СКЗИ «Шифр-X.509»

Работа с защищенными документами в среде Microsoft Office 2010 и 2013

ООО «Сайфер БИС», к.т.н. Влад Ковтун

Содержание

- Предпосылки
- Возможности
- Архитектура
- Работа с почтой (Outlook)
- Работа с документами (Word, Excel, PowerPoint)
- Лицензирование

Предпосылки

- Большое количество документов
- Обмен документами
- Защита от НСД
- Удаленный доступ
- Мобильные сотрудники
- Юридическая значимость документов
- Сложная схема визирования документов

Актуальность

- **Защита** документов реальна тогда, когда она **проста и прозрачна**
- **Прозрачность** защиты документов достигается **глубокой интеграцией** средств защиты в приложения Microsoft Office

Общее описание

- Возможность защиты документов реализована виде расширений Microsoft Office (Add-in)
- Расширения представлены в виде отдельного дистрибутива, для каждого компонента (Outlook, Word, Excel, PowerPoint) Microsoft Office 2010 & 2013 (x86)

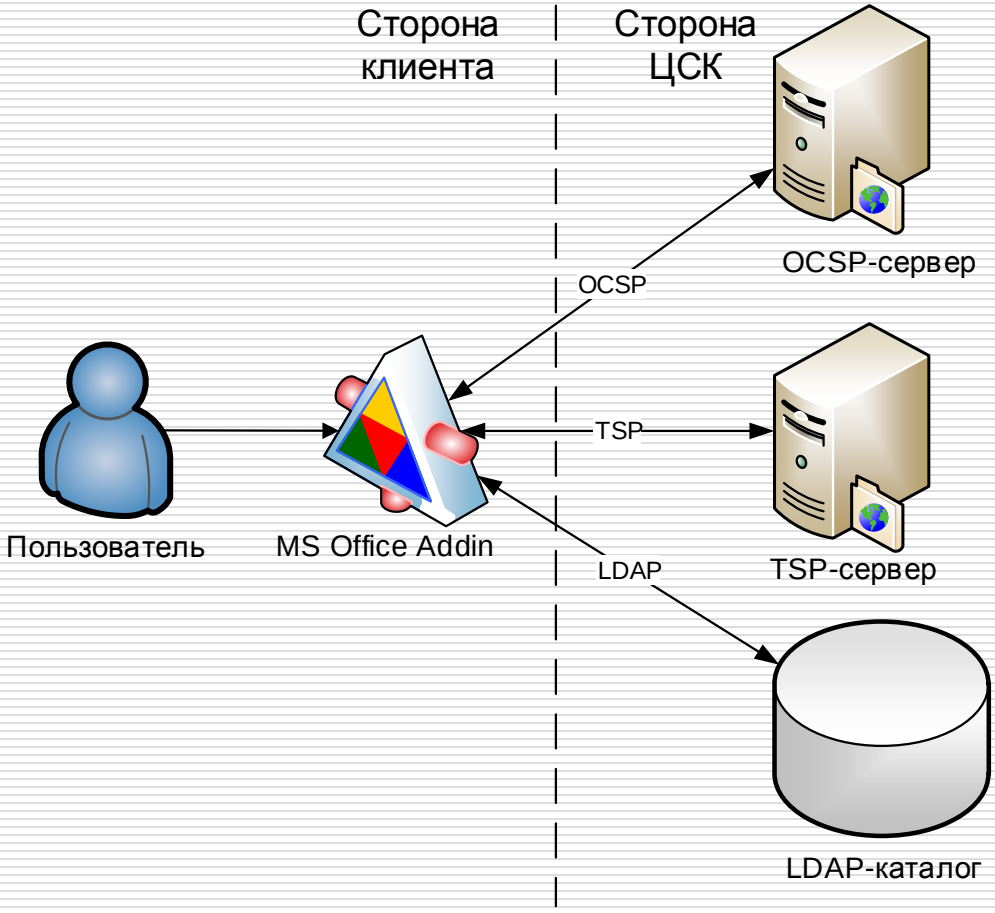
Общее описание

- Используются криптографические библиотеки СКЗИ «Шифр-X.509» для Win32
- Установка поддерживает одновременно две разные версии компонентов Microsoft Office 2010 & 2013

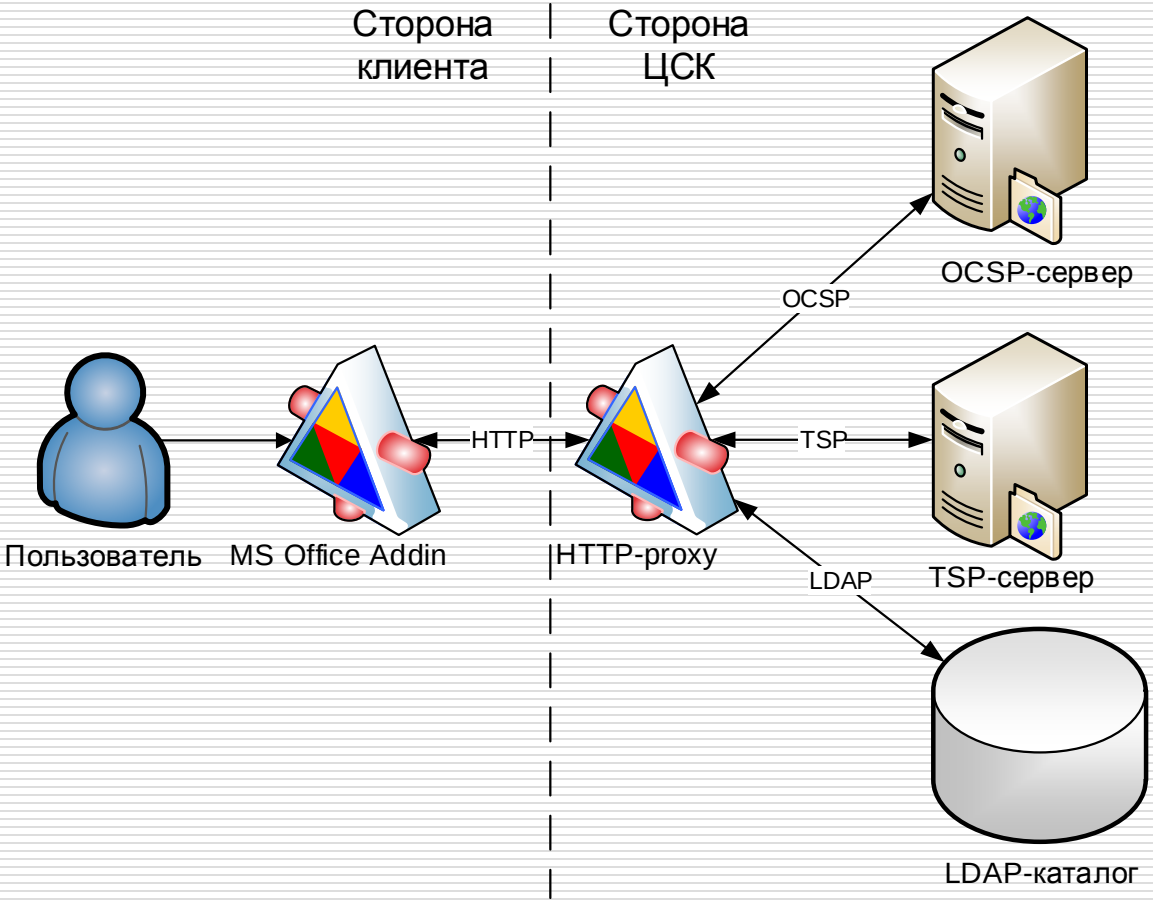
Общее описание

- Взаимодействуют с ЦСК СКЗИ «Шифр-X.509» по протоколам:
  - HTTP
  - OCSP, TSP, LDAP

