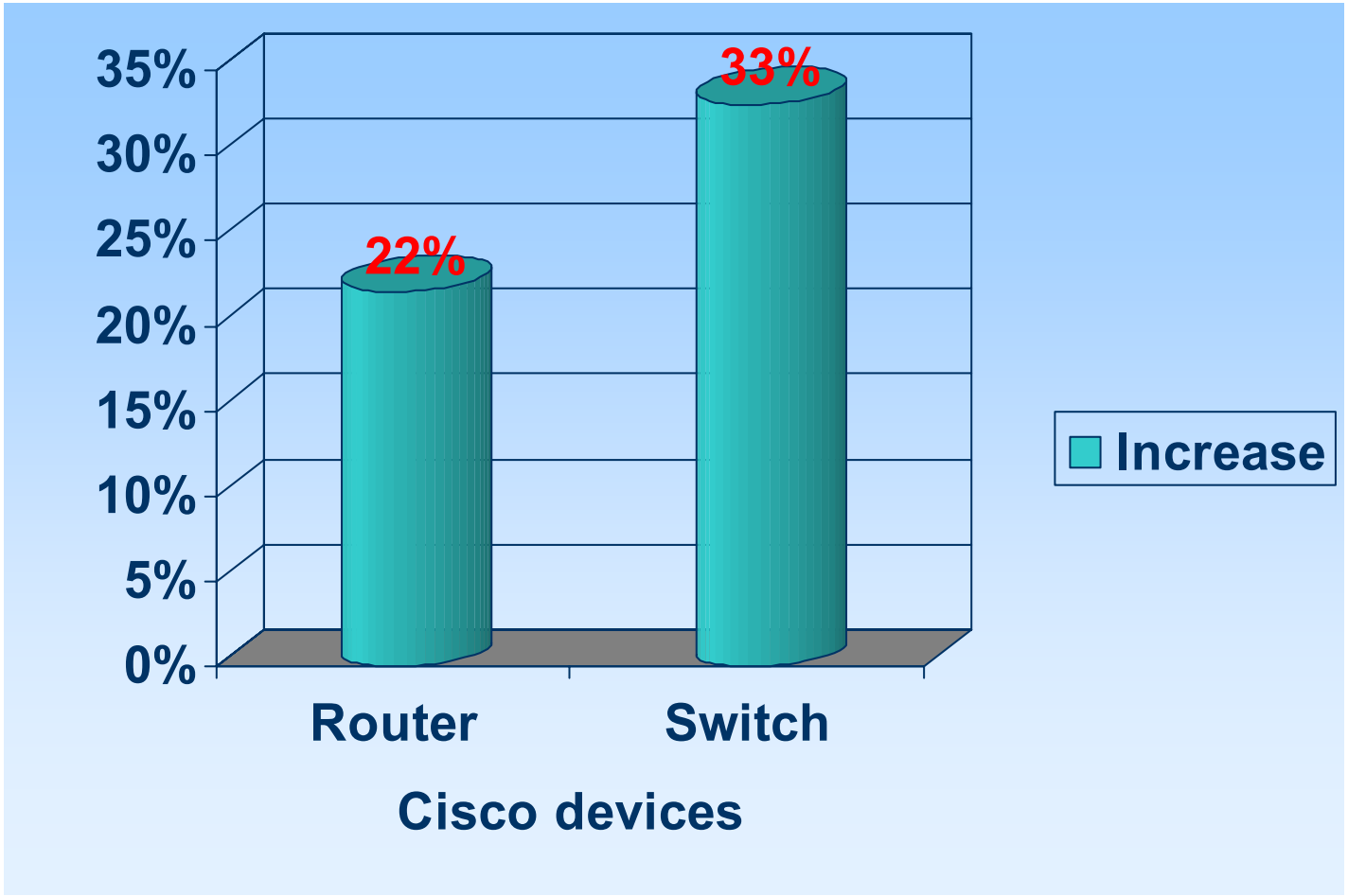
Значение защиты оборудования

- Безопасность телекоммуникаций имеет большое значение и актуальность. На данный момент у нас нет данных о продажах оборудования Huawei, однако в качестве примера мы можем привести данные о продажах продуктов Cisco в Украине

