

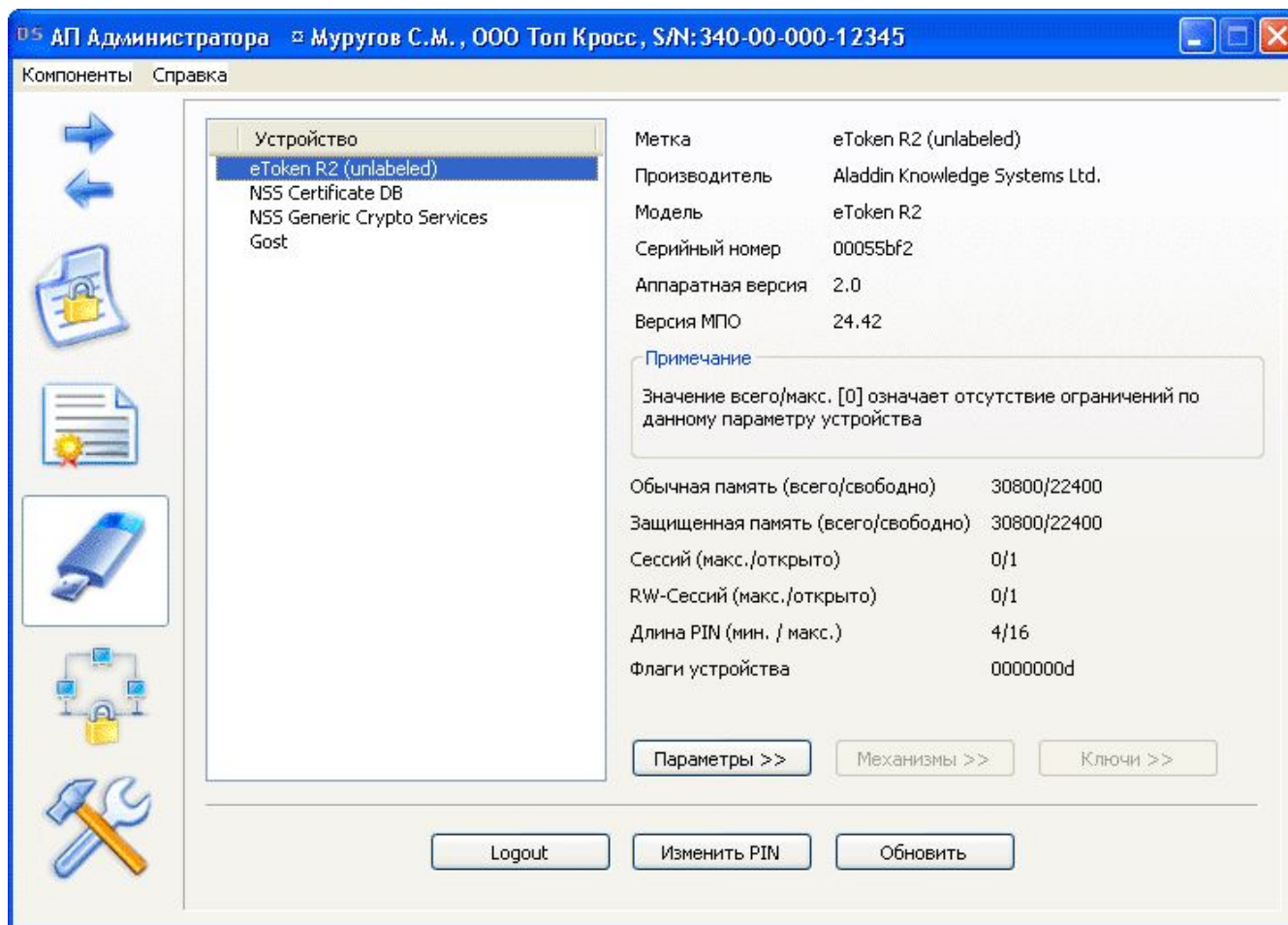
Прикладные аспекты использования идентификаторов семейства eToken

Аппаратные PKCS#11-устройства семейства eToken являются универсальным инструментом очень широкого диапазона применения.