Взаимодействие с ЦСК (1)



Взаимодействие с ЦСК (2)



Общее описание

- Поддерживают ключевые носители:
  - Файловые
  - Защищенные USB-токены и смарт карты

Поддерживаются носители

- Author 337 Series (USB Token, SmartCard)
- SafeNet eToken (USB Token)
- Giesecke & Devrient StarSign (USB Token, SmartCard)
- Gemalto IDPrime Series (SmartCard)
- Microcrypt Armorino (USB Token)
- Avest-UA (USB Token)
- eAladdin 72k Java (USB Token), JaCarta (USB Token, SmartCard)
- UAToken (USB Token)

Возможности

- Cipher Add-in Microsoft Outlook:
  - Шифрование
  - ЭЦП
  - Метки времени
- Cipher Add-in Microsoft Word, Excel, PowerPoint:
  - ЭЦП (иерархия, удостоверение множества подписей)
  - Метки времени

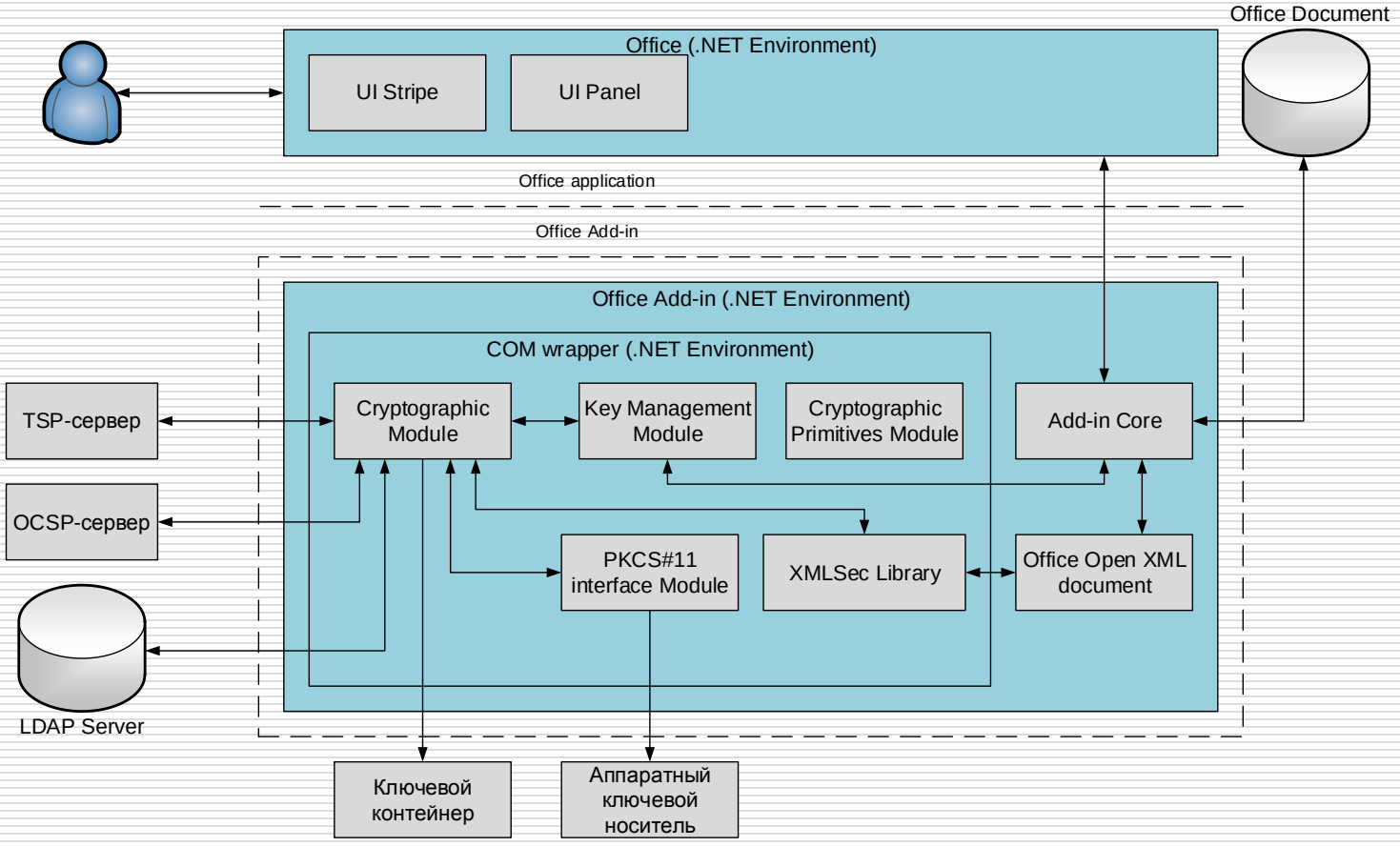
Компоненты

- Microsoft Office 2010
  - Outlook (ЭЦП+МВ+шифрование)
  - Word (иерархия ЭЦП+МВ)
  - Excel (иерархия ЭЦП+МВ)
  - PowerPoint (иерархия ЭЦП+МВ)