Увеличение Рынка продуктов защиты Cisco на Украине



Рост продаж оборудования Cisco после интеграции возможностей защиты в оборудование Cisco, Украина



Требования клиентов. Ч.1

Требования банков, организаций и государственных органов Украины – использовать цифровую подпись и шифрование для:

- Передачи банковских выписок по счетам;
- Подготовки и заключения контрактов (кредитных, депозитных и др.)
- Передачи налоговых деклараций, таможенных документов и др.
- Передача персональных данных и чувствительной бизнес-информации
- Защиты IP телефонии (шифрование голоса и видео, диалога-чата в on-line)

Требования клиентов. Ч.2

- Украинские банки, организации и правительственные структуры требуют, чтобы при использовании цифровой подписи и шифровании применялись следующие криптографические стандарты:

√ **RSA, 3DES, AES, MD5, и т.п. (международные и Европейские стандарты)**

√ **ГОСТ 34.310, ГОСТ 34.311, ГОСТ 28147, ДСТУ 4145 (национальные и межгосударственные стандарты для Украины, Белоруссии, России и других стран бывшего СССР)**

- Для обеспечения безопасности в больших корпоративных сетях, необходимым условием реализации протоколов VPN и IPSec является поддержка сильной аутентификации на базе цифровых сертификатов X.509

Текущее состояние

- **Сегодня существует ряд отдельных решений Huawei для применения сертификатов X.509 и построения комплексного решения Huawei PKI:**
- ✓ в задачах Huawei VPN, IPSec, SSL,
- ✓ аутентификации и др. (AAA)
- ✓ Huawei CallManager 4.0 и многие IP телефоны Huawei поддерживают цифровые сертификаты X.509, которое используют ключ шифрования для автоматического шифрования канала связи .
- ✓ Huawei CallManager может интегрироваться с Microsoft Active Directory (AD) , или Sun/iPlanet Netscape Directory Server

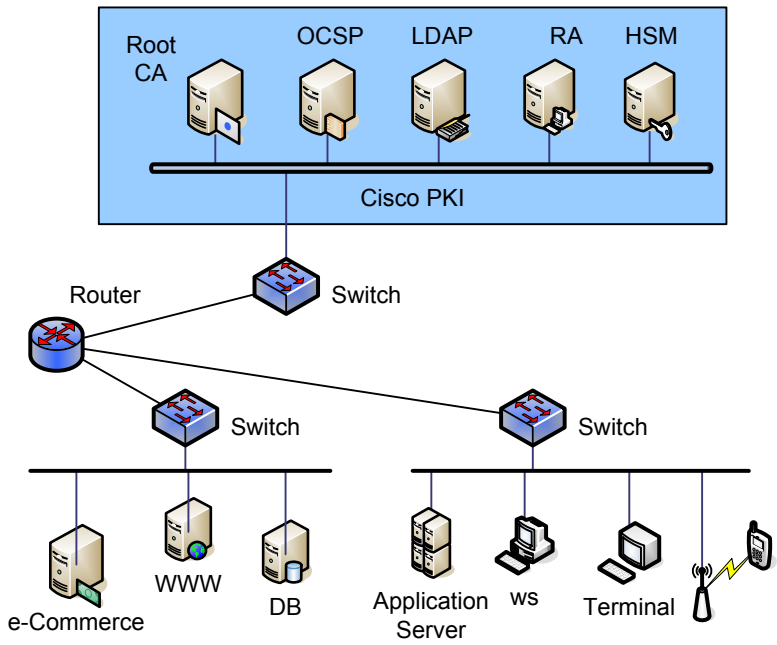
Проблемы **ч.1**

- Отсутствие гибких средств работы с сертификатами X.509
- Сложность применения PKI решений третьих (сторонних) производителей (Microsoft, Netscape, Baltimore, VeriSign, etc.), которые не интегрированы с Huawei.
- Не решены задачи замены ключей (плановой или в случае компрометации), особенно для Root CA и Subordinate CA. Отсутствует **динамическая** смена ключей.
- Не реализован пул ключей. В случае компрометации любого ключа - устройства Huawei или сертификата CA, это не позволит быстро переключиться на другой ключ. Поэтому качество обслуживания (QoS) не гарантировано

