

# Использование eToken

<http://www.Aladdin.ru>

# Средства аутентификации

Дискета

Touch Memory (iButton)

Магнитная карта

Скретч-карта

**Смарт-карта**

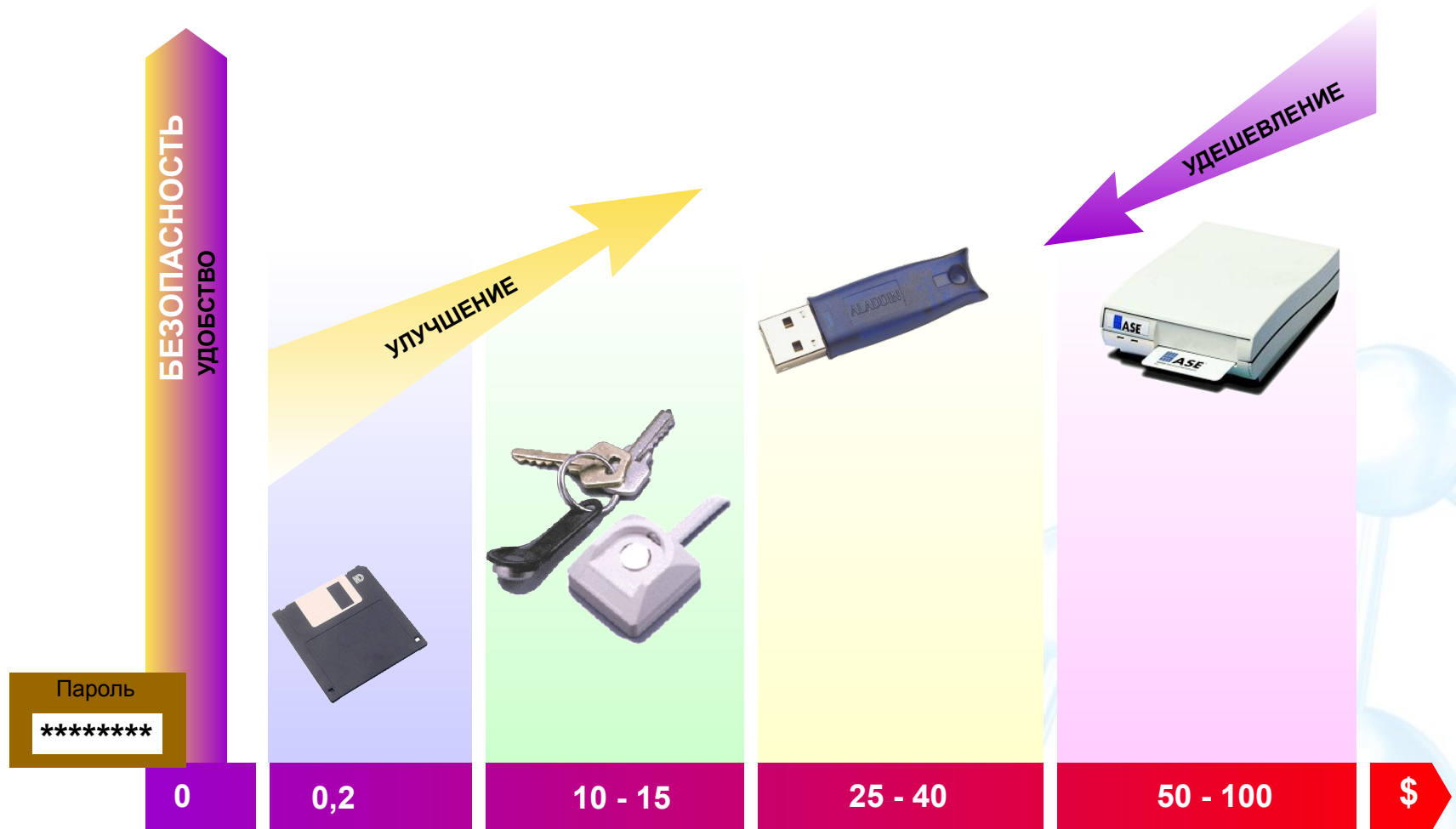
**USB-токен**

DigiPass, SecureID и пр. (генераторы одноразовых паролей)