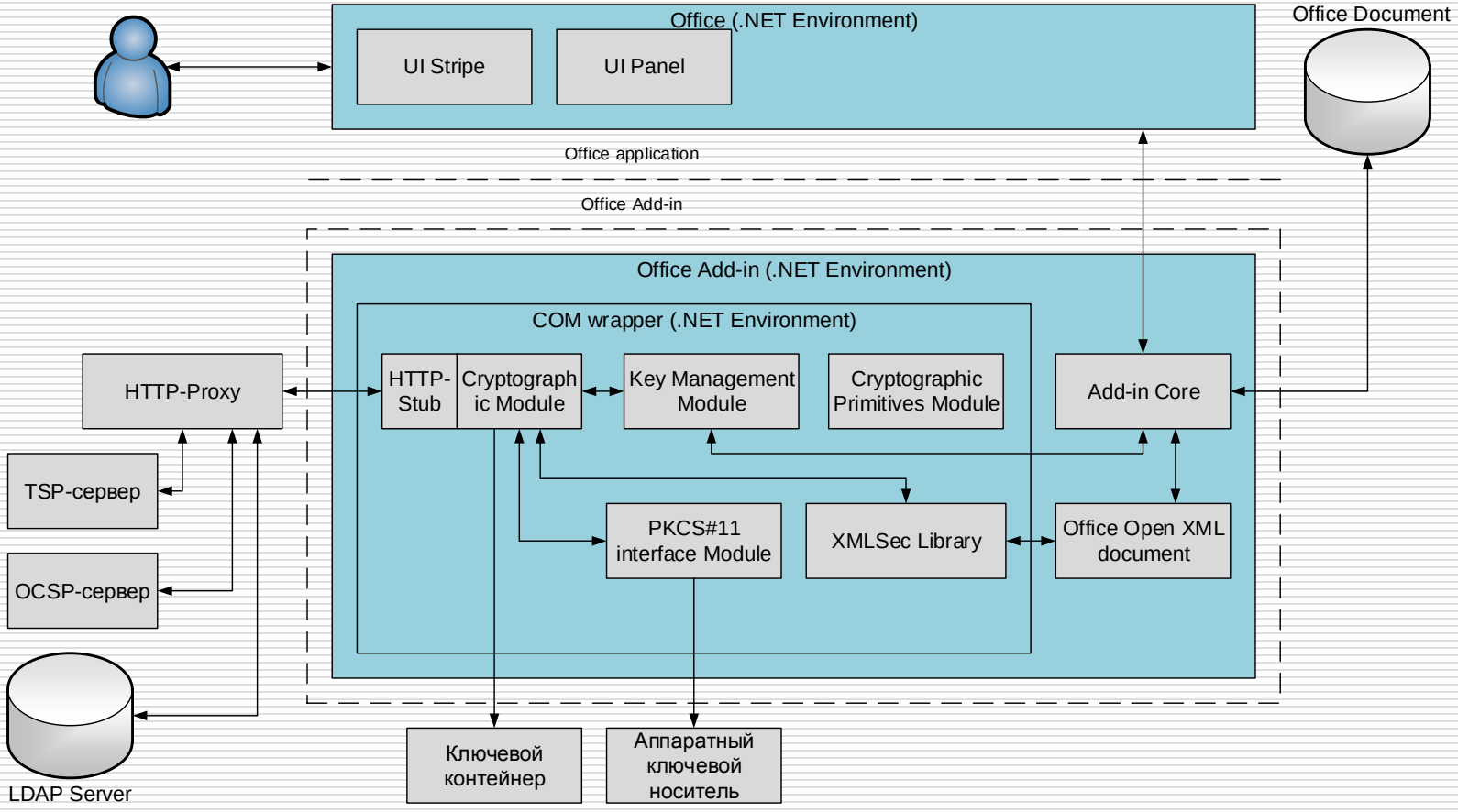
Компоненты

- Microsoft Office 2013
  - Outlook (ЭЦП+МВ+шифрование)
  - Word (иерархия ЭЦП+МВ)
  - Excel (иерархия ЭЦП+МВ)
  - PowerPoint (иерархия ЭЦП+МВ)

Архитектура



Архитектура



Пользовательская информация

- ЭЦП и МВ хранятся внутри документа в разделе <Sections> в формате XML
- Благодаря разделу <Sections> существует возможность интеграции с другими системами

Расширение для Microsoft Outlook 2010 & 2013

CIPHER OUTLOOK CRYPTO ADD-IN

Услуги

- Целостность и аутентичность
- Причастность
- Конфиденциальность
- Простота и прозрачность

Функции

- ЭЦП
- Шифрование* (тело, заголовок, отдельно каждое вложение)
- Метка времени
- Различные комбинации:
  - ЭЦП+МВ, ЭЦП+Ш, ЭЦП+МВ+Ш
  - Ш+МВ
  - Ш
  - МВ

*-перед зашифровыванием данные сжимаются с помощью ZIP

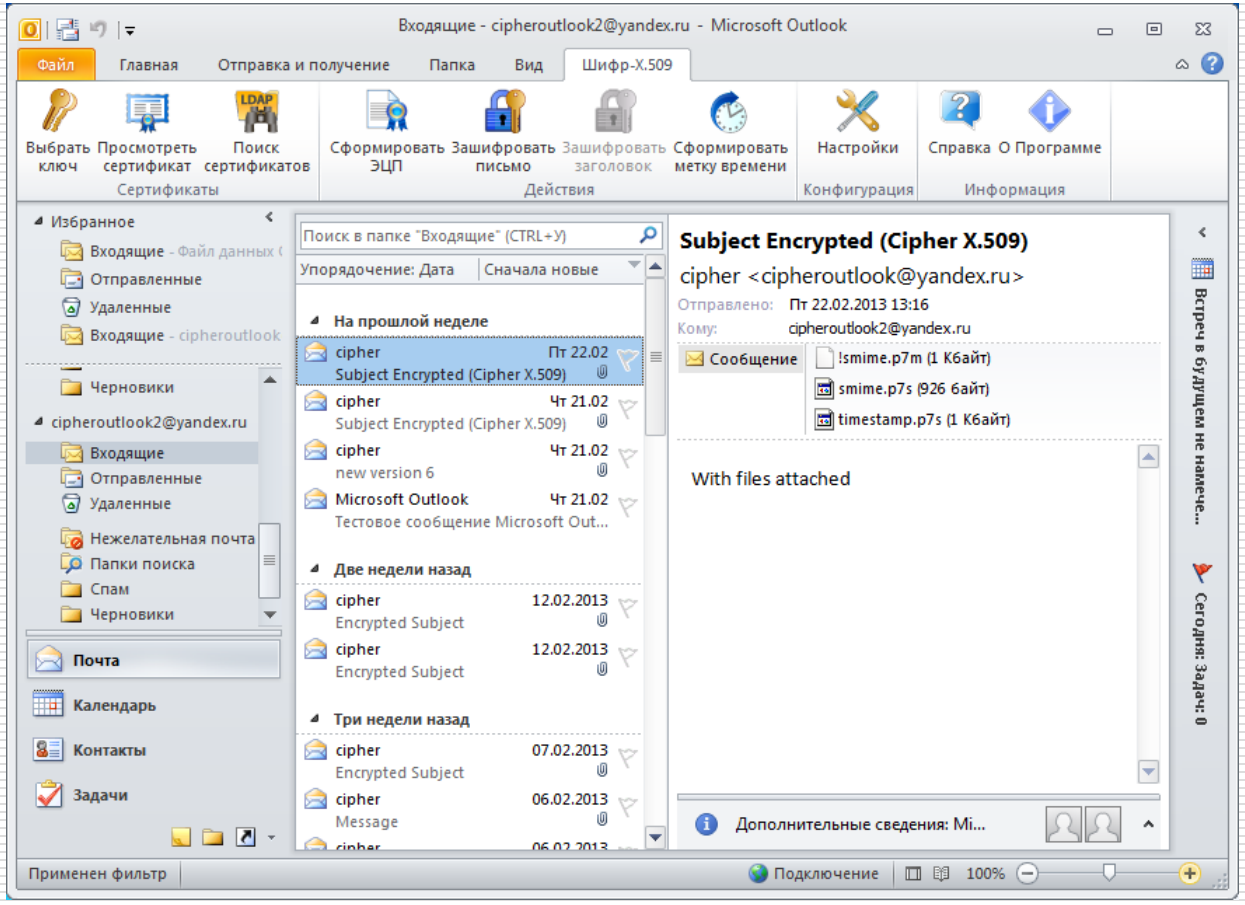
Функции

- Поиск сертификата в LDAP
- Просмотр своего сертификата
- Выбор другого ключа
- Проверка сроков действия ключей
- Работа с ключевым контейнером:
  - Файл
  - Защищенный носитель PKCS#11

