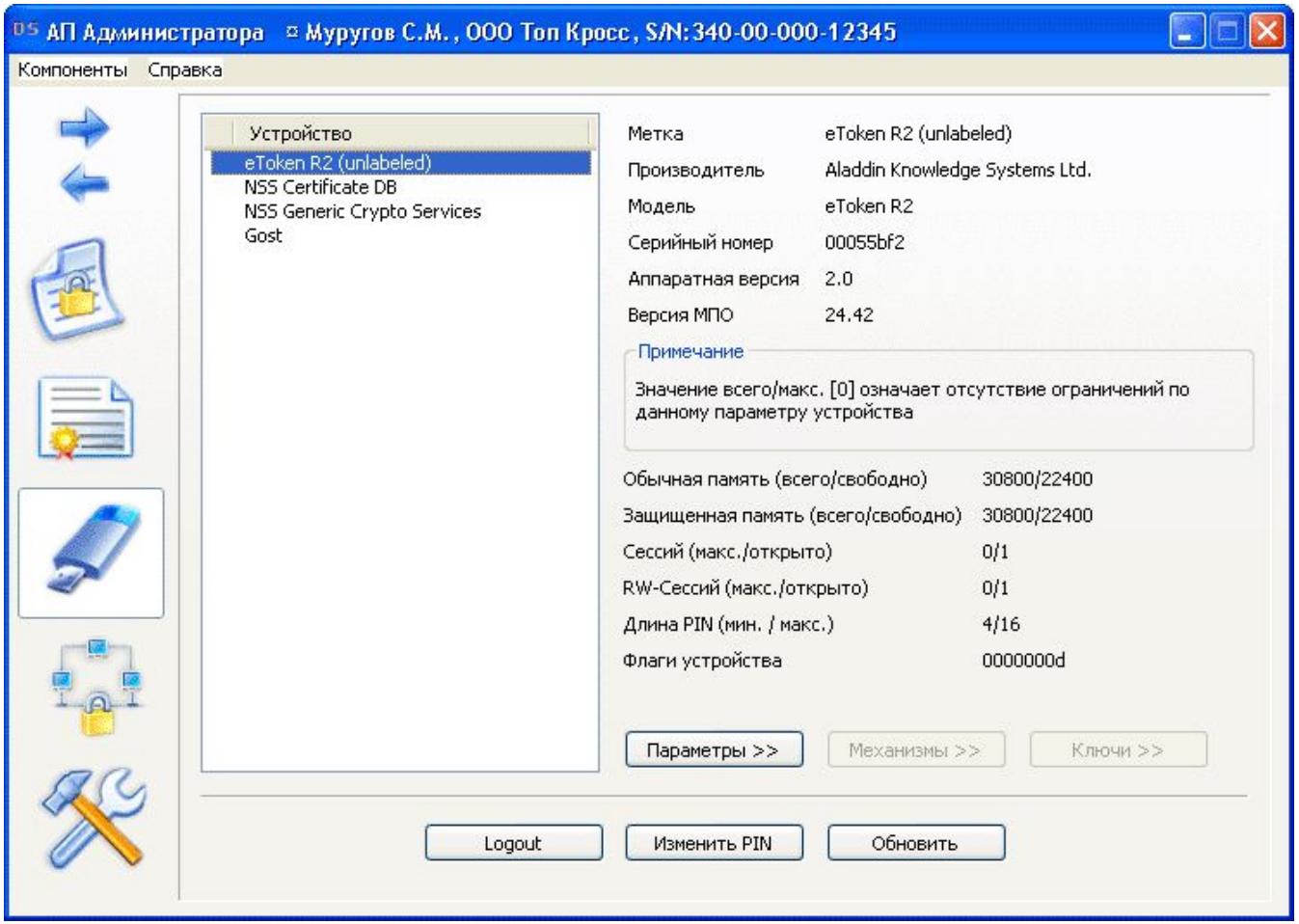
Прикладные аспекты использования идентификаторов семейства eToken

