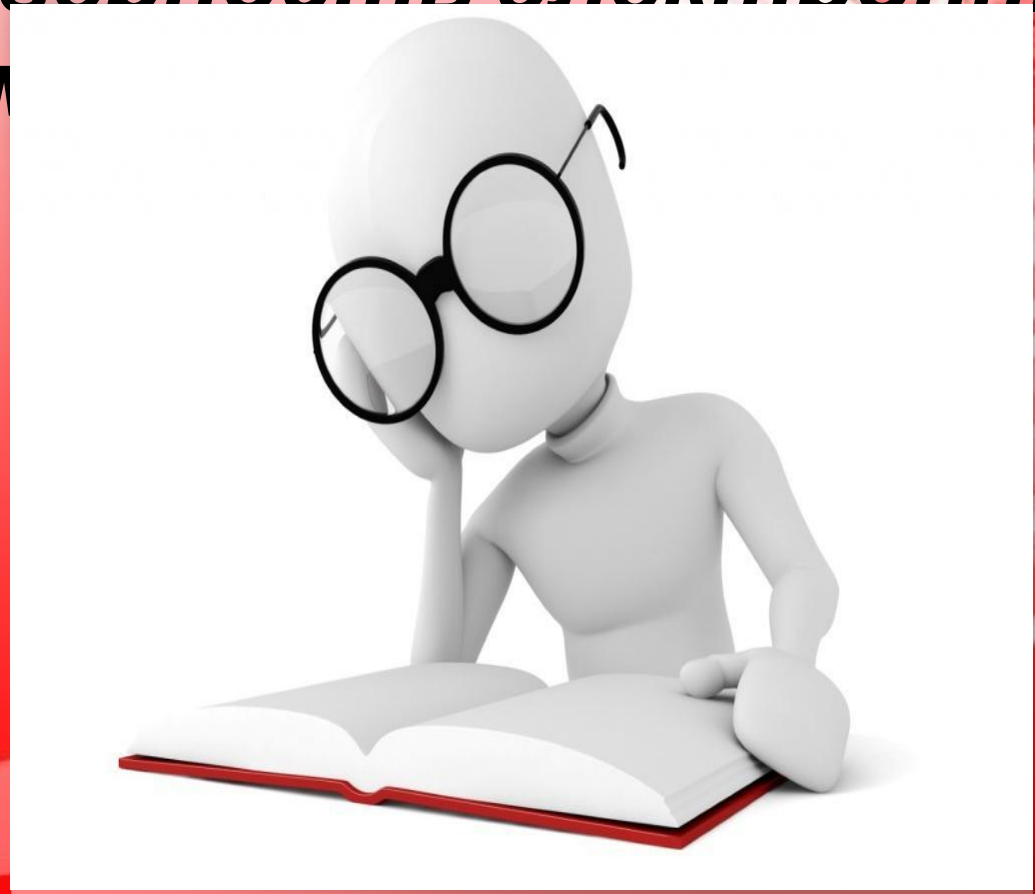
КРИПТО ПРО

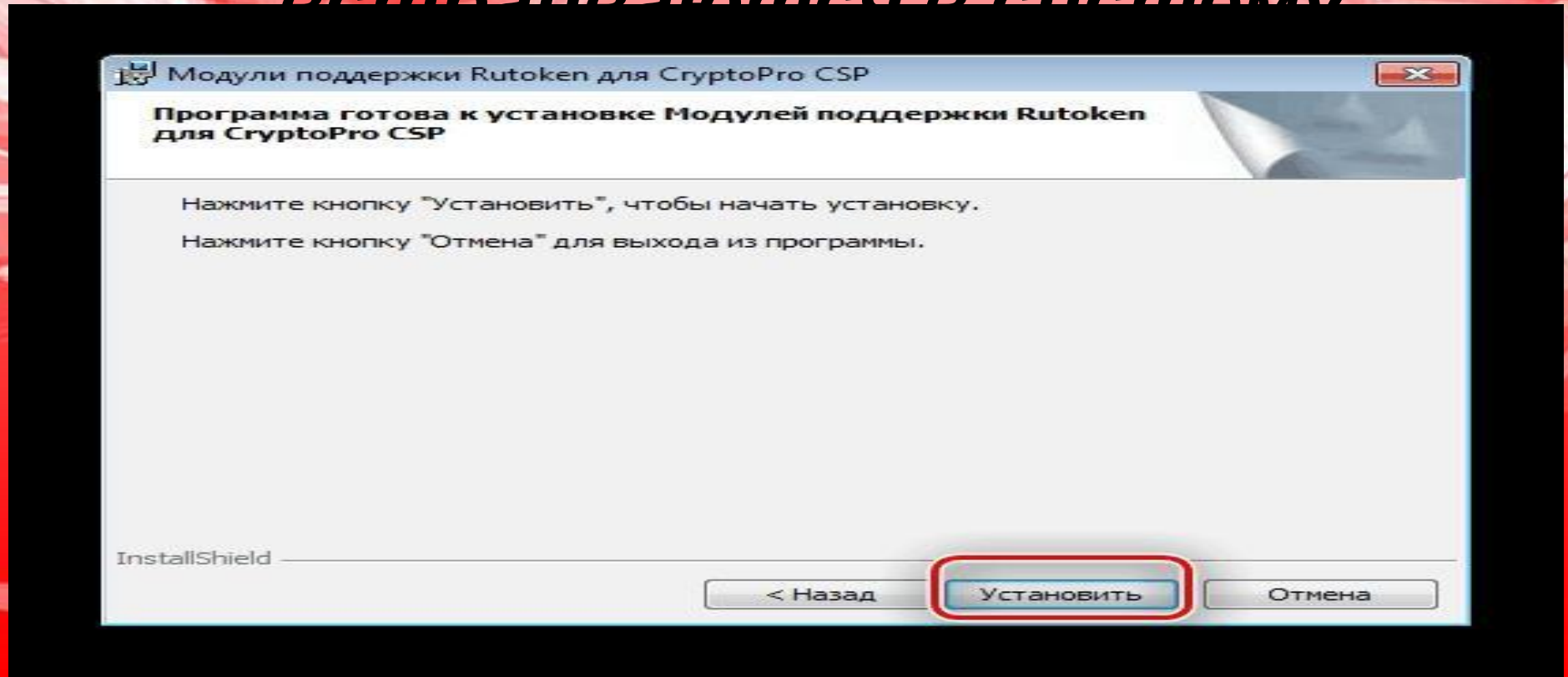
# Понятие Crypto Pro CSP

- *Crypto Pro CSP представляет собой криптопровайдер, средство криптографической защиты, предназначенное для обеспечения целостности программных приложений при помощи методов шифрования.*

- *Также ПО позволяет защитить конфиденциальную информацию при обмене данными через интернет и обеспечить юридическую достоверность электронных докум*