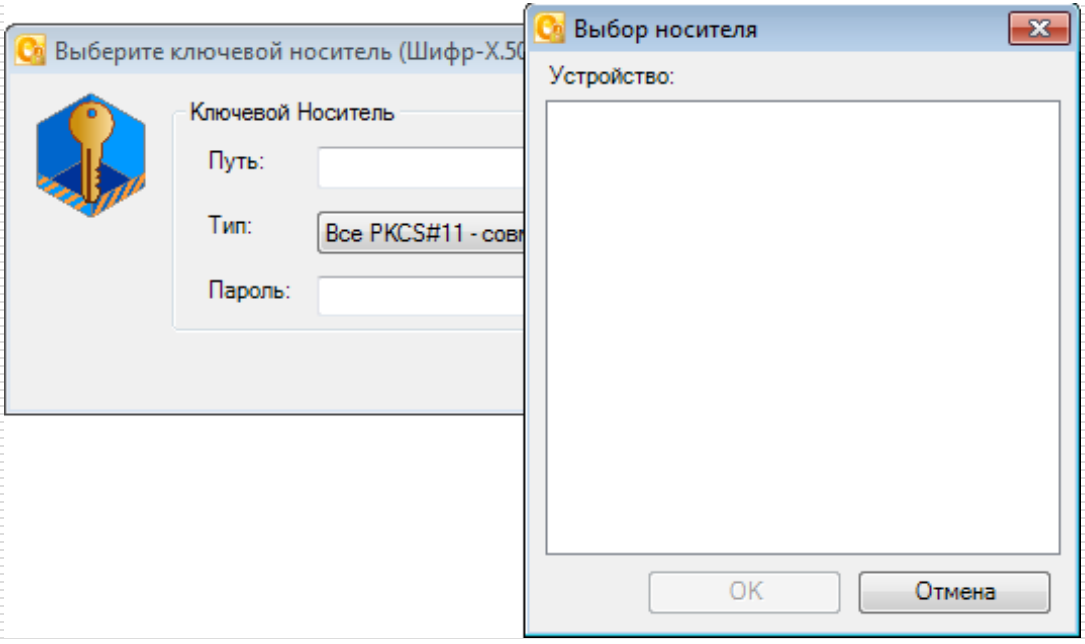
Функции

- Работа с почтовым сервером:
  - SMTP
  - POP3/IMAP
- Работа с серверами ЦСК (OCSP, TSP, LDAP):
  - Протоколы OCSP, TSP, LDAP
  - Проксирование через HTTP

