

# Использование двухфакторной аутентификации и ЭП на базе eToken в ЭДО

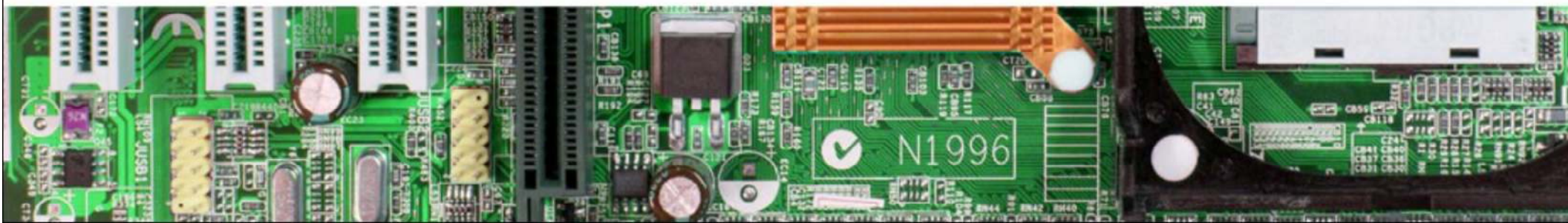
Александр Астахов

Генеральный директор



**Global  
Trust  
Solutions**

Продукты и услуги в области информационной безопасности



# Федеральный закон N 63-ФЗ "Об электронной подписи"

- **Квалифицированная ЭП** = квалифицированный сертификат + сертифицированные средства ЭП (признается равнозначной документу на бумажном носителе)
- **Квалифицированный сертификат ключа ЭП** = сертификат, выданные аккредитованным УЦ
- **Усиленная ЭП** соответствует документу, заверенному печатью (при условии использования сертифицированных средств ЭП)
- **Минкомсвязи**: определяет правила аккредитации УЦ, ведет реестр квалифицированных сертификатов, выполняет функции головного УЦ
- **ФСБ**: устанавливает требования к формированию квалифицированного сертификата, к средствам ЭП и УЦ, проводит сертификацию

# Удостоверяющий Центр

- УЦ – служба, выдающая сертификаты
  - Служба, которой доверяют все объекты, взаимодействующие с помощью инфраструктуры открытых ключей
- УЦ
  - ✓ Выдача сертификатов клиентам
    - Генерация ключей по требованию
  - ✓ Отзыв сертификатов
    - Публикация Certificate Revocation List (CRL)
  - ✓ Хранение истории всех выданных сертификатов



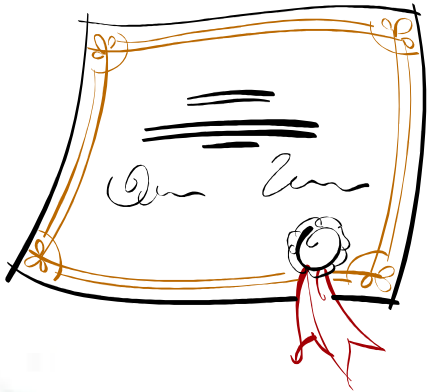


# Цифровой сертификат



- Цифровое удостоверение
  - Стандарт X.509 версия 3
- Информация, однозначно идентифицирующая субъекта
  - Его открытый ключ
  - ФИО, название и адрес организации
- Информация, необходимая для проверки сертификата
  - Срок действия сертификата
  - Информация о службе, выдавшей сертификат
  - Средства ЭП и стандарты
- Цифровая подпись УЦ

# Цифровой сертификат



- Цифровой документ, удостоверяющий подлинность соответствия:
  - ✓ «Данный открытый ключ действительно принадлежит предъявителю сертификата»
- Основной элемент инфраструктуры открытых ключей
  - ✓ Построен по ITU X.509

# Факторы аутентификации

Для прохождения процедуры аутентификации пользователь должен:





# Средства аутентификации

- Дискета (1 фактор)
- Touch Memory (1 либо 2 фактора)
- Смарт-карта (2 фактора)
- USB-токен (2 фактора)
- Технология одноразовых паролей, OTP (2 фактора)



# Семейство eToken



- eToken ГОСТ (ГОСТ Р 34.10-2001, серт. ФСБ)
- eToken PRO (Java) (загрузка апплетов)
- КриптоПро eToken CSP (поддержка СКЗИ КриптоПро CSP)
- eToken NG-FLASH (Java) (16 Гб)
- eToken NG-OTP (Java) (генератор OTP)
- eToken PASS (автономный OTP)
- eToken PRO Anywhere (доступ к веб-ресурсам без установки клиентского ПО)