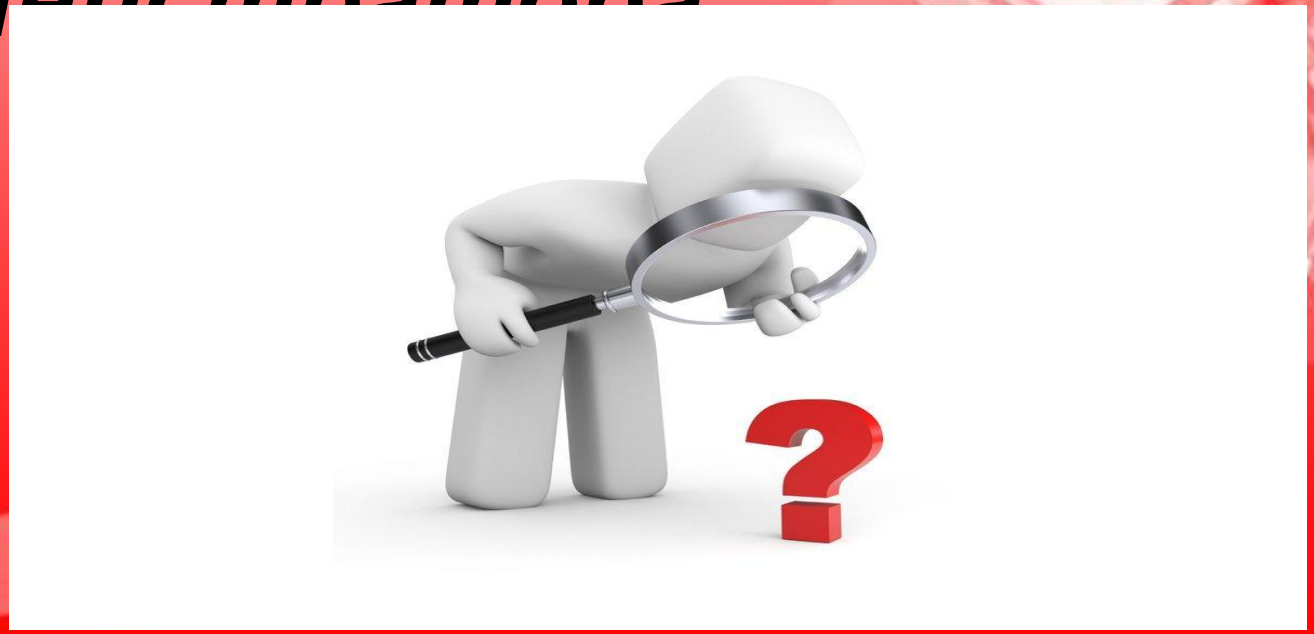
- ***В соответствии с российскими государственными стандартами, принятыми в сфере криптозащиты ПО позволяет обезопасить электронную информацию при помощи