Криптография в продуктах – сегодня и завтра

Владимир Мамыкин
Директор по информационной безопасности
Microsoft в России
vladim@microsoft.com

РусКрипто
24 марта 2016

Криптография в продуктах сегодня - 1

У каждого вендора свой подход к архитектуре крипто в своих продуктах, как правило у каждого продукта своя криптография

Ряд вендоров сосредотачивают крипто только в основных продуктах (например, в операционных системах), остальные продукты используют коннекторы к крипто-функциям

Криптография в продуктах сегодня - 2

Интерфейсы для крипто (Crypto API) у зарубежных вендоров:
- разные,
- не дают возможность встраивать крипто, отличную от уже ими используемой, во всех местах, где используется крипто

Криптография в продуктах сегодня - 3

Зарубежная крипто от разных вендоров совместима между собой:
- причина понятна

Российская крипто требует дополнительных шагов для совместимости между различными ее производителями:
- что надо делать тоже понятно…

Криптография в продуктах сегодня - 4

Новые быстро развивающиеся сферы ИТ:
- Облака
- Мобильные платформы
- Интернет вещей,
- И д.р.

недостаточно обеспечены в своих потребностях криптографическими услугами

Шаги для продвижения российской криптографии

Вводная.
Российская криптография интересует многие страны, это серьезный рынок

Что нужно делать.

1. **Всеми силами помогать ТК26 в их работе по внедрению российской крипто как международного стандарта**
2. **Работать с зарубежными вендорами для изменения их CryptoAPI в сторону интеграции с криптографией других стран.**
   - этого очень хотят многие страны: Франция, Германия, Испания, Япония, Бразилия, Китай,....

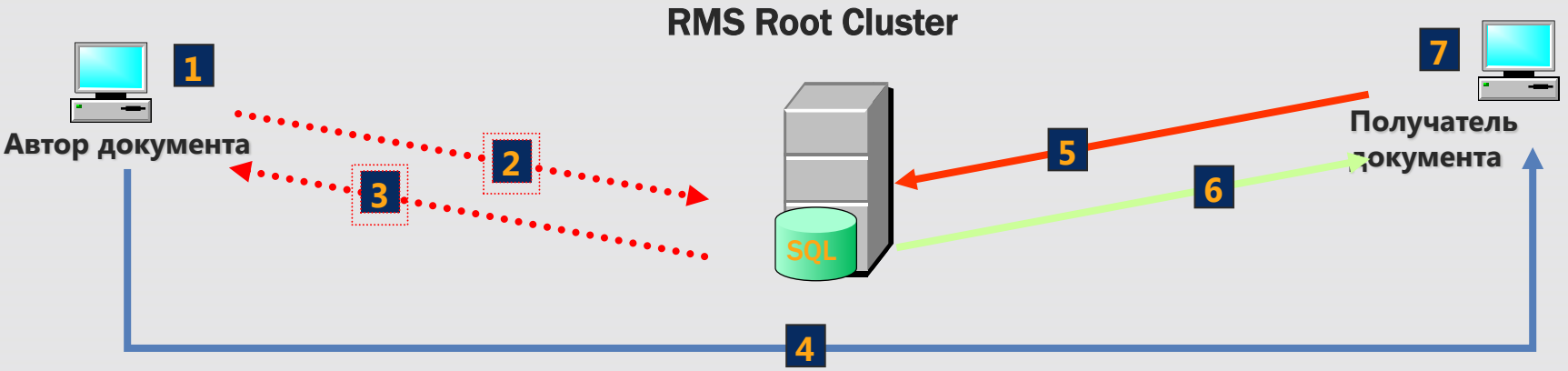
Криптография в продуктах завтра

- Международный стандарты CryptoAPI, позволяющие работать с криптографией любой страны

- Криптография только в операционных системах, все остальные продукты используют коннекторы для работы с ней

- Система криптографических сервисов для работы с различными вендорами

Начало пути в завтра - крипто в RMS (a la крипто-сервис в Microsoft Office)



1. Автор создает документ. Автор формирует набор прав и правил для документа (Publishing License). Приложение зашифровывает документ с симметричным ключом
2. Приложение посылает Publishing License серверу RMS на подпись
3. RMS подписывает Publishing License и возвращает ее приложению
4. Автор пересылает файл получателям документа
5. Получатель открывает файл. Приложение посылает серверу RMS запрос на Use License. В этот запрос включаются RM Account Certificate (RAC) получателя и Publishing license документа
6. RMS проверяет запрос и RAC, идентифицирует получателя. При успешной проверке RMS выдает получателю лицензию на работу с документом
7. Приложение получает лицензию от RMS и отрабатывает правила, заложенные в ней. Получатель работает с документом

Microsoft

Спасибо !

Поставка доверенного ПО в России – более 10 лет

vladim@microsoft.com

Основы доверия

Доступность в России исходных кодов для проверки - более 10 лет

Сертификация на соответствие требованиям безопасности ФСБ и ФСТЭК - более 10 лет

Поставка сертифицированных обновлений российскими партнерами - более 10 лет

Отсутствие «закладок» в продуктах - нет закладок

Наличие версий для работы с высшими уровнями безопасности - да

Аналоговая атака … - здесь крипто не спасает…

Microsoft

И еще раз

Спасибо !

Владимир Мамыкин
vladim@microsoft.com