# Назначение смарт-карт/USB-ключей eToken

- **Аппаратная генерация криптографических ключей**
- **Безопасное выполнение криптографических операций**
- **Надежное хранение атрибутов доступа, ключевой информации и персональных настроек**

# Использование смарт-карт технологий и цифровых сертификатов

Аутентификация пользователей:

- Операционные системы: Windows (SmartCard Logon), Novell ...
- Web – ресурсы и порталы: IBM WebSphere, MS IIS, Apache и т.д.
- VPN сети (EAP RADIUS)

# Использование смарт-карт технологий и цифровых сертификатов

Аутентификация пользователей :

- Терминальный или доступ (Citrix MF, MS Terminal Service)
- Административный доступ (SSH)
- Бизнес приложения и КИС(SAP R/3, Oracle, Lotus)
- Банковские и платежные системы



# eToken Network Logon


В простейшем сценарии использования eToken Network Logon:

- сгенерирует для пользователя новый сложный пароль для входа в Windows (длиной 14 символов, обязательно содержащий буквы верхнего и нижнего регистра, цифры, спецсимволы);
- сменит текущий пароль пользователя Windows на новый сложный пароль;
- сохранит новый сложный пароль для входа в Windows в защищенной памяти USB-ключа или смарт-карты eToken.

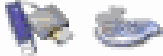
# eToken Network Logon

Операционная система Windows

**eToken**  
YOUR KEY TO SECURITY



**Aladdin**  
SECURING THE GLOBAL VILLAGE

 Connect a token or press Ctrl-Alt-Delete to begin.

Нажатие этого сочетания клавиш обеспечивает безопасность ввода пароля. Нажмите кнопку "Справка" для получения дополнительных сведений.

[Справка](#)

[Logon using a token \(CTRL+L\)](#)


[Troubleshooting](#)

[I lost my token](#)

Aladdin Knowledge Systems Ltd. Copyright (C) 2009

Вход в Windows

**eToken**  
YOUR KEY TO SECURITY



**Aladdin**  
SECURING THE GLOBAL VILLAGE

Пользователь:

Token password:

[I forgot my eToken Password](#)

[Create Profile on Token](#)

Вход в:

С использованием удаленного доступа

**EN**

# Token Management System

- **Поэкземплярный учет и регистрация** всех аппаратных и программных токенов, используемых сотрудниками.
- **Ускорение ввода в эксплуатацию** токенов, автоматизация процессов выдачи eToken сотруднику, персонализация eToken, запись ключевой информации и аутентификационных данных в память eToken.
- **Управление жизненным циклом** токенов: обновление аутентификационных данных и ключевой информации, предоставление / отзыв прав доступа к приложениям при изменении служебных обязанностей / увольнении сотрудника, замена устройства при его утере / повреждении, вывод устройства из эксплуатации.
- **Аудит использования** сотрудником выданного ему токена (фиксируются все факты использования устройства сотрудником на компьютере предприятия, изменения хранящихся в памяти устройства данных).
- **Подготовка отчетов** для руководителей служб ИТ и ИБ об использовании сотрудниками токенов (на основе данных аудита средствами встроенного генератора отчетов, также имеется возможность экспорта данных во внешние средства построения отчетов).
- **Техническая поддержка** и сопровождение пользователей токенов через веб-сайт технической поддержки: переустановка забытого пользователем PIN-кода устройства, синхронизация генератора одноразовых паролей, обработка типовых ситуаций "пользователь забыл eToken", "пользователь потерял eToken", "пользователь повредил / сломал eToken".



# Архитектура TMS

## Организационные политики



## Приложения безопасности

## Пользователи и устройства



# Спасибо за внимание!



**Global  
Trust  
Solutions**

**ООО «ГлобалТраст Солюшинс»**

Продукты и услуги в области  
информационной безопасности

**Астахов  
Александр Михайлович**

генеральный директор

---

123317, Россия, Москва,  
Пресненская наб., 10, блок С,  
Бизнес-центр «Регус»  
[www.globaltrust.ru](http://www.globaltrust.ru)

Тел.: +7 (495) 651-66-17  
Моб.: +7 (495) 991-80-37  
Факс: +7 (495) 967-76-00  
E-mail: [AlexAstahov@globaltrust.ru](mailto:AlexAstahov@globaltrust.ru)