модулей, которые встраиваются в систему***



- ***Программа обеспечивает идентификацию и авторство при электронном документообороте.***

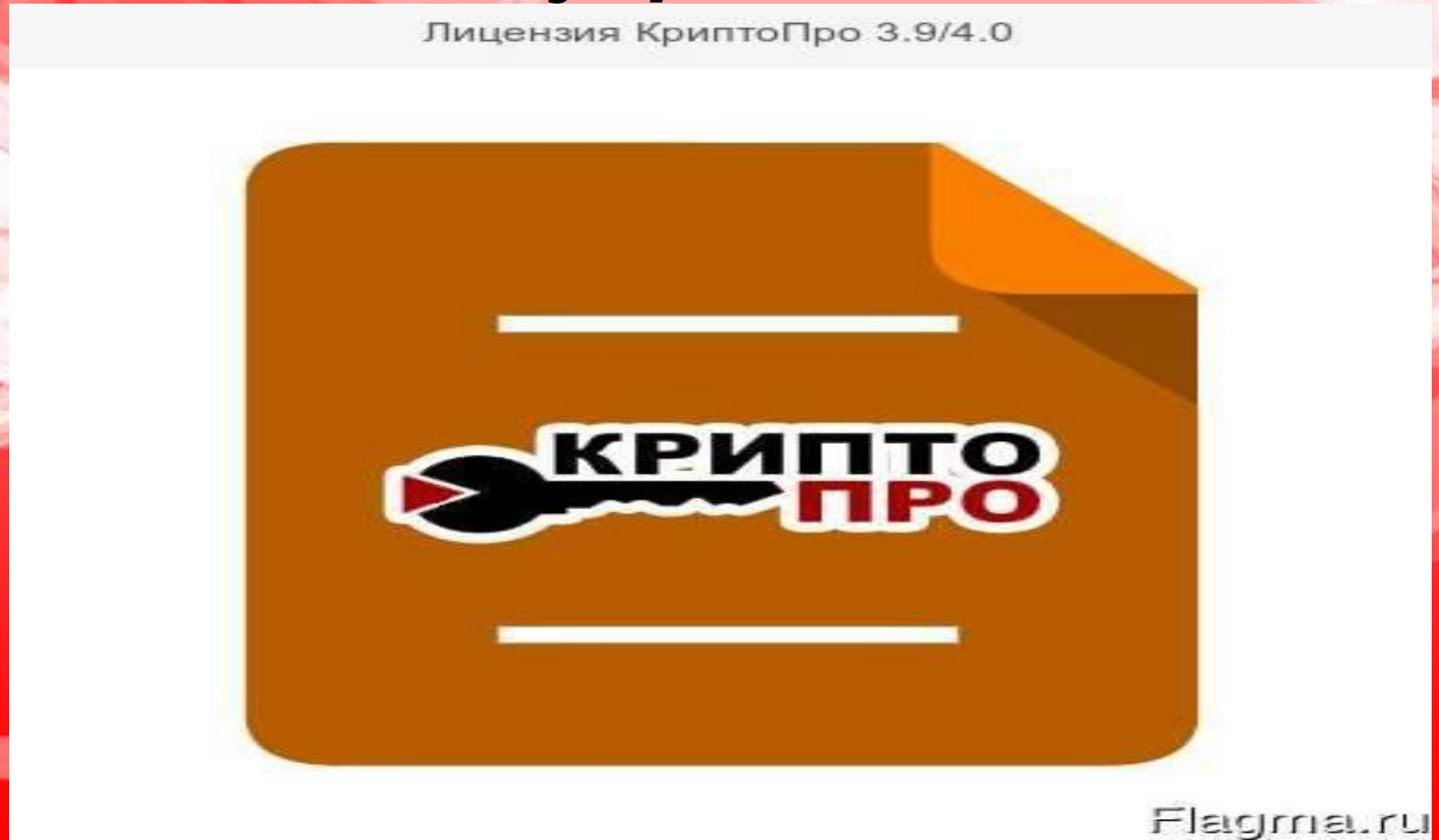
# Как включить Crypto Pro ?