Биометрические системы



# Идентификаторы



## Способы аутентификации:

- Логин + пароль                      1 фактор
- Дискета + пароль в ПО              2 фактора
- Touch Memory + пароль            2 фактора
- Смарт карта + PIN                  2 фактора
- Отпечаток пальца                    1 фактор
- USB-ключ + PIN                    2 фактора

# Что такое eToken?



Брелок для  
USB-порта

аппаратное средство для  
аутентификации и безопасного  
хранения ключевой информации



Смарт-карта



Считыватель смарт- карт  
+ кабель для подключения

# USB

## Достоинства

Нет ограничений на IRQ или окно памяти

Поддерживается до 127 устройств

быстрота

USB 1.1 (12 Мбит/сек)

USB 2.0 (480 Мбит/сек)

Параллельные и последовательные устройства можно перемещать между несколькими устройствами

## Недостатки

Нет поддержки Microsoft для Windows NT

Очень ограниченная поддержка для Windows 95

Разъемы часто на обратной стороне PC



# Пример устройства: e-token

Конструкция  
ITSEC Level 4

Крепление  
для  
кольца



Интерфейс USB 1.1

Внутренний LED  
для указания  
статуса  
устройства



# eToken – полнофункциональный аналог смарт карты

**eToken** выполняется в виде брелка, напрямую подключается к компьютеру через порт USB (Universal Serial Bus) и не требует наличия кард-ридера



**eToken** обладает уникальным серийным номером (ID) и имеет до 64 Кбайт защищенной энергонезависимой памяти

**eToken** поддерживает работу и интегрируется со всеми основными приложениями, использующими технологию PKI

## Назначение:

- строгая двухфакторная аутентификация пользователя при доступе к защищенным ресурсам;
- портативный контейнер для безопасного хранения ключей шифрования, цифровых сертификатов и другой конфиденциальной информации;
- использование в качестве электронного кошелька в системах ЭК.



# ИПК для входа в Windows 2000

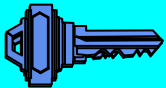


Интерактивный вход в систему с применением Active Directory, протокола Kerberos версии 5 и сертификата открытого ключа

# ИПК для входа в Windows 2000



Smart  
Card



PIN, который указывается пользователем в диалоговом окне при входе в систему, обеспечивает аутентификацию только по отношению к смарт-карте, но не к собственно домену

# Практическая работа

## Программирование смарт-карт (на примере eToken)



- **Настройка функции подачи заявок:**
  - **Настройка агента подачи заявок и станции подачи заявок**
  - **Установка рабочей среды eToken (RTE) на осуществляющем выпуск сертификатов компьютере.**

Подавать заявку на сертификат пользователя смарт-карты может только обладатель учетной записи с

