

Технологии обеспечения безопасной работы клиентов ДБО

Строгая аутентификация и квалифицированная электронная подпись для порталых решений и облачных сервисов

Как получить квалифицированную электронную подпись при работе в недоверенной среде

Сергей Груздев
Генеральный директор

7.06.2012

Облачные сервисы – акселератор развития рынка

- По прогнозам IDC, к концу 2015 года объем российского рынка облачных услуг превысит отметку в \$1,2 млрд.
 - Среднегодовой темп роста более 100%
- Примеры действующих Web (облачных) сервисов
 - Единый Портал Госуслуг
 - ДБО
 - Предоставление электронной отчетности и т.д.
- Многие сервисы требуют юридической значимости
 - Требуется **строгая** аутентификация и **квалифицированная** электронная подпись
 - **Аутентификация и ЭЦП теперь всегда идут вместе!**
 - Необходимым условием является применение electronic signature creation device (смарт-карты или USB-токена с ЭЦП «на борту» и УЦ

Примеры подходов

- Поставить CSP, включить SSL/TLS (по ГОСТу)
 - Получается толстый клиент
 - CSP надо установить
 - Требуются права локального администратора
 - Как доставить (это СКЗИ)
 - Не для всех платформ
 - Как обеспечить контроль целостности среды (АПМДЗ не поставишь)
 - Срок хранения закрытого ключа всего 1 год – для массовых сервисов этого мало
 - Доля успешных атак на кражу ключей или несанкционированное использование СКЗИ (на примере ДБО)
 - более 70%

Примеры подходов

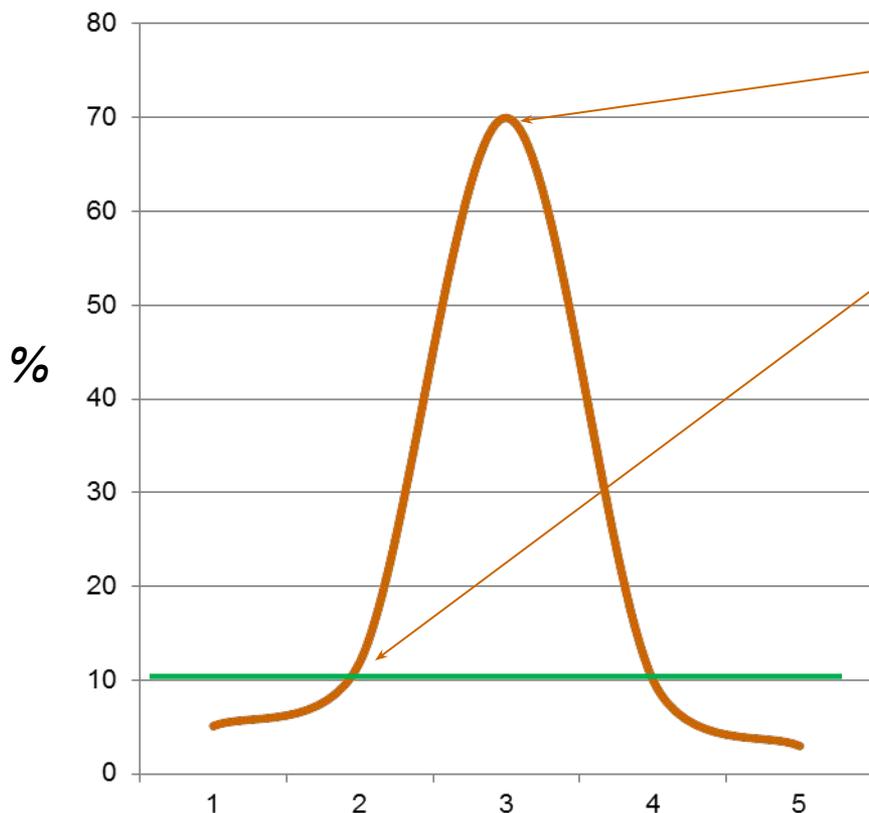
- Подписывать документы на стороне сервера
 - Поставить HSM с закрытыми ключами пользователей
 - Доступ к ключам ЭЦП предоставлять после аутентификации пользователей по одноразовому паролю (OTP-токен, генерация OTP в телефоне)
 - Удобно, можно работать с любыми платформами, в т.ч. и с мобильными, использовать так полюбившиеся iPad, iPhone и пр.
- НО:
- Надежность системы определяется самым слабым ее звеном – ненадежностью OTP-аутентификации пользователя (кто дал распоряжение за меня подписать документ?)
 - *Так можно получить только усиленную эл. подпись*

Примеры подходов

- Подписывать документы на стороне клиента
 - Куча проблем:
 - Как сделать строгую аутентификацию на тонком клиенте, для разных платформ
 - Как доверять тому что подписывается в недоверенной среде (новые атаки с подменой документа)
 - Токен (карта) с аппаратной ЭЦП (с неизвлекаемым закрытым ключом) сами по себе не панацея...
 - Еще варианты:
 - Загрузка доверенной среды с USB-Flash токена
 - Проблемы с сетевыми настройками, сильная зависимость от аппаратуры