Проблемы **ч.2**

- Отсутствие аппаратного и программного интерфейса API (Application programming interface) для интеграции национальных стандартов шифрования. Поэтому нельзя применять шифрование в государственных учреждениях Украины (около 40% рынка), России и других стран.
- Отсутствует комплексное решение PKI для телекоммуникационного оборудования (например – Cisco). Во втором полугодии 2006 года это может привести к снижению рынка в банковском и коммерческом секторах (около 60% рынка Украины)
- Нет гибкого решения по объединению корпоративных VPN сетей WAN через Bridge CA

Интегрированное решение Huawei PKI

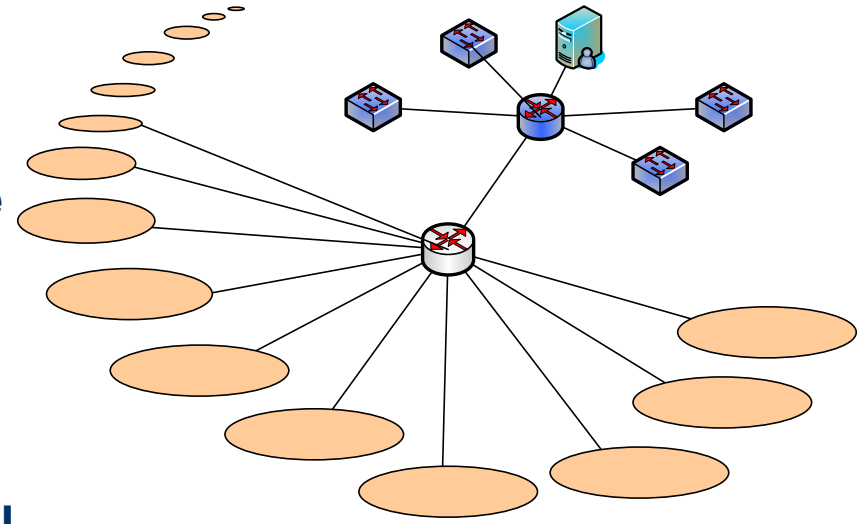


- Huawei PKI предназначен для выдачи и управления сертификатами устройств Huawei, серверов приложений и пользователей
- Каждая из служб Huawei PKI использует собственный сертификат, который хранится в Key Store HSM;
- Служба OCSP работает по протоколам HTTP (HTTPS), LDAP (LDAPS);

- LDAP – репозиторий сертификатов и списков CRL
- RA – Registration Authority
- HSM – Hardware Security Module (аппаратный модуль защиты)

Trusted Bridge CA

- Одна из проблем сегодня – объединение различных PKI доменов (корпорации, банки и др.) в единую систему PKI (государства или межгосударственную).
- Есть отдельные глобальные PKI домены – VISA, SWIFT, Identrus LLC.
- Необходимо решение Bridge CA, который устанавливает доверительные отношения для объединения разных PKI доменов (сетей).



Миссия проекта

- **Создать единое решение Huawei PKI, которое удовлетворяет потребностям :**
  - ✓ частных клиентов;
  - ✓ корпоративных клиентов: мелких и крупных компаний, в том числе **международных** компаний;
  - ✓ международных телекоммуникационных операторов;
- Создать **межнационального** оператора цифровой подписи (Bridge CA of PKI)

Геополитический аспект

- **Украина обладает уникальным геополитическим положением. Это позволяющем ей стать доверительным центром (trust-centre) между:**
  - ✓ Европой,
  - ✓ Соединенными Штатами Америки,
  - ✓ Российской Федерацией
  - ✓ Средней Азией.