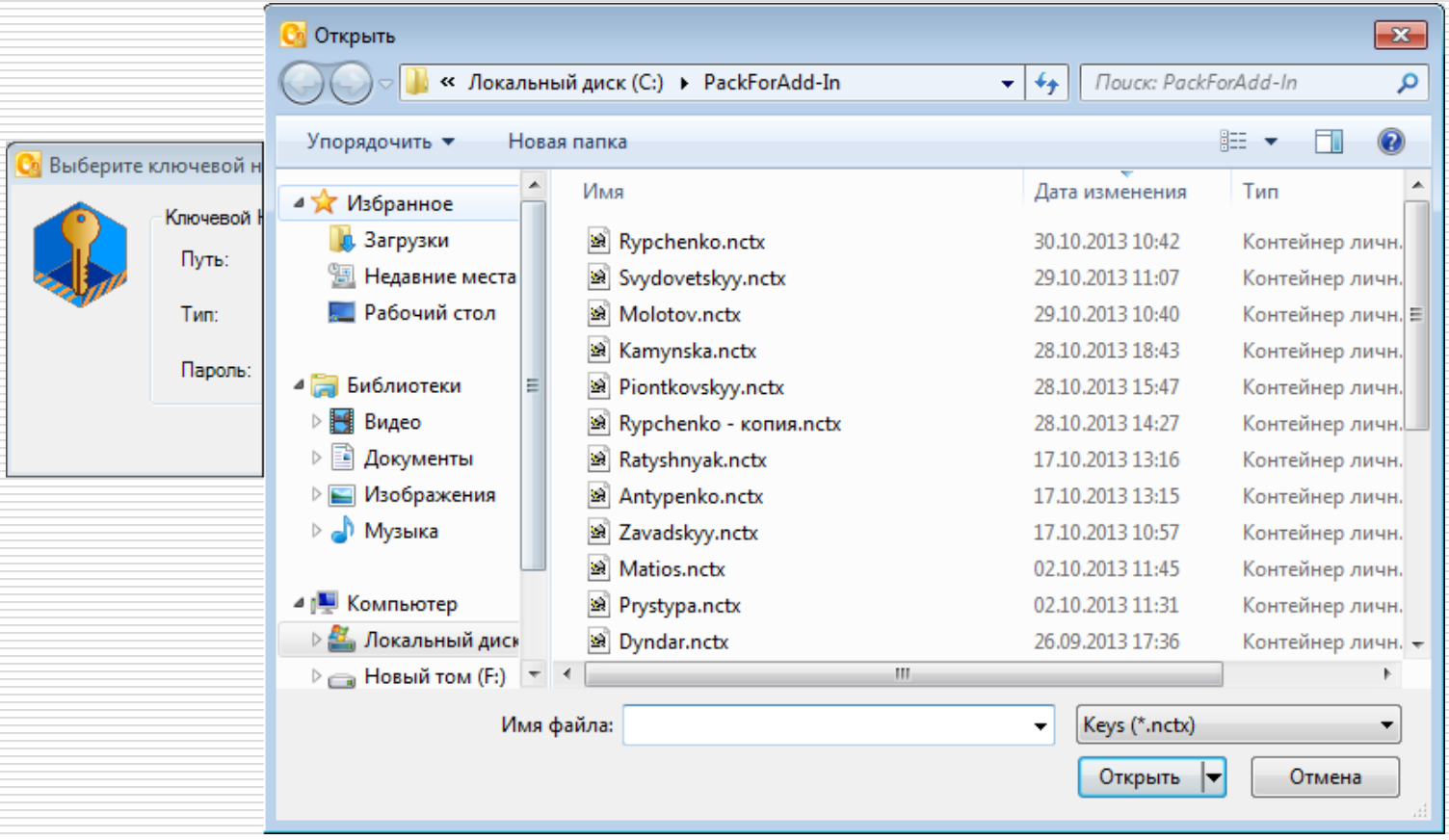
Пользовательский интерфейс



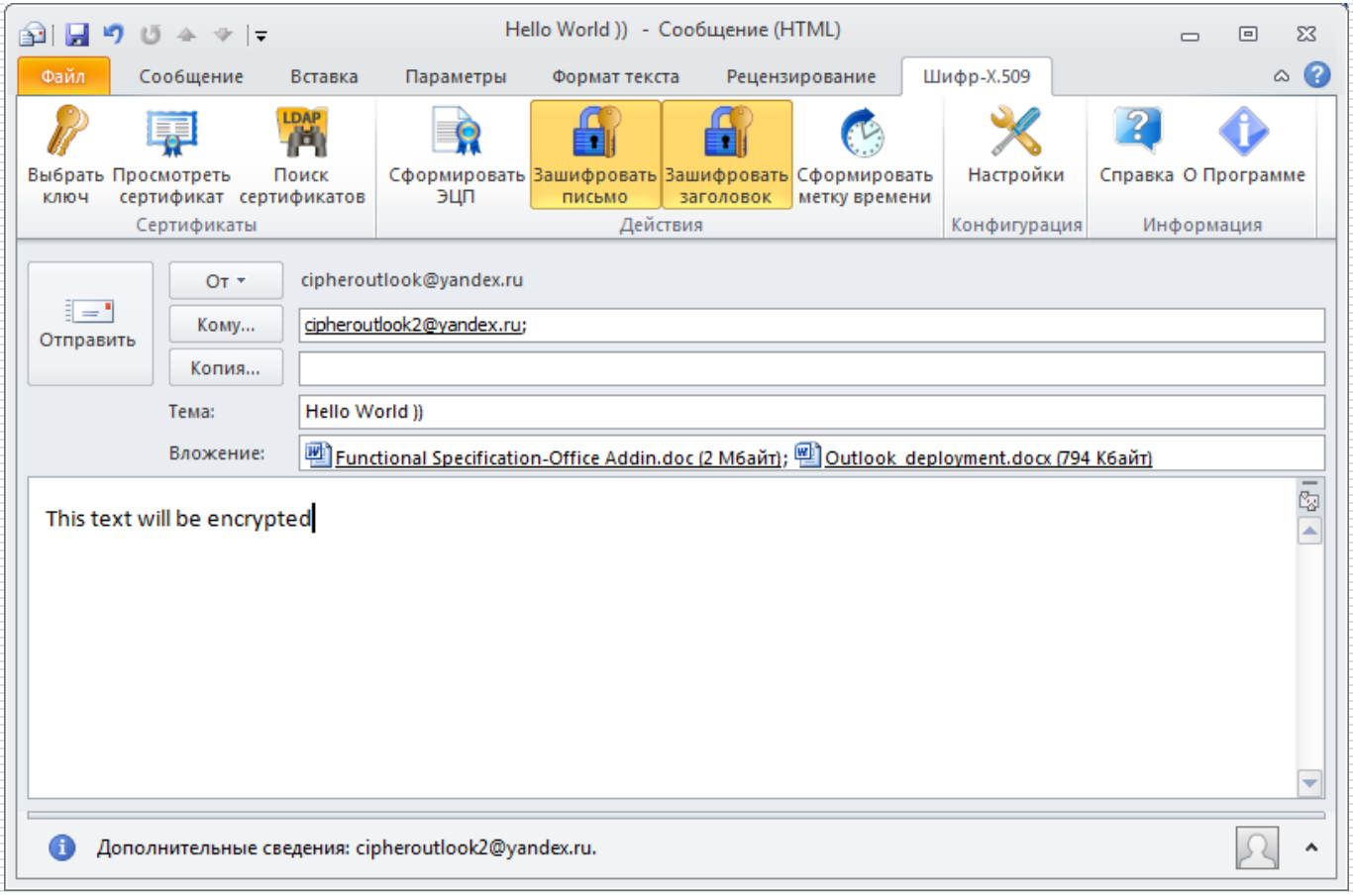
Выбор ключа (1)



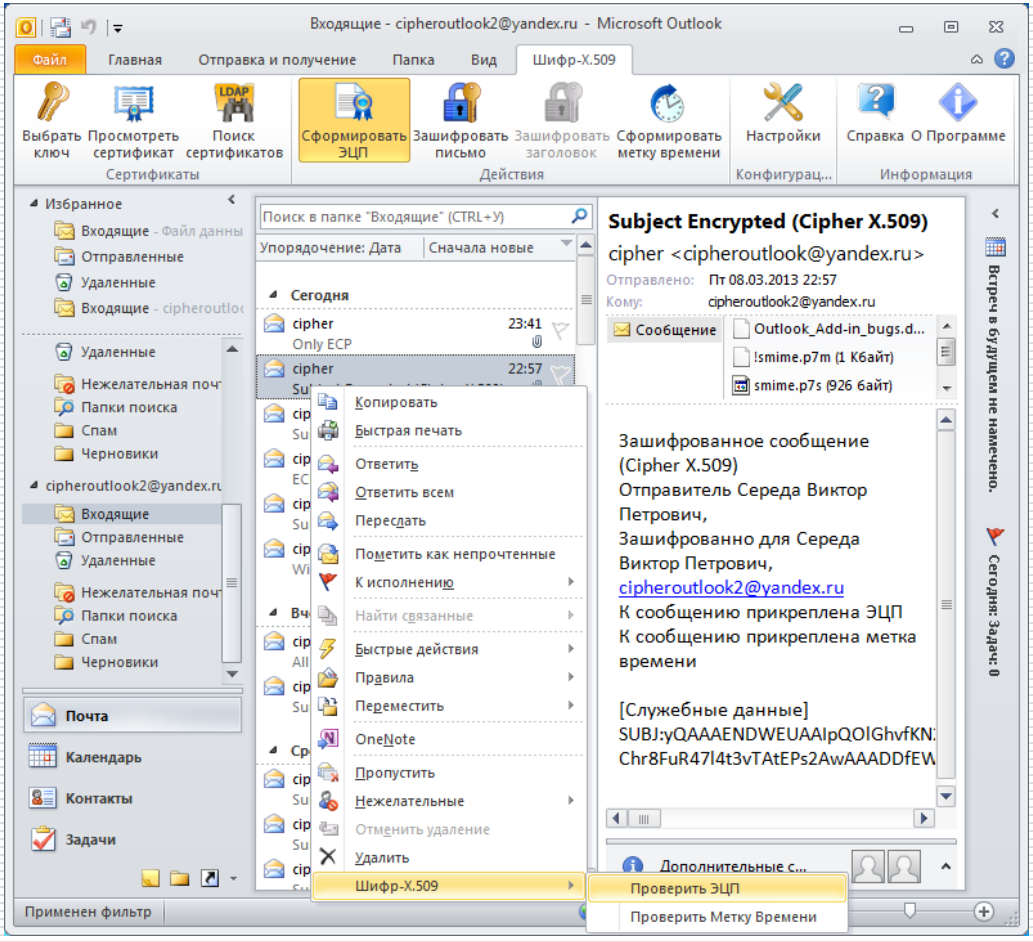
Выбор ключа (2)