Хорошей иллюстрацией являются варианты применения eToken в продуктах компании «Топ Кросс»:

- eToken используется в качестве криптографического токена на стороне клиентского ПО на технологии PKI и выступает инструментом для генерации ключевого материала, выработки и проверки ЭЦП и .т.п. для зарубежных криптографических алгоритмов.
- eToken используется в качестве хранилища ключей и сертификатов сформированных для отечественных криптографических алгоритмов.
- eToken – фундамент технологии HT (Hardware Token Only), обеспечивающей контроль целостности программной инфраструктуры клиента.

eToken – криптографическое устройство



Генерация ключевого материала

The image shows two overlapping windows from a Windows operating system. The background window is the 'Мастер управления сертификатами' (Certificate Management Wizard) in the 'Алгоритм ключевой пары' (Key Pair Algorithm) step. It shows 'eToken R2 (unlabeled)' selected for the PKCS#11 device and 'rsaEncryption' for the key algorithm. The foreground window is the 'AP Администратора' (Certificate Administrator) console, displaying a list of certificates. The selected certificate is 'CN=TEST' with the device 'eToken R2 (unlabeled)'. Below the list, the 'Краткая информация:' (Summary) section shows details for the selected certificate.

Мастер управления сертификатами

Алгоритм ключевой пары
Выберите алгоритм, параметры, и устройство сертификата

PKCS#11-устройство для локальной генерации ключа: eToken R2 (unlabeled)

Алгоритмы ключа сертификата: rsaEncryption

Параметры алгоритма
Данный алгоритм не предусматривает возможных параметров

Запретить экспорт сформированного приватного ключа

< Назад

AP Администратора

Компоненты Справка

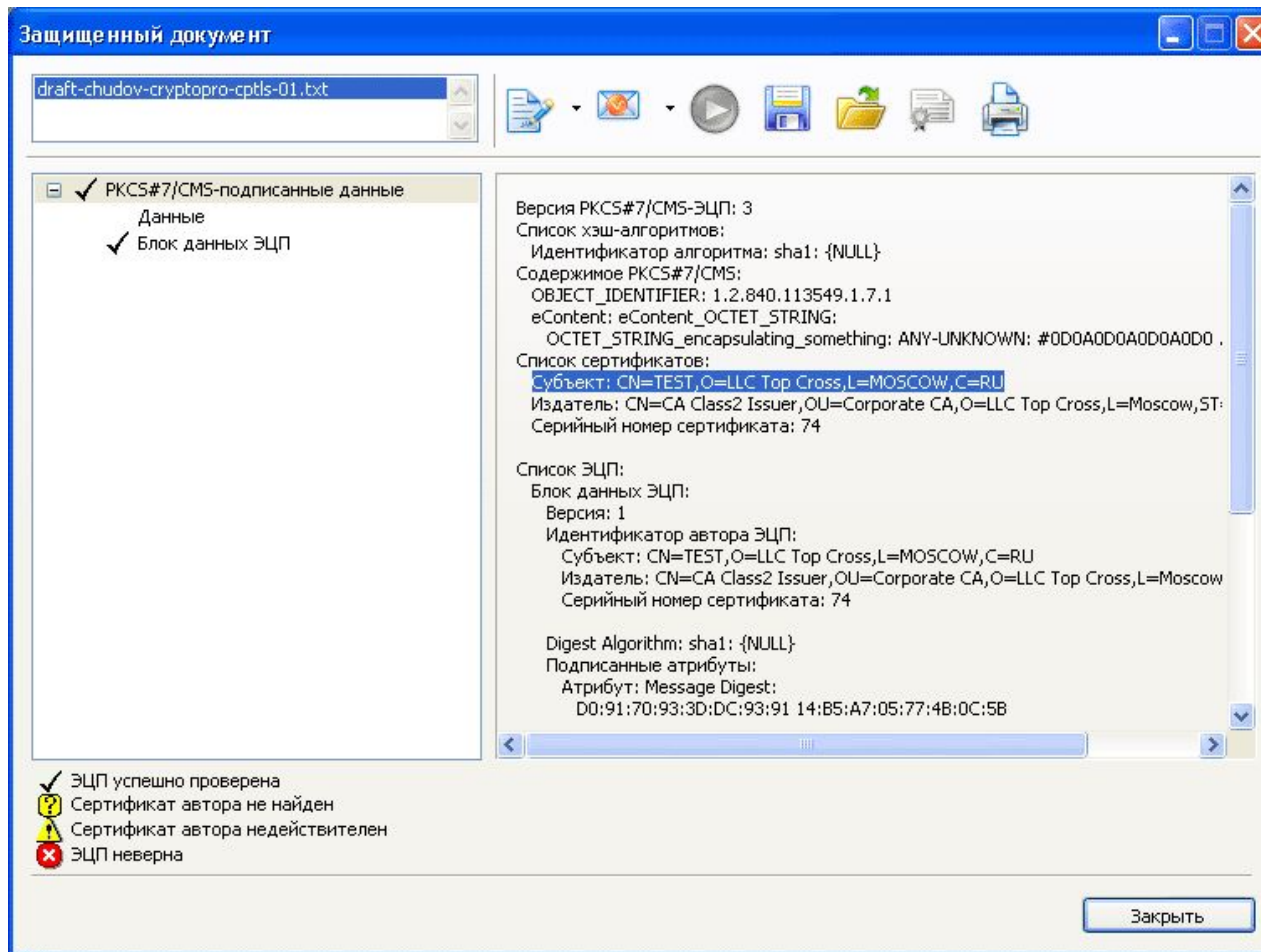
Персональные Другие пользователи Промежуточные издатели Доверенные издатели Отозванные