сертификатом агента подачи заявок

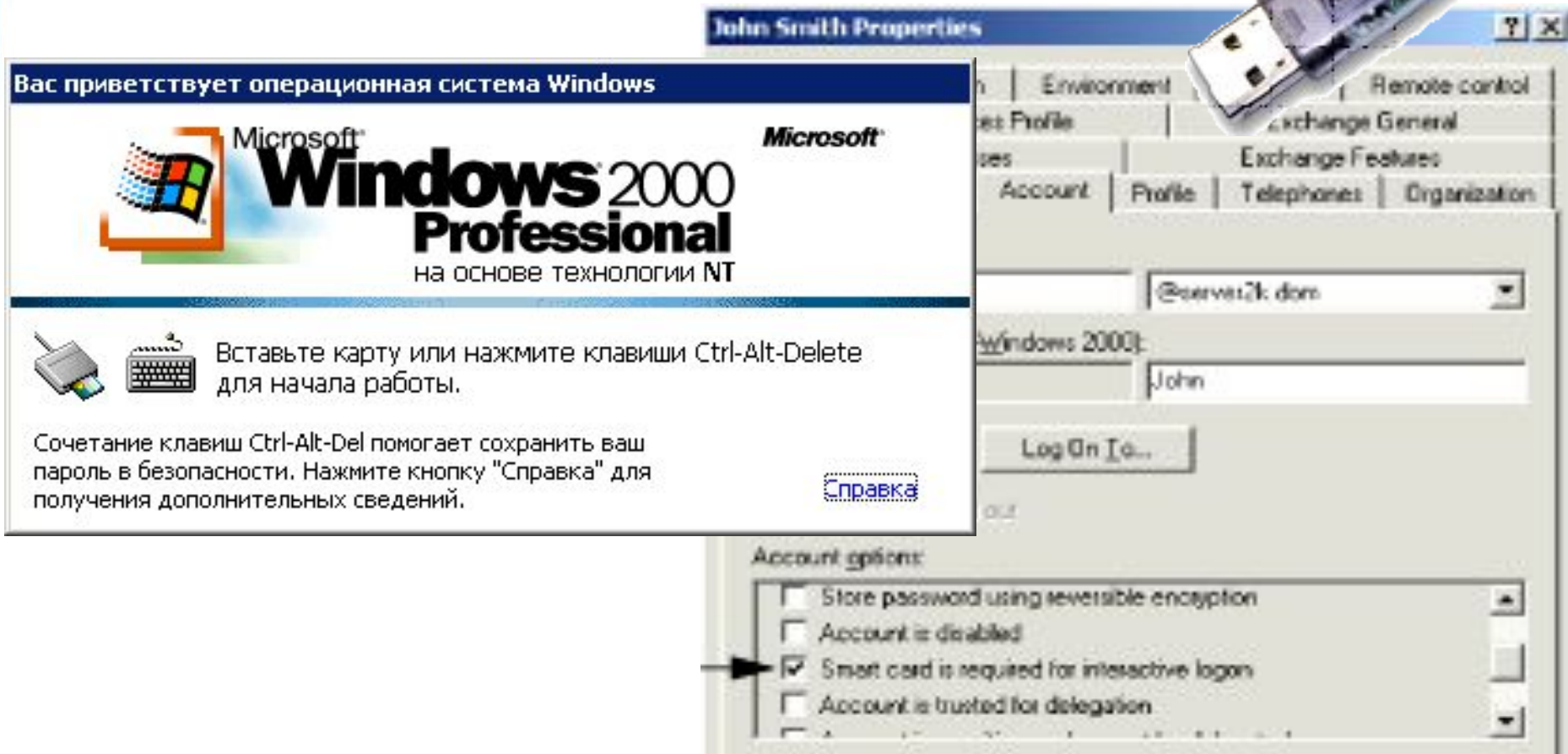
## Персонализация и администрирование eToken



# Практическая работа

Программирование смарт-карт (на примере eToken)

Определение настроек входа



The image shows a Windows 2000 Professional desktop environment. In the foreground, a blue USB smart card (eToken) is shown. The background features the Windows 2000 Professional logo and a login dialog box for 'John Smith Properties'. The login dialog includes fields for the user name 'John' and domain '@server2k.dcom', a 'Log On' button, and an 'Account options' section. The 'Account options' section contains several checkboxes: 'Store password using reversible encryption', 'Account is disabled', 'Smart card is required for interactive logon' (which is checked and highlighted by a black arrow), and 'Account is trusted for delegation'.

Вас приветствует операционная система Windows

Microsoft® **Windows 2000 Professional** на основе технологии NT

Вставьте карту или нажмите клавиши Ctrl-Alt-Delete для начала работы.

Сочетание клавиш Ctrl-Alt-Del помогает сохранить ваш пароль в безопасности. Нажмите кнопку "Справка" для получения дополнительных сведений.

John Smith Properties

Environment Remote control  
es Profile Exchange General  
ses Exchange Features  
Account Profile Telephones Organization

@server2k.dcom

Windows 2000:  
John

Log On [o...]

Account options:

- Store password using reversible encryption
- Account is disabled
- Smart card is required for interactive logon
- Account is trusted for delegation