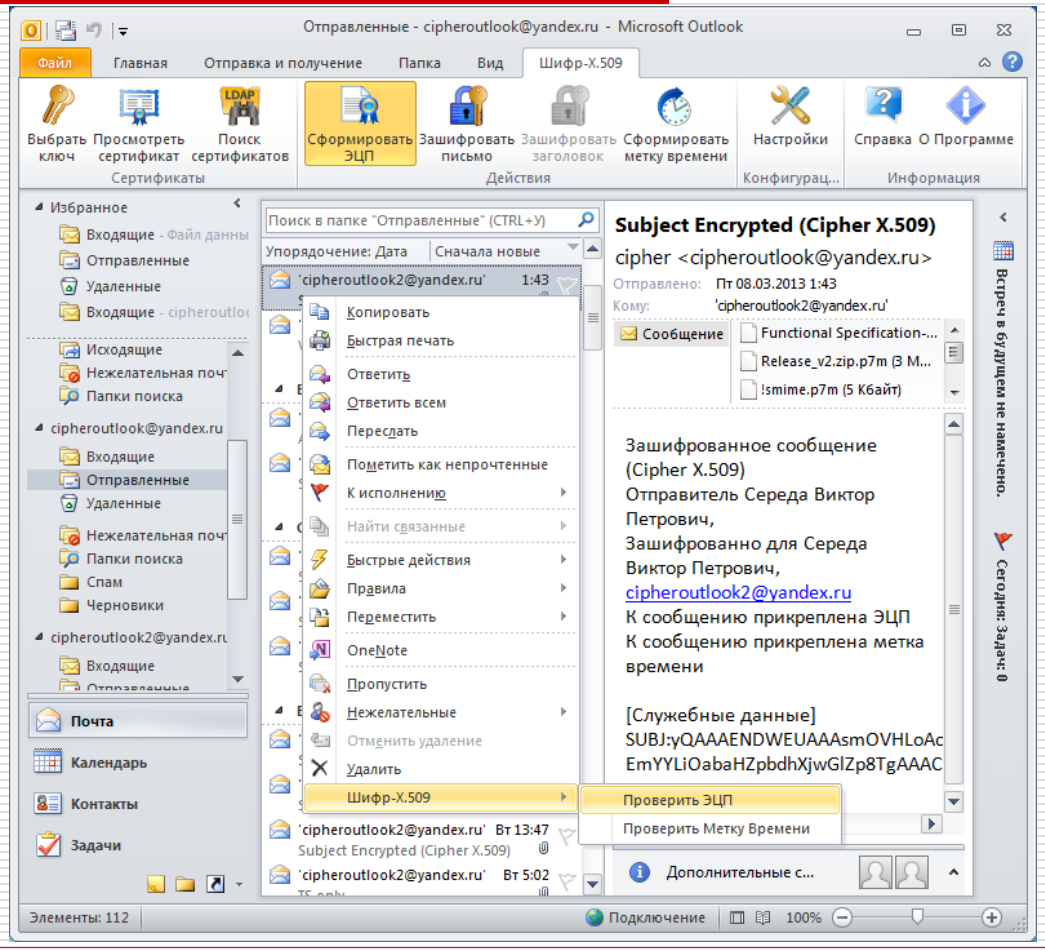
Создание письма



Работа с входящими письмами



Работа с исходящими письмами



Работа с письмами

- Исходное письмо может быть просмотрено в «открытом» виде лишь в режиме просмотра в отдельном окне
- Защищенное письмо может быть просмотрено в «закрытом» виде в режиме предпросмотра (только служебная информация)

CIPHER WORD, EXCEL, POWERPOINT CRYPTO ADD-IN

Услуги

- Целостность и аутентичность
- Причастность
- Простота и прозрачность

Требования

- Защита документов только в формате Office Open XML (OpenXML)
  - Word
  - Excel
  - PowerPoint

