

Использование eToken

<http://www.Aladdin.ru>

Средства аутентификации

Дискета

Touch Memory (iButton)

Магнитная карта

Скретч-карта

Смарт-карта

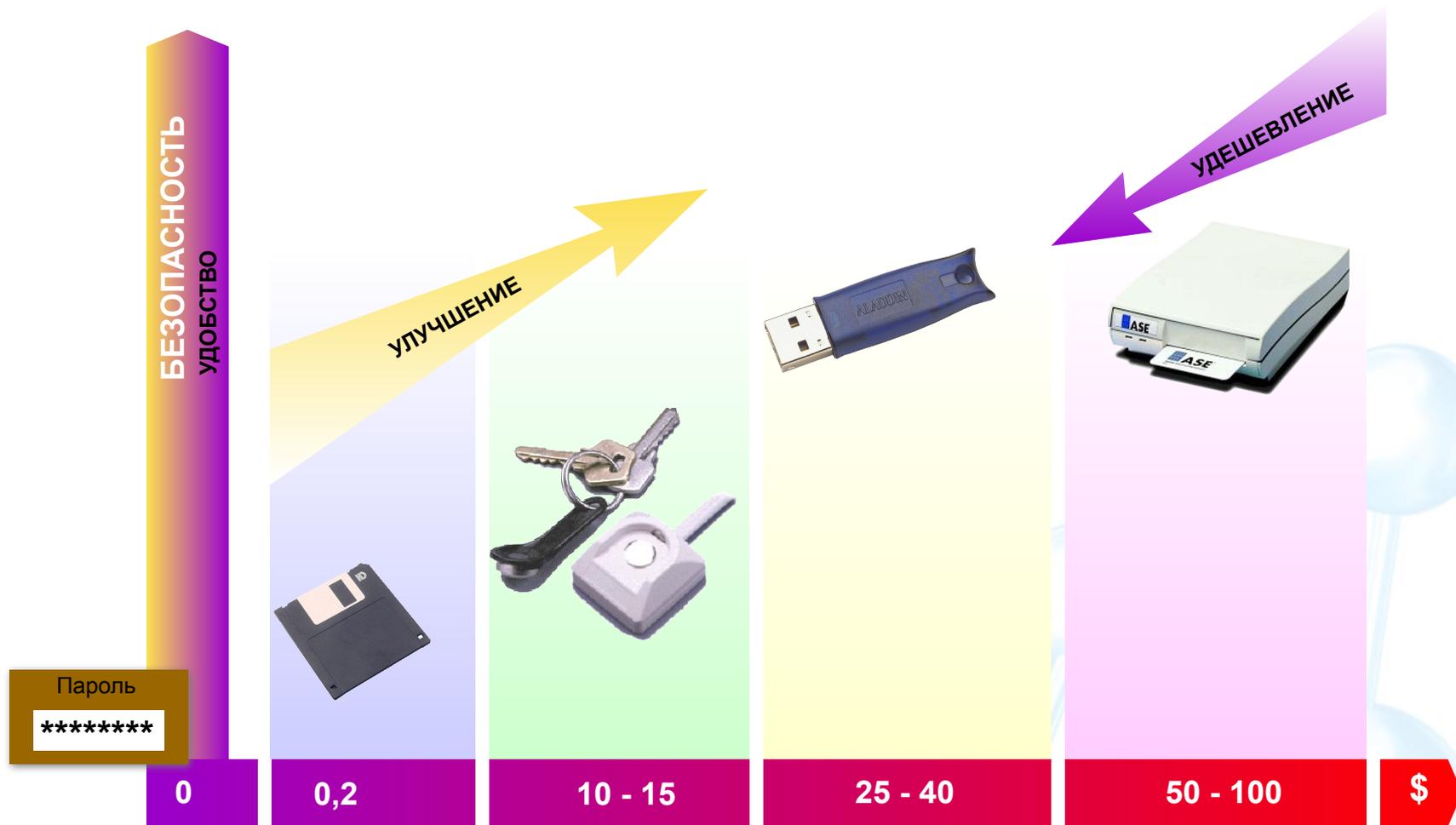
USB-токен

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?



аппаратное средство для
аутентификации и безопасного
хранения ключевой информации

Брелок для
USB-порта

=



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:

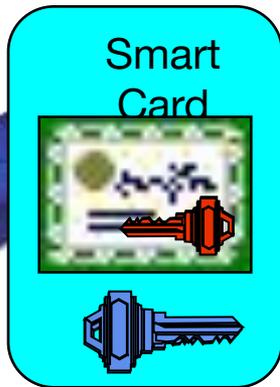
- строгая двухфакторная аутентификация пользователя при доступе к защищенным ресурсам;
- портативный контейнер для безопасного хранения ключей шифрования, цифровых сертификатов и другой конфиденциальной информации;
- использование в качестве электронного кошелька в системах ЭК.

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



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 login screen with a 'John Smith Properties' dialog box open. The dialog box has tabs for 'Environment', 'Remote control', 'Exchange General', 'Exchange Features', 'Account', 'Profile', 'Telephones', and 'Organization'. The 'Account' tab is selected, showing a dropdown menu with '@server2k.doms', a text field with 'John', and a 'Log On I...' button. Below this, the 'Account options' section has several checkboxes: 'Store password using reversible encryption', 'Account is disabled', 'Smart card is required for interactive logon' (checked), and 'Account is trusted for delegation'. A mouse cursor points to the 'Smart card is required for interactive logon' checkbox. In the background, a Windows 2000 Professional splash screen is visible with the text 'Вас приветствует операционная система Windows' and 'Microsoft Windows 2000 Professional на основе технологии NT'. Below the logo, it says 'Вставьте карту или нажмите клавиши Ctrl-Alt-Delete для начала работы.' and 'Сочетание клавиш Ctrl-Alt-Del помогает сохранить ваш пароль в безопасности. Нажмите кнопку "Справка" для получения дополнительных сведений.' with a 'Справка' button.