Распределение по типам атак *

- Банки, ДБО – лакмусовая бумажка – что нас ждет
- Рынок ДБО - «средняя температура по больнице» выглядит так:



- Кража закрытого ключа с диска или незащищённого носителя **#3** – (>70%)
- Удаленное управление компьютером (с пробросом USB-порта) **#2** – (~10%)
- Кража СКЗИ, несанкционированное использование **#4** – (<10%)
- Кража ключей из памяти **#1** (<5%)
- Подмена документа **#5** (около 1%)

70% угроз снимается простым использованием токенов (S/C)

По данным GroupIB

Аутентификация и ЭЦП для облачных сервисов

Для облачных сервисов на первое место ставится удобство использования

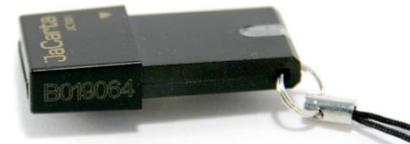
Технология взаимной двухфакторной аутентификации и квалифицированной электронной подписи для Web-порталов и облачных сервисов (*тонкий клиент ДБО*)



- Без предварительной установки драйверов, дополнительного ПО третьих фирм, без административных прав
- Для любой клиентской платформы – Windows, Mac, Linux
- Для любого браузера – MS IE, Firefox, Chrome, Opera, Safari
- С любым Web-сервером
- С защитой от современных атак и возможностью работы из недоверенной среды
- С поддержкой PKI смарт-карты

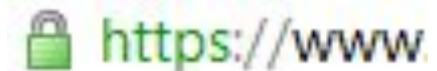
Работа с Web-порталами и облачными сервисами

- **USB-токен или смарт-карта с реализацией сертифицированной российской криптографии «на борту»**
 - Используется как персональное средство взаимной строгой двухфакторной аутентификации пользователя и портала, для формирования ЭЦП с неизвлекаемым закрытым ключом
 - Не требуется установка драйверов в современных ОС (Windows XP, MacOS, Linux), не требуются права локального администратора
 - Сертификат ФСБ (КС2), срок хранения закрытого ключа до 3х лет с возможностью самостоятельной регенерации ключей (*у конкурентов надо принести токен и переформатировать его на АРМе*)



Работа с Web-порталами и облачными сервисами

- **Кроссплатформенный мультибраузерный плагин**, обеспечивающий взаимодействие Web-приложения с токеном/картой в контексте браузера
 - **Устанавливается автоматически** при первом посещении Web-портала (как плагин в IE, Firefox, Chrome, Safari, Opera), *права локального администратора не нужны*
 - **Аутентификация** – с использованием ЭЦП (на прикладном уровне)
 - **Защита данных** – устанавливается SSL-соединение, поверх него – шифрование передаваемых данных по ГОСТ 28147-89 (на прикладном уровне)
- **ЭЦП Web-форм / файлов** (аппаратно – токеном или картой)



Работа с Web-порталами и облачными сервисами

Пример:
www.gosuslugi.ru



A screenshot of the gosuslugi.ru website in a Mozilla Firefox browser. The page title is "Вход - Mozilla Firefox". The address bar shows "gosuslugi.ru https://esia.gosuslugi.ru/idp/Authn/UserPassword?method=RFETOKEN_FLASH". The main content area is titled "ЭЛЕКТРОННОЕ ПРАВИТЕЛЬСТВО ГОСУСЛУГИ". It includes a contact number "8 (800) 100-70-10" and a section for "АВТОРИЗАЦИЯ ПО ЕТОКЕН ГОСТ" (Authentication by eToken GOST). This section contains a "Войти" (Login) button and a "PIN-код" (PIN code) input field. Navigation tabs include "ГРАЖДАНЕ РФ", "ЮРИДИЧЕСКИЕ ЛИЦА И ИП", and "ИНОСТРАННЫЕ ГРАЖДАНЕ". On the right side, there are buttons for "ПО ПАРОЛЮ" (By password), "ПО ЭЛЕКТРОННОЙ ПОДПИСИ" (By electronic signature), and "РЕГИСТРАЦИЯ" (Registration). The footer includes the Russian coat of arms, "МИНКОМСВЯЗЬ РОССИИ", and the "Ростелеком" logo.