- Чтобы включить программу Crypto Pro необходимо, чтобы она была установлена на компьютере. Для инсталляции программы потребуются права администратора



- ***В момент установки ПО можно будет также установить дополнительные настройки через панель свойств. После установки потребуется перезагрузить компьютер для того,***

- *Чтобы включить программу, необходимо зайти в меню «Пуск» и зайти в пункт «Программы». В открывшемся списке доступен не только запуск программы, но и панель настройки, а также средство для управления лицензиями.*



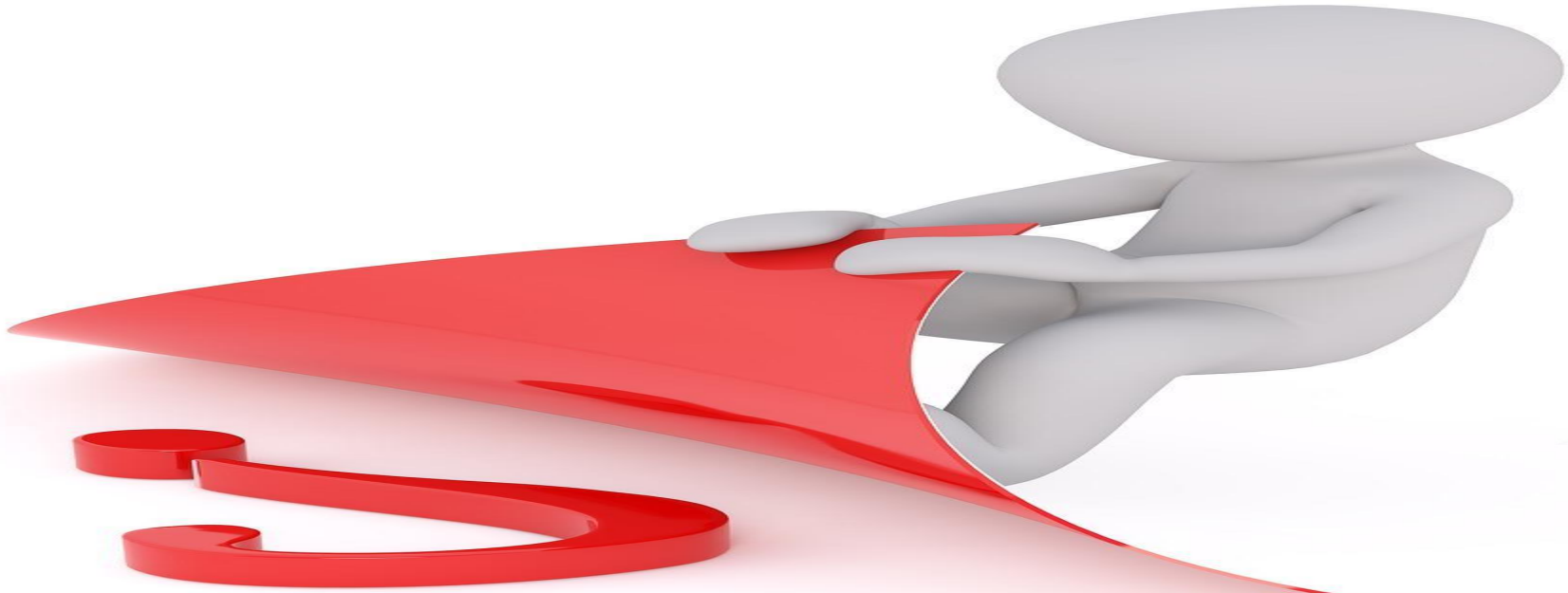
# Как пользоваться ЭЦП Crypto Pro?