*-пользовательская информация внутри документа

Функции

- ЭЦП
- Метка времени
- Комбинации:
  - ЭЦП+МВ
  - иерархия ЭЦП+МВ

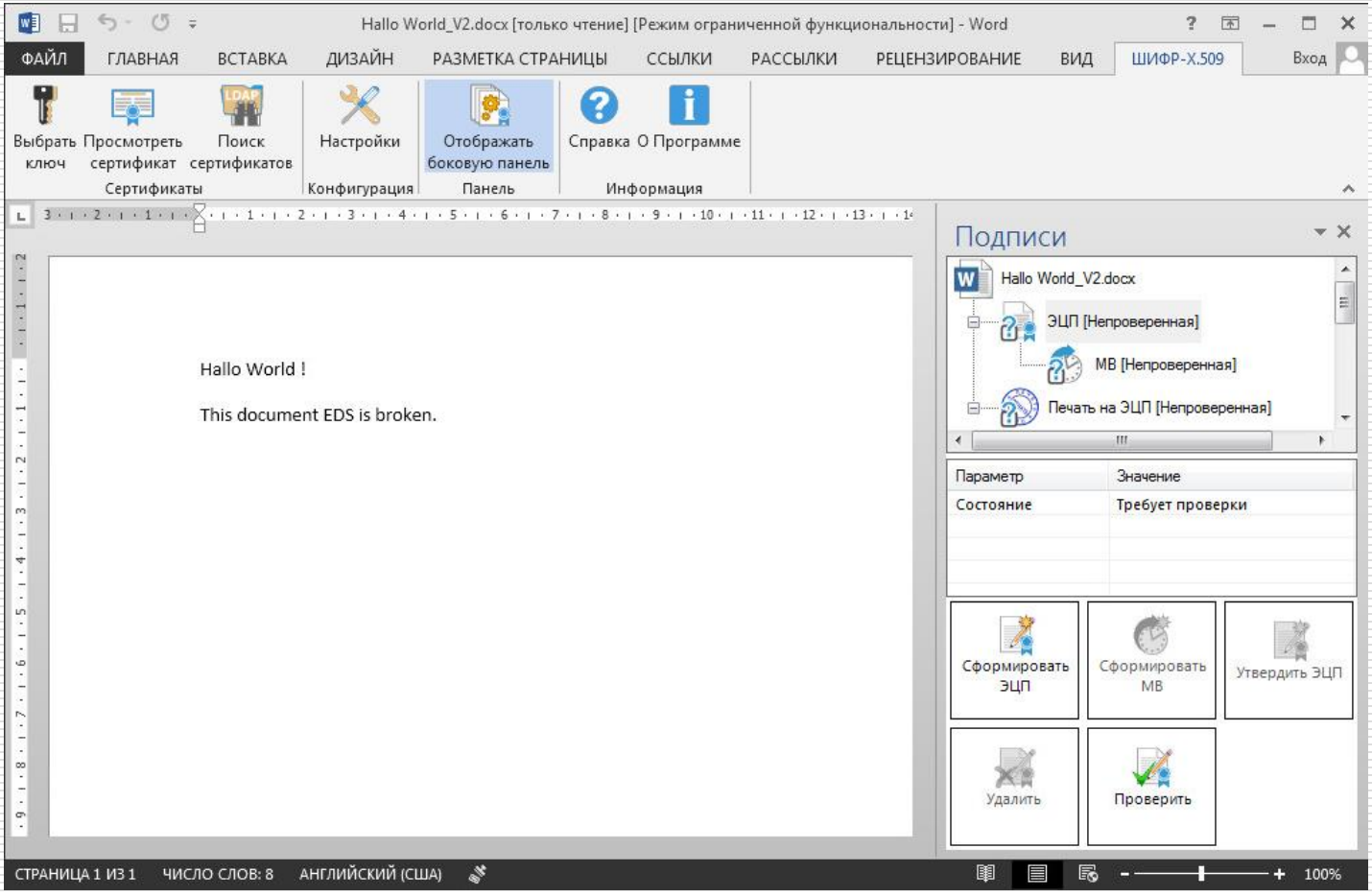
Функции

- Поиск сертификата в LDAP
- Просмотр своего сертификата
- Выбор другого ключа
- Проверка сроков действия ключей
- Работа с ключевым контейнером:
  - Файл
  - Защищенный носитель PKCS#11

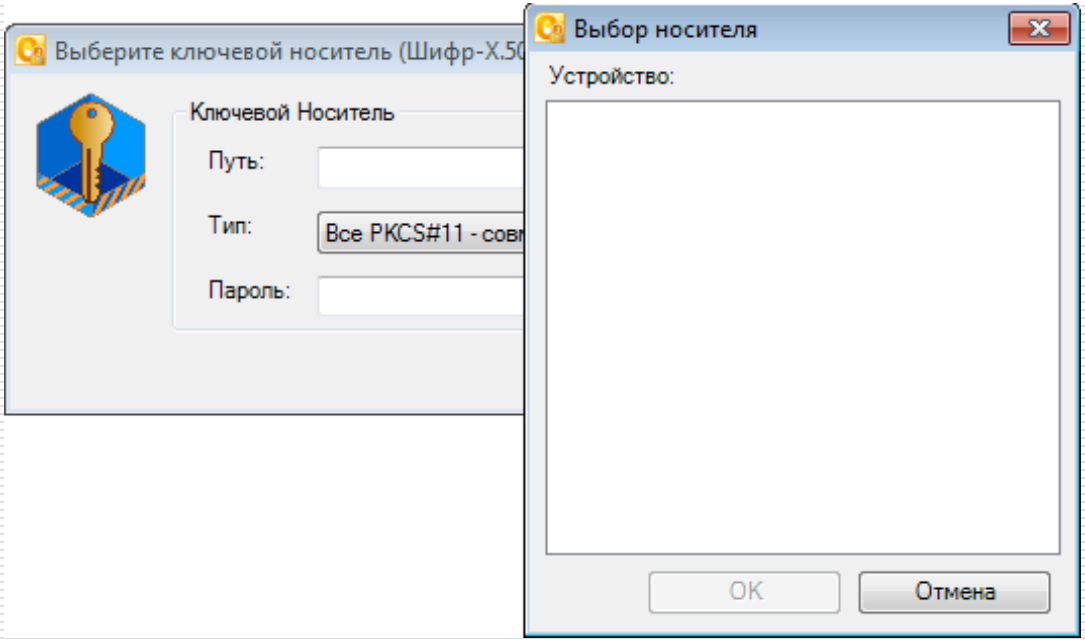
Функции

- Работа с серверами ЦСК (OCSP, TSP, LDAP):
  - Протоколы OCSP, TSP, LDAP
  - Проксирование протоколов OCSP, TSP, LDAP через HTTP