- **Украина может стать центром альтернативных путей сертификации (кросс-сертификации)**

Стратегия проекта

Для успешной реализации проекта необходимо привлечение компаний-производителей, признанных лидеров в сфере телекоммуникаций и технологий smart card.

Объединение усилий этих компаний позволит им:

- ✓ Расширить рынок
- ✓ Получить конкурентные преимущества
- ✓ Развить новые направления деятельности.

Предполагаемые партнеры

- **Huawei Systems, USA** – признанный лидер рынка телекоммуникационного оборудования;
- **Axalto, Aladdin, GemPlus и др.** – признанные лидеры рынка smart card и eToken технологий;
- **ООО «НВФ «БКП-консалтинг»** - лидер рынка Украины в сфере криптографической защиты информации.

Бизнес-модель. Часть 1.

- Украина гарантирует, что решение Huawei PKI будет внедрено в масштабах государства в рамках реализации Национальной программы информатизации. (04.02.1998 №74).
- В Украине будет создан межнациональный оператор цифровой подписи (trust-centre). Участие Huawei в проекте является значимым фактором успеха, так как 80% публичных сетей Украины построены на оборудовании компании Cisco, что, как было сказано выше, не соответствует принципам безопасности.
- В Украине будет развернуто производство smart card, совместимых с Huawei PKI.

Бизнес-модель. Часть 2

- Huawei Technologies расширит свою линейку оборудования. Это позволит получить дополнительную прибыль от продажи нового решения и оборудования.
- Насыщение рынка Украины телекоммуникационным оборудованием с базовым функционалом можно осуществить за 1-2 года.
- В 2004-2005 годах в Украине было проведено обновление оборудования Cisco. Следующий цикл обновления будет через 6 лет. Если за это время Huawei Technologies реализует технологии защиты, она может потеснить Cisco на рынках Украины и России.
- В то же время, выпуск нового оборудования с новыми функциями, позволит заменить морально устаревшее оборудование и обновить оборудование (до достижения 6-ти летнего срока).
- Это приведет к появлению качественно нового рынка телекоммуникационного оборудования.

Бизнес-модель. Часть 3

- Реализация архитектуры PKI на базе оборудования Huawei - это значительный фактор стимулирования продаж VPN-концентраторов и Call-центров. Это увеличит объемы продаж Huawei.
- Интеграция смарт карт с решением Huawei PKI приведет к увеличению рынка и смарт карт, и решений Huawei.

Маркетинг

- Решение PKI, которое интегрировано с телекоммуникационным оборудованием, не имеет аналогов в мире.
- Проект априори успешен, т.к. решения третьих производителей не ориентированы на телекоммуникационное оборудование и имеют ряд проблем – различие в форматах сертификатов, отсутствие схем замены ключей, отсутствие алгоритма организации многих точек доступа к CRL и др.
- Корпорации, которые используют оборудование Huawei, охотнее выберут решение Huawei PKI, чем решение PKI третьих производителей.

Выводы ч.1

- Реализация PKI, как модульного решения, компании Huawei Technologies станет, де-факто, стандартом комплексного решения PKI.
- Этот проект станет основой технологий ePassport, без которой нельзя реализовать такие программы, как eCommerce, eHome, eHealth, eGovernment, невозможно реализовать программу Connected Government (Republic, Cities, Homes & Health), eCustoms, eVoting and etc.

(электронные коммерция, медицина, электронный дом, правительство, таможня, голосование…)

Выводы ч.2

- **Создание Huawei PKI позволит:**
- ✓ **значительно увеличить безопасность корпоративных сетей, которые построены на Huawei Routers;**
- ✓ **Обеспечить защиту решений Huawei;**
- ✓ **обеспечить безопасность Huawei IP Contact Center и других решений Huawei.**