- Использование электронной подписи необходимо для идентификации и авторства электронных документов, юридической верификации электронного

- ***Электронная подпись решает вопрос доказательства момента подписи документа и действительность сертификата на данный момент. Для примера, приводится момент подписания документа Microsoft Word 2010.***

***Помимо программного комплекса Crypto Pro CSP, необходимы корневой сертификат УЦ и личный сертификат владельца ЭЦП. Для подписания документа, должен быть установлен плагин «КриптоПро Oj***

•*Открыв документ, нужно зайти в пункт «Файл», зайдя во вкладку «Сведения» нужно выбрать пункт «Добавить цифровую подпись». В окне подписания документа нужно указать личный сертификат либо выбрать его из списка имеющихся. Указав пароль к контейнеру ключа, если он имеется, в документе появится окно о статусе подписания документа.*



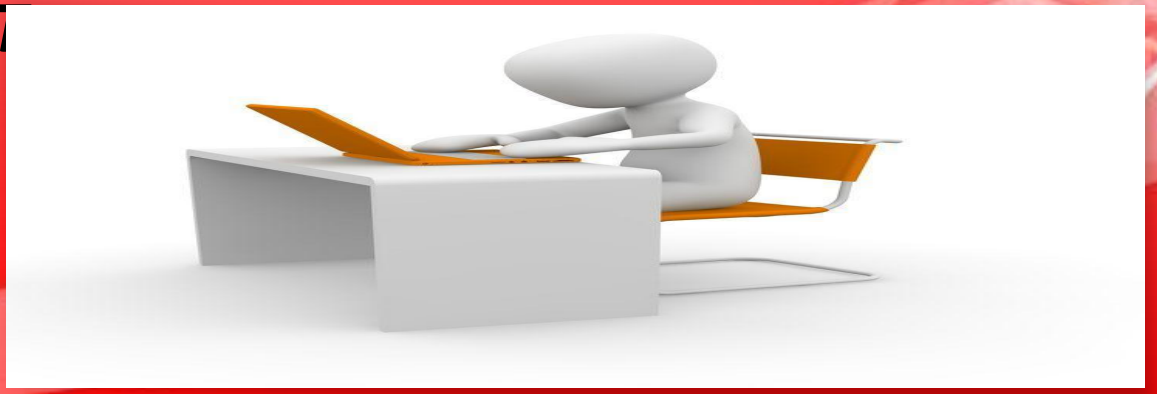
# Crypto Pro PKI: что это?

- *КриптоПро PKI представляет собой систему управления открытыми ключами, благодаря которой можно управлять криптографической защитой. Используя данную инфраструктуру, можно регулировать политику выпуска цифровых сертификатов, признавать их недействительность. В перечень функций входит также хранение информации, которая необходима для проверки*

- *КриптоПро PKI поддерживается: электронной почтой, платежами, протоколами, документами с электронной цифровой подписью и многим другим. PKI применяется при использовании программного инструментария Microsoft для конструирования решений на основе инфраструктуры открытых ключей.*