Понятное имя	Устройство
CN=TEST	eToken R2 (unlabeled)
CN=CLN TEST -RSA-	NSS Certificate DB
CN=FEODOR N. KRASHENINNIKOV	NSS Certificate DB
Imported Certificate	NSS Certificate DB
CN=(UPDATE) SERGEY M. MURUGOV	NSS Certificate DB
CN=msm1-1	Gost
CN=user1	Gost
CN=CLN P10 -DS-	Gost
CN=АДМИНИСТРАТОР ТК-УЦ	Gost
CN=(G) SERGEY M. MURUGOV	Gost
CN=TEST FROM TEST	Gost

Краткая информация:

Субъект: CN=TEST,O=LLC Top Cross,L=MOSCOW,C=RU
Издатель: CN=CA Class2 Issuer,OU=Corporate CA,O=LLC Top Cross,L=Moscow,ST=MSK,C=RU
Серийный номер: 74
Период действия:
Начало: 22.06.2006 09:29:59
Окончание: 22.06.2007 09:29:59
Алгоритмы ключевой пары: rsaEncryption

Выработка и проверка ЭЦП

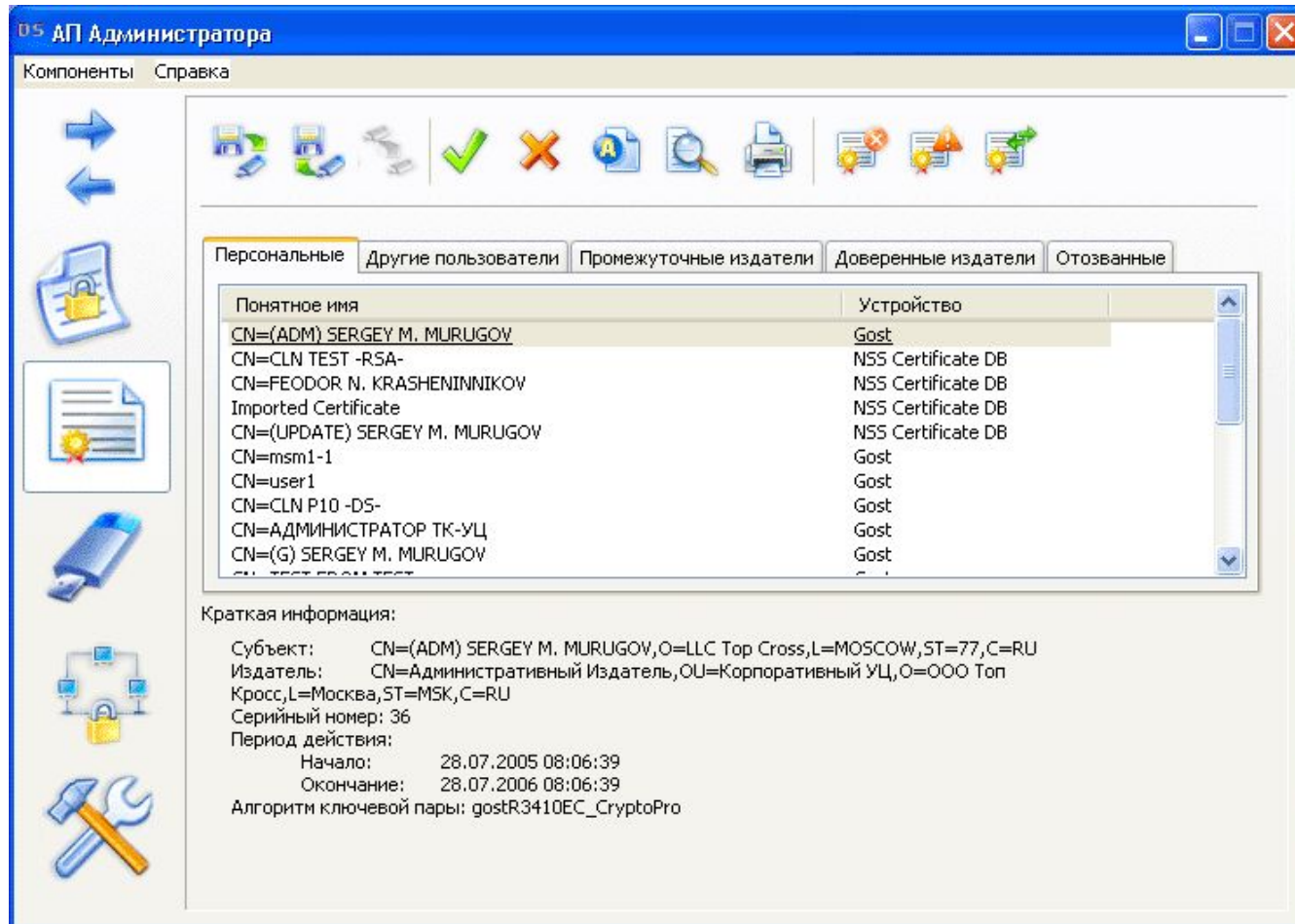


еToken-хранилище ключей и сертификатов для отечественных криптоалгоритмов

The screenshot displays the 'АП Администратора' (AP Administrator) software interface. In the background, a table lists certificates with columns for 'Понятное имя' (Friendly name) and 'Устройство' (Device). The table contains entries for 'CN=CLN TEST -RSA-' and 'CN=FEODOR N. KRASHENINNIKOV'. Overlaid on the interface are two dialog boxes. The foreground dialog, titled 'Контейнер PKCS#12', contains a question mark icon and the text 'В устройстве найден PKCS#12 контейнер.' (A PKCS#12 container found in the device). It has three buttons: 'Загрузить' (Load), 'Пропустить' (Skip), and 'Удалить' (Delete). Below the buttons is a 'Примечание:' (Note) section with text: 'Сертификаты и ключи будут загружены временно - до извлечения устройства. Для постоянной загрузки воспользуйтесь штатной процедурой импорта сертификатов.' (Certificates and keys will be loaded temporarily - until device removal. For permanent loading, use the standard certificate import procedure). The background dialog, titled 'Авторизация в PKCS#11-устройстве' (Authorization in PKCS#11 device), shows an eToken R2 device icon and details: 'eToken R2 (unlabeled)', 'eToken R2', 'Aladdin Knowledge Systems Ltd.', and '00055bf2'. It includes an unchecked 'Администратор' (Administrator) checkbox, a 'Введите PIN:' (Enter PIN) field with masked characters, and 'OK', 'Пропустить' (Skip), and 'Пропустить все' (Skip all) buttons.