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

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

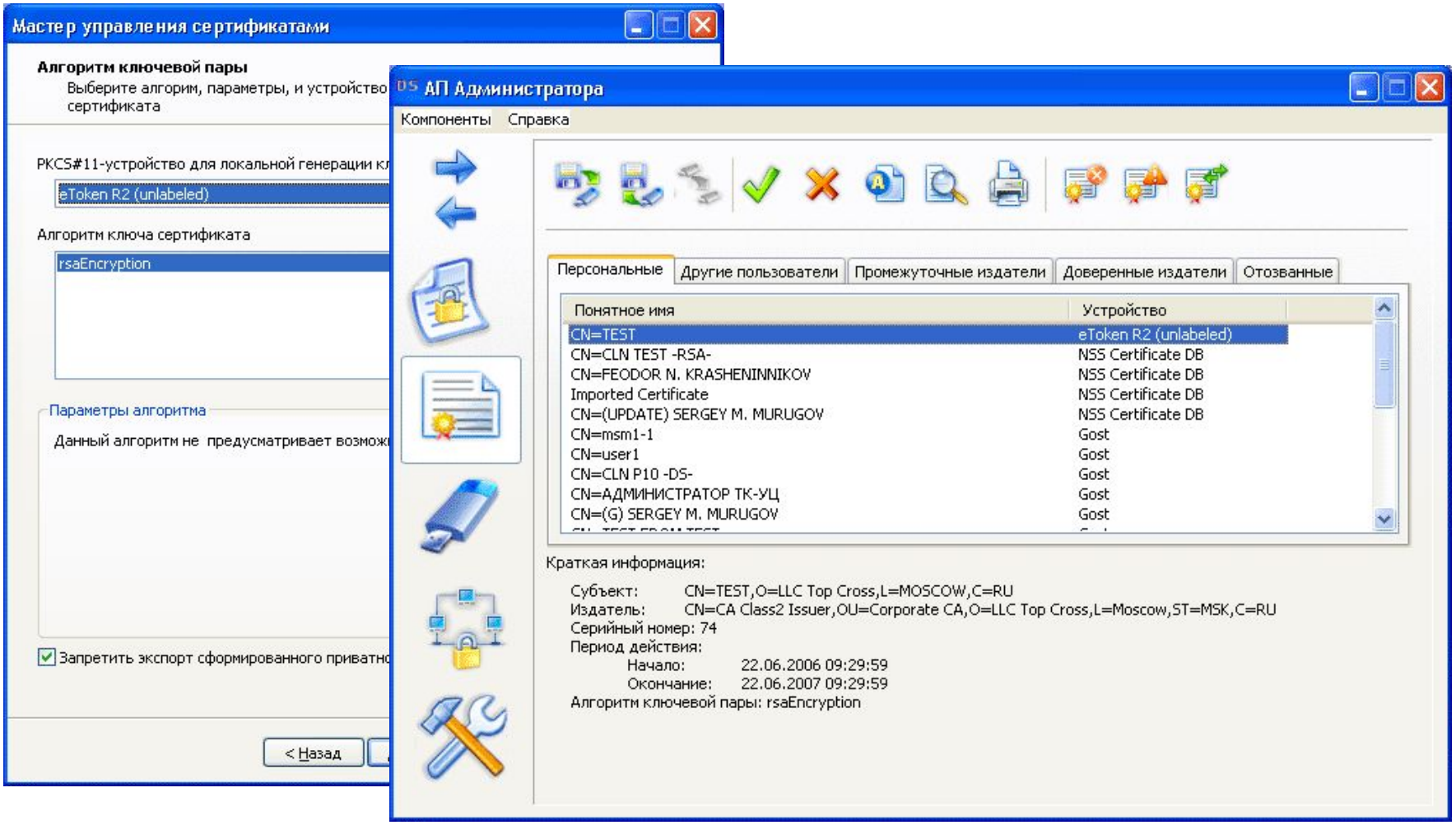
- eToken используется в качестве криптографического токена на стороне клиентского ПО на технологии PKI и выступает инструментом для генерации ключевого материала, выработки и проверки ЭЦП и .т.п. для зарубежных криптографических алгоритмов.
- eToken используется в качестве хранилища ключей и сертификатов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

