

Insurance and IT Technologies

Thursday April 26, 2012

Открытое мероприятие АЕБ “Страхование и
информационные технологии”
26 апреля 2012

Технологии и решения для применения
электронной подписи в страховом
бизнесе

Юрий Маслов
коммерческий директор

ООО «КРИПТО-ГРУПП»
maslov@cryptogroup.ru

сколько видов электронной подписи – регулирование иных аналог собственноручной подписи

Простая электронная подпись



Усиленная электронная подпись



Неквалифицированная электронная подпись

Квалифицированная электронная подпись



Средство электронной подписи СКЗИ «КриптоПро CSP»

защиты: КС1, КС2, КС3

ационные системы:

MS Windows 2000/2003/2008/2008 R2/XP/Vista/7 (IA32, IA64, x64)

Linux Standard Base ISO/IEC 23360 (IA32, x64)

ALT Linux (ia32, x64), Debian (ia32, x64), Red Hat Enterprise Linux Version 3
date 3 (ia32, x64), Trustverse Linux XP (ia32);

FreeBSD 7/8 (IA32)

Solaris 9/10 (IA32, x64, SPARC)

UNIX 5/6 (Power PC)

iOS, MacOS, Android

льзование для организации VPN с пакетом «КриптоПро IPsec»

рация: MS Office, Outlook, IIS, IE, Mozilla Firefox, Opera, Chrome; Safari,

Средство удостоверяющего центра ПАК «КриптоПро УЦ»

Версия 1.5

управление ключами и сертификатами открытых ключей
(ЭЦП, шифрования, аутентификации)

Основные возможности в новой версии:

Управление сертификатами открытых ключей на всём протяжении жизненного цикла;

Гибкая масштабируемость решения;

Высокая производительность;

Гибкая настройка политик безопасности;

Широкие возможности настройки по составу сертификатов открытых ключей;

Многоуровневая модель управления;

Наличие программных средств в виде веб-сервиса по интеграции со

иными системами;

Интегрированные веб-приложения, реализующие функционал АРМ пользователя.

Интегрированный справочник сертификатов LDAP (на основе Microsoft "Active

Организовать УЦ свой или воспользоваться услугами стороннего УЦ

Чужой: до 1000 пользователей УЦ

более 1000 пользователей УЦ



Создать свой УЦ:

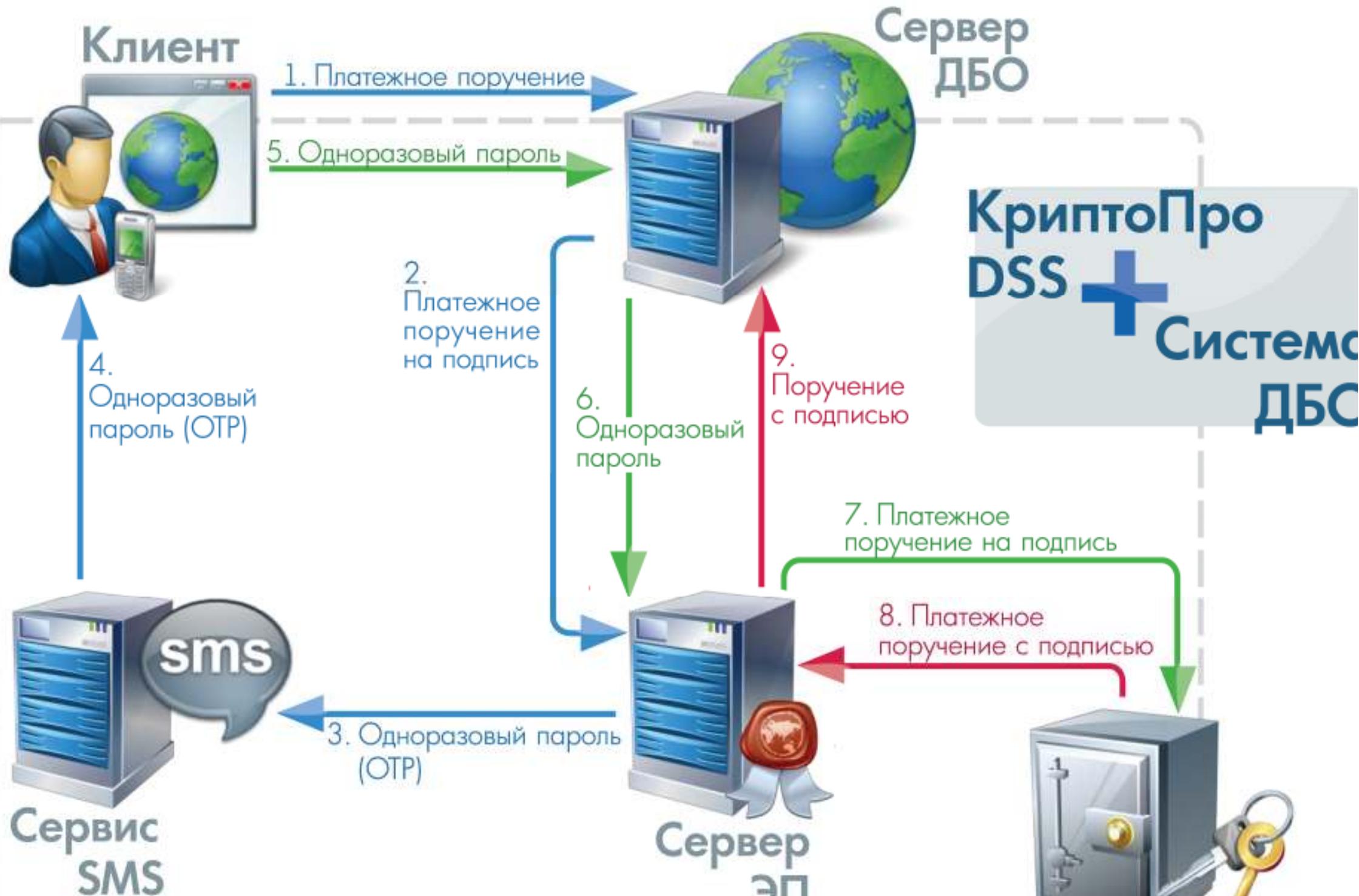
Около 3 миллионов рублей

Услуги ООО «КРИПТО-ПРО» по УЦ:

Проверка электронной подписи КристоПро DSS (СЭП КристоПро DSS)
предназначен для централизованного, защищенного хранения закрытых ключей пользователей, а также для удаленного выполнения операций по созданию электронной подписи в интересах пользователей при взаимодействии с специализированными программно-аппаратными криптографическими модулями.

СЭП КристоПро DSS обеспечивает:

- Создание ЭП в электронном документе;
- Широкий охват платформ и устройств, с которых пользователь может работать с СЭП КристоПро DSS. Необходим лишь браузер;
- Отсутствие необходимости установки клиентской части;
- Снижение риска компрометации ключей пользователей за счёт их централизованного защищённого хранения;
- Снижение стоимости развертывания и владения инфраструктурой ЭП, т.к. нет необходимости установки средства ЭП на каждое рабочее место пользователя, а управление всей инфраструктурой сосредоточено на одном сервере;
- Лёгкость встраивания функций создания ЭП в прикладные системы за счёт простоты интерфейсов автоматизации на базе стандартных средств протокола HTTP и веб-сервисов;
- Возможность применения различных схем аутентификации пользователя для





Клиент



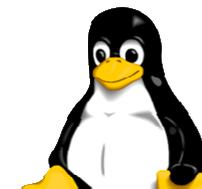
Любые
устройства



Любые
платформы

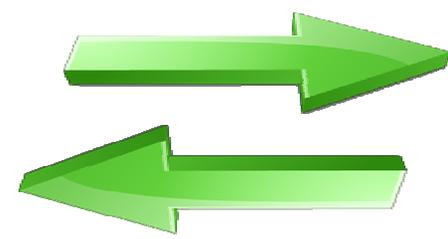


Любой
веб-браузер





Сервер
ЭП



Хранилище
ключей HSM

Сервер, который
предоставляет программный и
пользовательский интерфейс
выполнения операций по
управлению ключами,
формированию запросов на
подпись, формированию ЭП
электронного документа.
осуществляет обращение к
криптографическим функциям,
HSM

Имеет интерфейс обращения
Cryptographic Service Provider
(CSP)

Обеспечивает надежное
взаимодействие (взаимную
аутентификацию Сервера ЭП
HSM, шифрование и
целостность передаваемых
между ними данных)



Хранилище
ключей HSM

КриптоПро HSM



КМ «КриптоПро HSM» предоставляет криптографический сервис пользователям и предназначен для выполнения следующих функций:

- создание и проверка электронной цифровой подписи;
- вычисление хэш-функции;
- шифрование и расшифрование блоков данных;
- вычисление имитовставки блоков данных;
- генерация и защищенное хранение ключевой информации (все ключи хранятся в зашифрованном виде);

СПАСИБО ЗА ВНИМАНИЕ!

Юрий Маслов
maslov@cryptopro.ru

КРИПТО-ПРО – ключевое слово в защите информации

<http://www.cryptopro.ru>

info@cryptopro.ru

alexg@cryptopro.ru

Тел./факс

+7 (495) 780-48-

+7 (495) 660-23-