# •Crypto Pro Sharpei: что это?

*Crypto Pro Sharpei предназначен для создания новых приложений, которые надежно защищены.*
*Также благодаря применению этого дистрибутива можно использовать стандартное ПО, например, Microsoft Office Forms Server 2007 чтобы подписывать и верифицировать ЭЦП при помощи отечественных государственных стандартов.*
*Согласно информации, на официальном сайте на данный момент продукт КриптоПро Sharpei не разрабатывается, а его функции перенесены в КриптоПро .NET*



# Рутокен ЭЦП: что это?

- *Рутокен ЭЦП 2.0b - электронный идентификатор с аппаратной реализацией российских стандартов электронной подписи, шифрования и хеширования. Обеспечивает безопасное хранение ключей электронной подписи во встроенной защищенной памяти без возможности их экспорта*

# Для чего нужен Рутокен ЭЦП?

- Рутокен ЭЦП предназначен для безопасной двухфакторной аутентификации пользователей, генерации и защищенного хранения ключей шифрования и ключей электронной подписи, выполнения шифрования и самой электронной подписи «на борту» устройства, а также хранения цифровых

# eToken: что это?

- ***eToken – персональное устройство идентификации и хранения персональных данных, аппаратно поддерживающее работу с цифровыми сертификатами и электронно-цифровой подписью (ЭЦП). eToken выглядит ровно как USB-флэшка.***

# Основное назначение

- *Чёткая двухэтапная идентификация пользователей при доступе к закрытым ресурсам (компьютерам, сетям и приложениям).*
- *Безопасное хранение закрытых ключей цифровых сертификатов и криптографических ключей.*
- *Аппаратное исполнение криптографических операций в доверенной среде (генерация ключей шифрования, формирования ЭЦП).*

# Клиентские сертификаты: что это?

- **Клиентские сертификаты – предназначены для аутентификации владельца в защищенных клиент-серверных приложениях и для использования в системах юридически значимого электронного документооборота при формировании и проверке электронной цифровой подписи (ЭЦП) .**
- **Контроль достоверности данных в сертификате обеспечивает строгую криптографическую аутентификацию и неотказуемость владельца сертификатаот своей подписи под электронными документами.**

УДОСТОВЕРЯЮЩИЙ ЦЕНТР
ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ
Некоммерческое партнерство инновационной деятельности в социальной сфере
«МосГорУслуга»
111397, г.Москва, Зеленый проспект, д. 20

СЕРТИФИКАТ
КЛЮЧА ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

№: 260E 41EB 0000 0000 092A

*Владелец сертификата:* Башков Владимир Анатольевич
*Организация:* ЗАО "Вимком Оптик ТС"
*Действителен с:* 2 февраля 2011 г. 14:05:00 UTC
*Действителен до:* 25 ноября 2011 г. 14:15:00 UTC

*Сведения об отношениях:*
Использование на электронных площадках отобранных для проведения аукционов в электронной форме
Юридическое лицо
Участник размещения заказа
Администратор организации
Уполномоченный специалист
Специалист с правом подписи контракта
Проверка подлинности клиента
Защищенная электронная почта

*Открытый ключ ЭЦП:*
0440 8ED8 967E DDA7 CAD8 0550 0666 E374 EBB8 E62A 2500 6816
EA08 1A6F 0196 261B 84F0 D930 7831 BD4C D123 FF86 5D69 AE2A
EEC4 C39A 6CBA C4F2 0721 DA13 E497 2FAE DC6F

*Наименование СКЗИ:* КриптоПро CSP
*Ключевой контейнер:* RaUser-eae995a3-bd90-4078-abf8-08bb3042430e
*Ключевой носитель:* ETOKEN_JAVA_00578e9c

*Подпись владельца сертификата:* _____
*Получил:* _____ (подпись) _____ (ФИО)
По доверенности

*Уполномоченное лицо УЦ: Хотченков А. И.* _____

№ 0001820

«МосГорУслуга» Удостоверяющий центр электронной цифровой подписи

# Клиентский SSL сертификат: для чего используется?

- Протокол SSL, используемый обычно для безопасной передачи данных, может применяться для авторизации клиентов на сервере – для этого используются клиентские SSL сертификаты.
- Клиентские SSL-сертификаты используются для идентификации клиента или пользователя и аутентификации клиента на сервере. Обычно в таком случае используется двухфакторная идентификация – через логин/пароль, а также через