eToken – криптографическое устройство



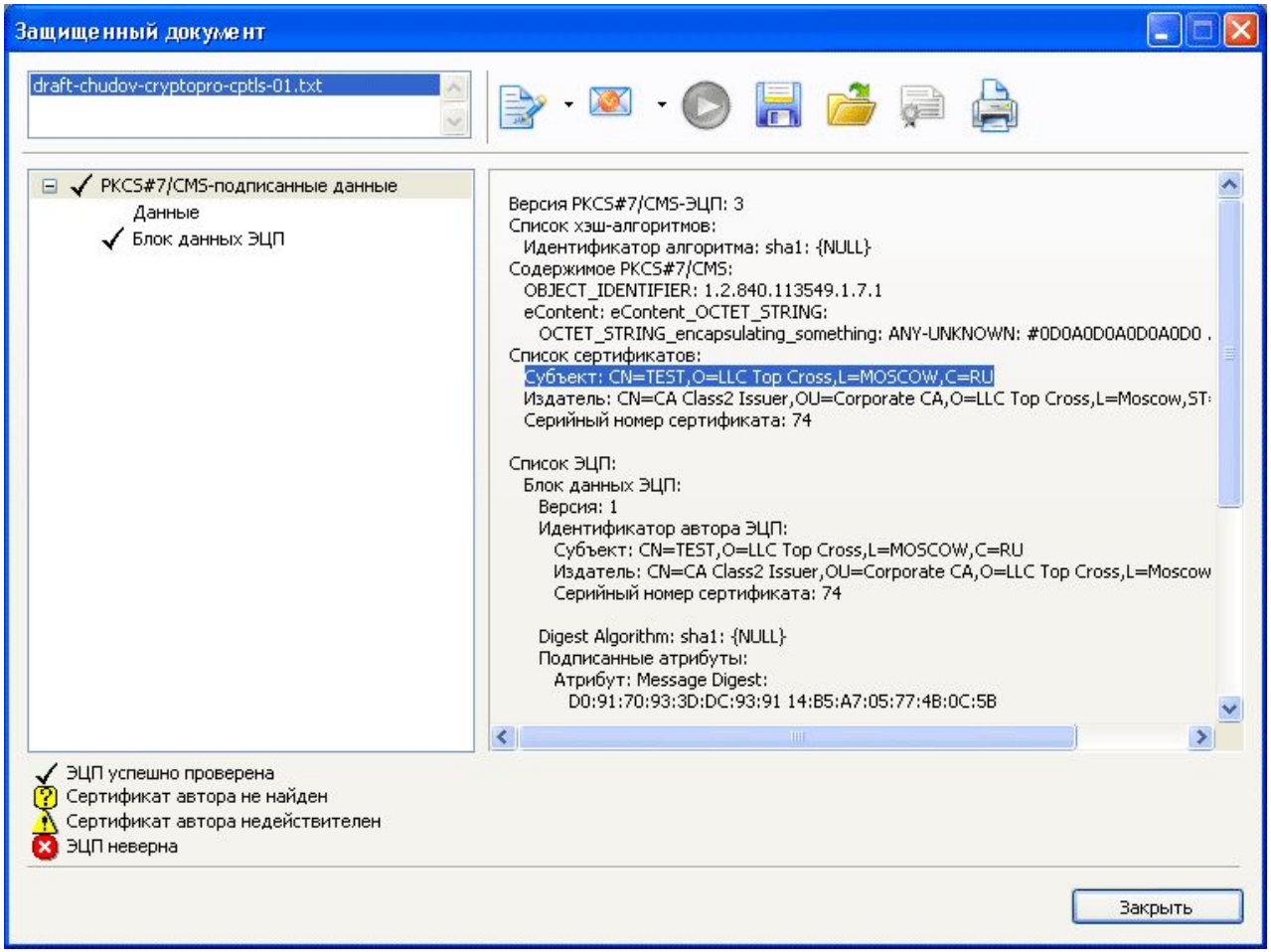
TOP CROSS

Генерация ключевого материала



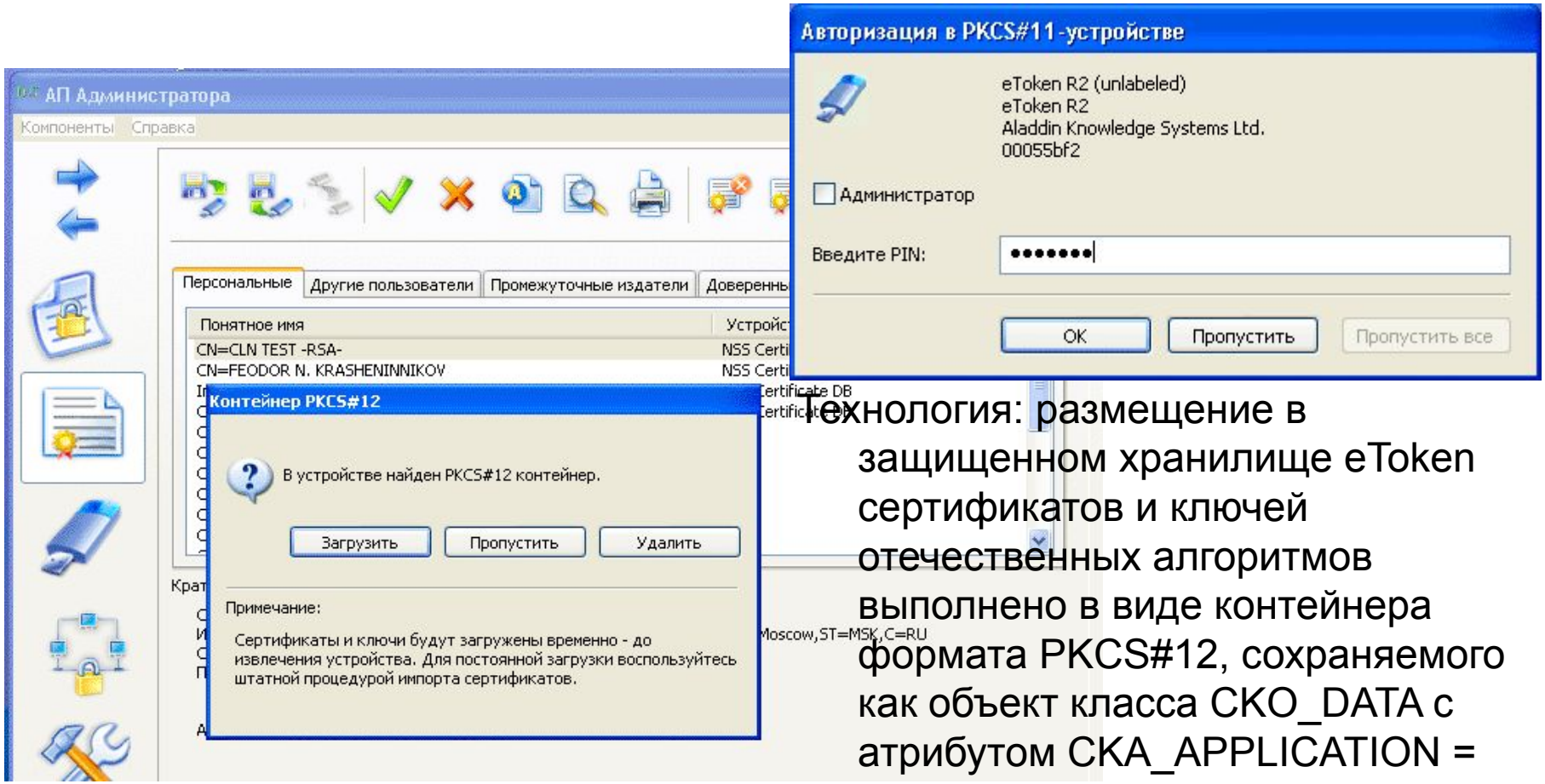
TOP CROSS