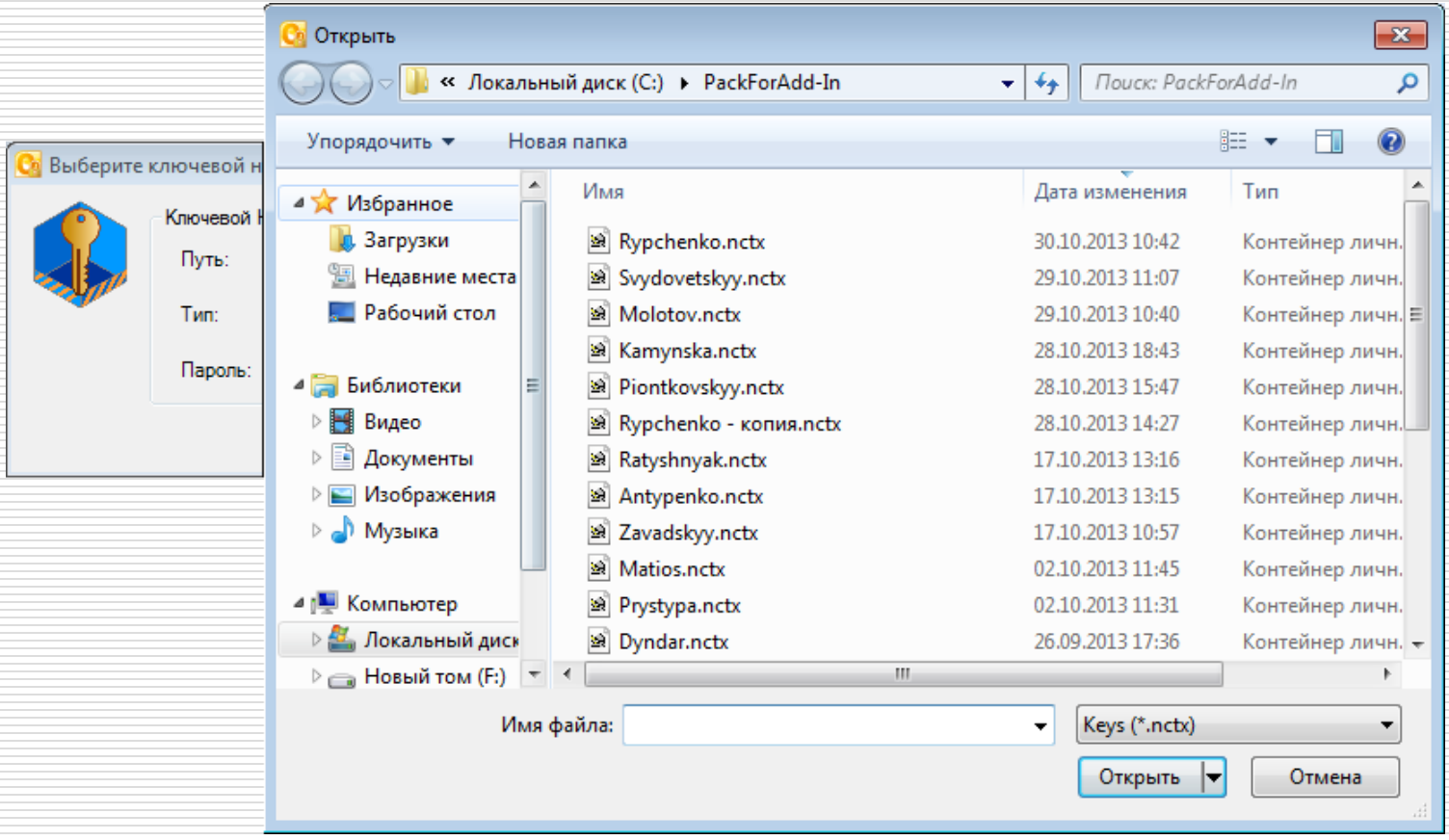
Пользовательский интерфейс



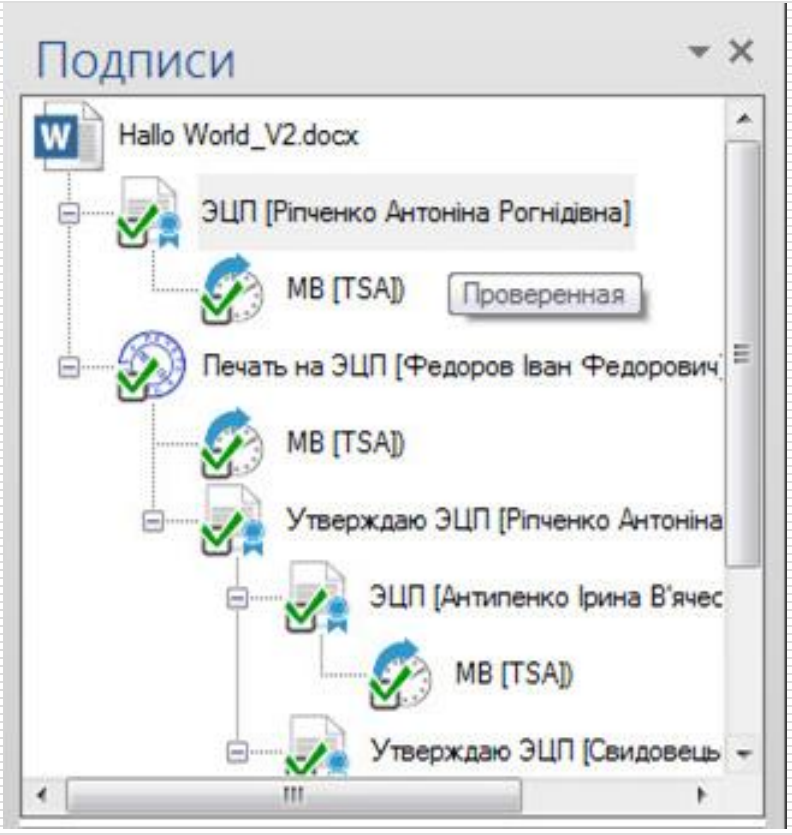
Выбор ключа (1)

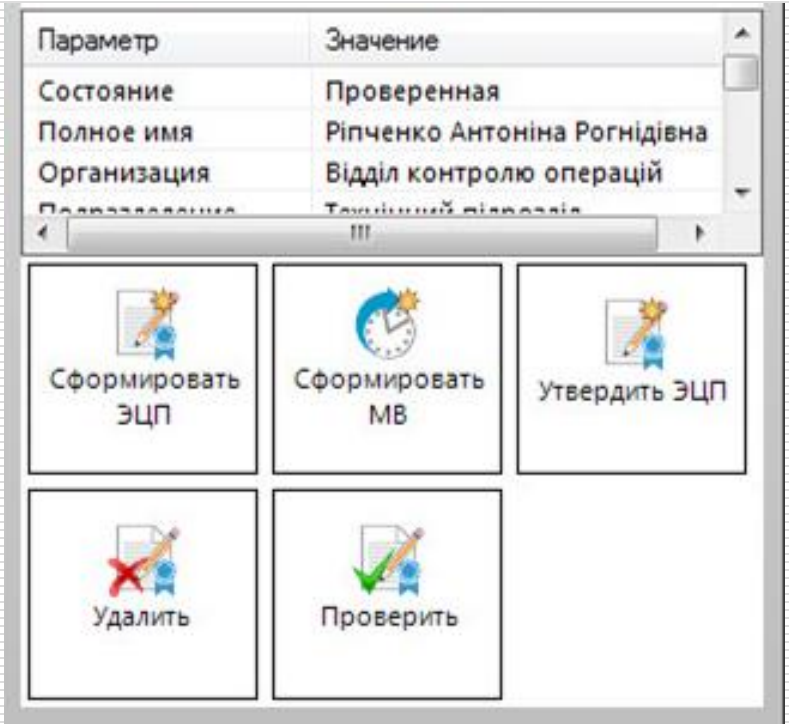


Выбор ключа (2)



Иерархия ЭЦП и МВ





Иерархия ЭЦП и МВ

- Электронная цифровая печать (в зависимости сертификата)
  - Поставить
  - Проверить
  - Удалить
- Метка времени
  - Поставить
  - Проверить
  - Удалить

Иерархия ЭЦП и МВ

- Электронная печать (в зависимости от сертификата)
  - Поставить (ставится на ЭЦП)
  - Проверить
  - Удалить

Интеграция с другими приложениями

РАБОТА С ДОКУМЕНТАМИ WORD, EXCEL, POWERPOINT

Интеграция

- В виде сборки (*.DLL) для .NET Framework 4.0+
- Поддержка платформ x86, x64-86

Функции

- Работа с деревом ЭЦП, МВ и печатями
- Поиск сертификата в LDAP
- Просмотр своего сертификата
- Выбор другого ключа
- Проверка сроков действия ключей

Функции

- Работа с ключевым контейнером:
  - Файл
  - Защищенный носитель PKCS#11
- Работа с серверами ЦСК (OCSP, TSP, LDAP):
  - Протоколы OCSP, TSP, LDAP
  - Проксирование протоколов OCSP, TSP, LDAP через HTTP

Политика лицензирования

CIPHER OUTLOOK, WORD, EXCEL, POWERPOINT CRYPTO ADD-IN

Лицензирование

- Поштучно
  - Отдельный компонент
  - Комплект компонентов
- Без ограничений
  - Отдельный компонент
  - Комплект компонентов

Вопросы?

Спасибо за внимание!

ООО «Сайфер БИС»

Владислав Ковтун

email: vk@cipher.kiev.ua
www: http://cipher.kiev.ua