Технология: размещение в защищенном хранилище eToken сертификатов и ключей отечественных алгоритмов выполнено в виде контейнера формата PKCS#12, сохраняемого как объект класса SKO_DATA с атрибутом SKA_APPLICATION = "PKCS#12"

Сессионное размещение ключей и сертификатов в программном хранилище



Почтовый агент («Буревестник») из проекта Mozilla

The screenshot displays a Mozilla-based email client interface. The main window is titled "Inbox - Mail/News" and features a menu bar (File, Edit, View, Go, Message, Tools, Help) and a toolbar with icons for Get Mail, Write, Address Book, Reply, Reply All, Forward, Delete, Junk, Print, and Stop. The left sidebar shows folders for "jim@top-cross.ru" (Inbox, Drafts, Sent, Trash, Junk, Нежелательная почта) and "Local Folders" (Inbox, Unsent, Drafts, Sent, Trash). The main pane shows a list of messages with columns for Subject, Sender, and Date. A message titled "Subject: Test S/MIME message [enciphered]" is selected, showing its details: From: Семенов М. О. <Maxim.Semenov@kami-sever.ru>, Date: 08.06.2006 17:04, To: kopylov@top-cross.ru. Below the message details, the beginning of the email body is visible, starting with "Приветствую, Ден..." and "Это зашифрован...".

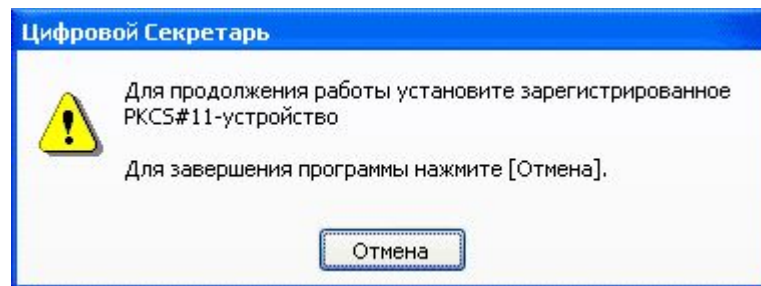
Overlaid on the bottom right is the "Device Manager" window, showing the "Security Modules and Devices" section. The "FSS" module is expanded, showing a "SUPER" device. The "Details" pane for the "SUPER" device shows the following information:

Details	Value
Status	Logged In
Description	GOST-Rus PKCS#11 software token
Manufacturer	CryptoEx Ltd., Top Cross LLC.
HW Version	0.0
FW Version	1.9
Label	SUPER
Manufacturer	CryptoEx Ltd., Top Cross LLC.
Serial Number	#####
HW Version	0.0
FW Version	1.9

Buttons for "Log In", "Log Out", "Change Password", "Load", "Unload", and "Enable FIPS" are visible on the right side of the Device Manager window.

eToken – фундамент технологии HT (Hardware Token Only).

- Предпосылки: необходимость контроля целостности программной инфраструктуры клиента PKI-системы.
- Тезис: «Успешный» запуск прикладного ПО гарантирует «легитимность» самого ПО, его целостность и обеспечивает доступ к хранилищу с двухфакторной авторизацией.
- Технология: Контроль целостности основан на зашифрованном блоке данных, записываемом в хранилище PKCS#11-устройства в виде объекта класса SKO_DATA.



Задачи, возлагаемые на всю процедуру «связывания»:

- Авторизация. Проверочные данные в блоке лицензионной информации зависят от конкретного PKCS#11-устройства и драйверов этого устройства. Т.е. блок лицензионной информации позволяет выявить несоответствие лицензии и аппаратного PKCS#11-устройства.
- Подтверждение целостности. Проверочные данные в блоке лицензионной информации зависят от исполняемого файла приложения.
- Подтверждение авторства. Устанавливаемая связь «Приложение» ↔ «PKCS#11-устройство» не может быть воспроизведена никем помимо разработчика прикладного ПО.

ИСПОЛЬЗУЕМЫЕ РЕШЕНИЯ:



ООО «Топ Кросс», г. Москва.

E-mail: info@top-cross.ru

WWW: <http://www.top-cross.ru/>

Компоненты Удостоверяющего Центра сертификатов ключей подписи, компоненты службы «Электронного нотариата», клиентское программное обеспечение: «Цифровой секретарь» (DS), продукты проекта Mozilla.



ООО «КриптоЭкс», г. Москва

E-mail: info@cryptoex.ru

WWW: <http://www.cryptoex.ru/>

Сертифицированные средства криптографической защиты.

Генеральный директор
ООО «Топ Кросс»
Муругов Сергей Михайлович

Вопросы ?...