Выработка и проверка ЭЦП



TOP CROSS

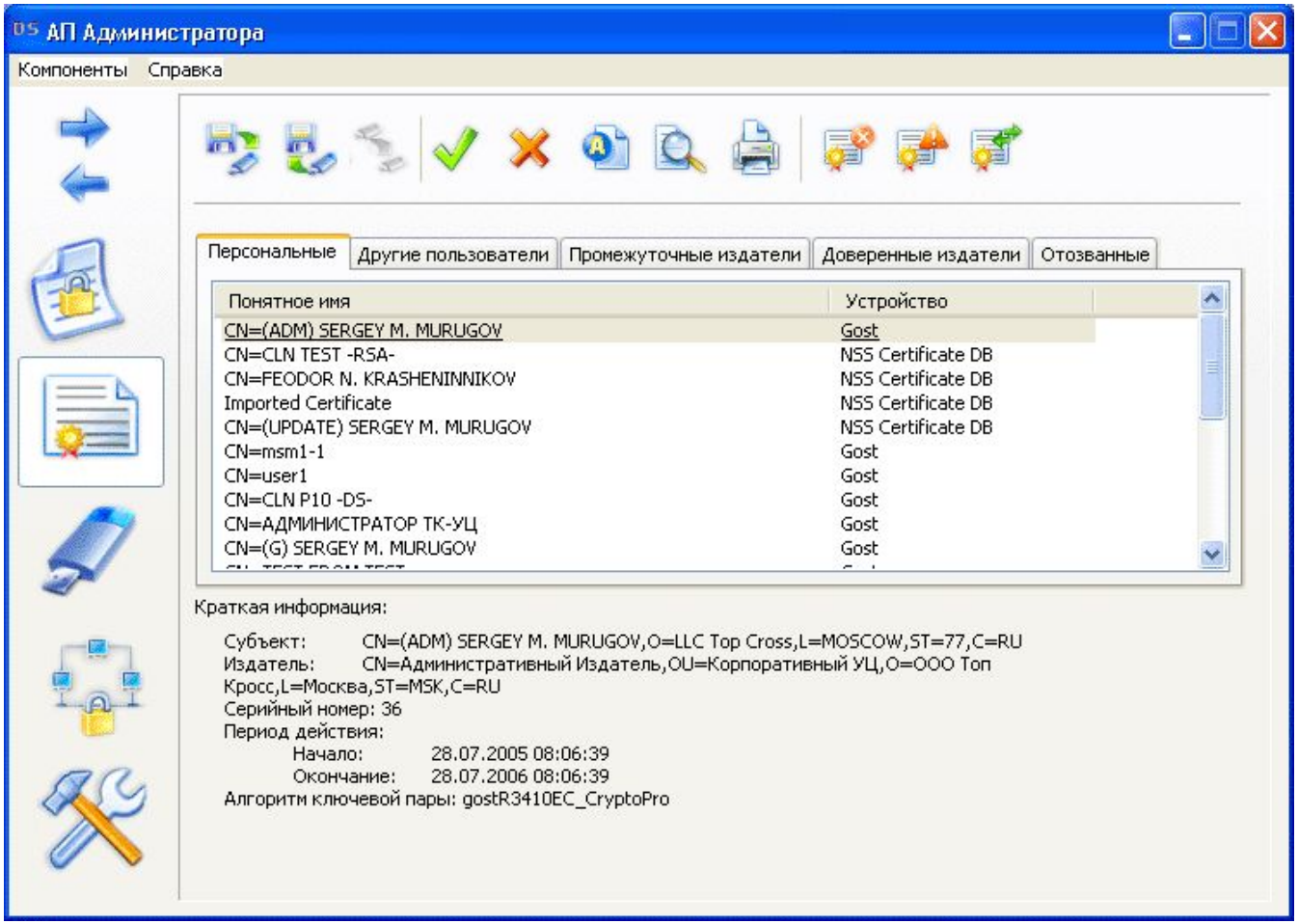
eToken-хранилище ключей и сертификатов для отечественных криптоалгоритмов



Технология: размещение в защищенном хранилище eToken сертификатов и ключей отечественных алгоритмов выполнено в виде контейнера формата PKCS#12, сохраняемого как объект класса CKO_DATA с атрибутом CKA_APPLICATION = “PKCS#12”