Платежная карта с ЭЦП на борту

- В рамках проекта «Электронное правительство» отработана технология выпуска и применения банковских карт MasterCard с сертифицированной Электронной Цифровой Подписью (ЭЦП)
 - Обеспечена **100% совместимость** карт в платежной инфраструктуре, в РКІ, с Web / облачными сервисами
 - В 2011-12 несколько крупных банков вместе с Ростелекомом запускают первые ко-бренд проекты
 - Зарплатные проекты
 - С доступом к portalу госуслуг
 - Для сотрудников банка - пропуск (ID + СКУД), доступ в ИС, ЭЦП, платежные функции
 - ЭЦП на карте может использоваться в других системах
 - ДБО, Home banking (в частности, с БСС, StepUp, R-Style)
 - е-отчетность, е-торги, е-декларирование, е-коммерция (счета-фактуры), облачные сервисы

Возможности комбинированной карты



Биометрия (опция) может использоваться как третий фактор (PIN+) или второй (вместо PIN) для доступа к ИС

PIN-коды для платежного приложения и для ЭЦП разные

RFID – опция

- Гальванически развязан с чипом s/c
- Может быть 2 разных RFID-модуля
- Доступ в помещения, на парковку
- Проезд в общественном транспорте

Возможности использования

- М\н платежная карта (MasterCard, Visa)
 - Зарплатный проект, карта сотрудника предприятия
- Персональное средство формирования квалифицированной ЭП (приравненной к собственноручной подписи)
 - Для использования в проектах, где требуется юридически значимый ЭДО
 - Получение гос. услуг (Единый и региональные порталы гос. услуг)
 - ДБО, Интернет-банкинг (карта поддерживается всеми крупными разработчиками: BSS, StepUp, R-Style и др.)
 - Сдача эл. отчетности (налоговая отчетность, декларации, пенсионная отчетность, статистика, таможенное декларирование и пр.)
 - Эл. счета-фактуры (поддержка КриптоПро CSP, УЦ, операторами: ТаксКом, Калуга-Астрал, сделана интеграция в 1С-Предприятие)
 - Российский союз автостраховщиков (единая база тех. осмотра)

Платежная карта с ЭЦП на борту (пример)

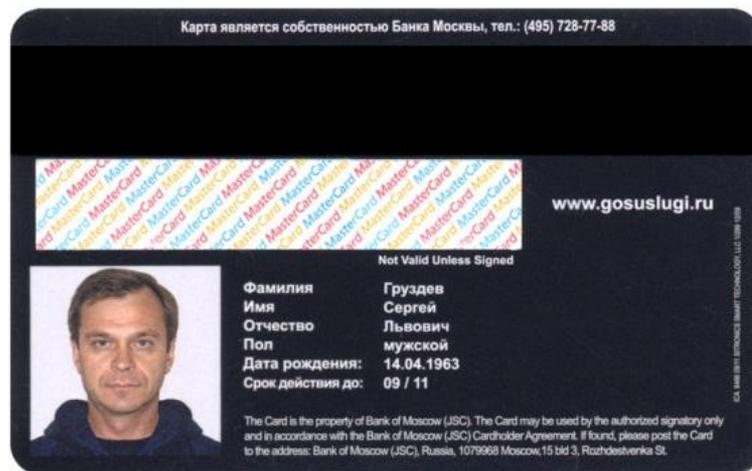
ЭЦП с
неизвлекаемым
закрытым ключом,
3 года с
возможностью
самостоятельной
перегенерации



Можем работать:

- MasterCard
- Visa
- Про100*

Можем
использовать
третий фактор –
биометрию



Проблемы недоверенной среды

Как получить квалифицированную электронную подпись при работе в недоверенной среде?



Проблемы недоверенной среды

...идут от недоверенного «железа»



Проблемы недоверенной среды

- Доверия невозможно добиться без доверенного “железа”
 - Закрытый модуль BMC, зашитый в BIOS код Management Agent (5 Мб бинарного кода!), выкусить его нельзя – в нем Clock-генератор
 - Использование сертифицированных ОС и др. средств ИБ, проверок BIOS на недоверенном “железе”, с новыми функциями удаленного управления **не решает проблем**
 - BIOS-гипервизор, закладки по технологии аппаратной виртуализации «не ловятся»

Работа с Web-порталами и облачными сервисами

- Защита от атак с подменой подписываемого документа на “зараженном” компьютере, с перехватом управления или с пробросом USB-порта на удаленный компьютер злоумышленника
 - Смарт-карт ридер с визуализацией подписываемого документа (значимые поля – по тегам)
 - Встроенная поддержка в плагин для браузеров



Что дальше? ЭЦП для мобильных платформ

Secure MicroSD для планшетов и телефонов

- Интегрирован чип смарт-карты с сертифицированной российской криптографией (ЭЦП с неизвлекаемым закрытым ключом)
- Функционал как у токенов и смарт-карт с ЭЦП на борту + Flash (2-8 Гб)
- Телефон может использоваться как средство визуализации подписываемого документа и как второй канал для подтверждения транзакций
 - В новой версии скорость аппаратного вычисления хэш и шифрование по ГОСТ 28147-89 – до 40 Кб/с



SIM-карта с ЭЦП на «борту»

- Технология аутентификации и ЭЦП документов через операторов мобильной связи



Спасибо за Ваше
внимание!

*Инновации
Лидерство
Партнерство*