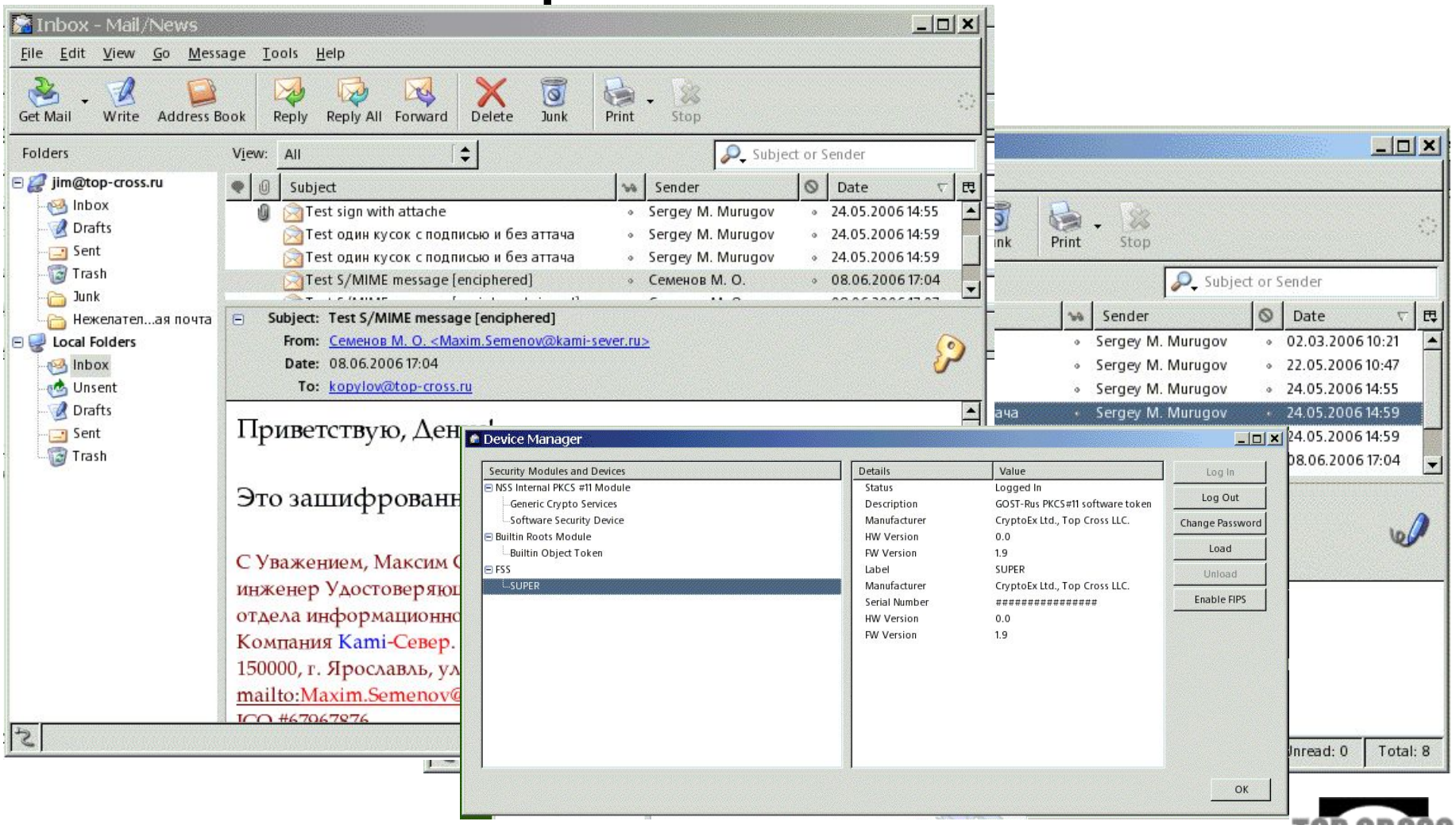
TOP CROSS

Сессионное размещение ключей и сертификатов в программном хранилище



TOP CROSS

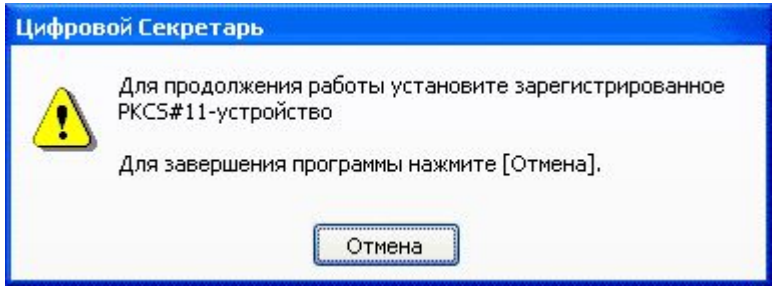
Почтовый агент («Буревестник») из проекта Mozilla



TOP CROSS

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 CKO_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.

КРИПТОЭКС

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 ?...