Лабораторная работа №6

Освоение программных средств для работы с сертификатами открытых ключей

Содержание задания

1. Начать сеанс работы. Для вызова утилит командной строки использовать командную строку Windows (Пуск | Программы | Microsoft Visual Studio 2005 | Visual Studio Tools | Visual Studio 2005 Command Prompt). Для завершения работы в режиме командной строки использовать команду exit.
2. Скопировать в свою индивидуальную папку на рабочей станции документ Microsoft Word «СИСТЕМНЫЕ ПРОГРАММЫ ДЛЯ РАБОТЫ С СЕРТИФИКАТАМИ» из указанного преподавателем места.
3. Открыть скопированный в п. 2 документ и ознакомиться с его разделом 1 «Создание сертификатов».
4. С помощью утилиты командной строки MakeCert выполнить следующее:
   - 4.1. создать закрытый ключ ЭЦП и сертификат, подписанный удостоверяющим центром по умолчанию, поместив их в файлы с расширениями соответственно pvk и cer (имена владельцев сертификатов должны совпадать с фамилиями и инициалами студентов);
   - 4.2. повторить п. 4.1, но поместить закрытый ключ и сертификат в хранилище сертификатов My;
   - 4.3. с помощью созданных в п. 4.2 закрытого ключа и сертификата создать и удостоверить новый сертификат, поместив его в хранилище TrustedPeople;
   - 4.4. создать закрытый ключ и самоподписанный сертификат, поместив их в хранилище CA;
   - 4.5. включить в отчет о лабораторной работе
     - 4.5.1. сведения о назначении и основных функциях утилиты MakeCert;
     - 4.5.2. протокол работы в режиме командной строки, полученный при выполнении п.п. 4.1-4.4 (с помощью системного меню окна командной строки и буфера обмена).
5. С помощью утилиты из состава пакета Microsoft Office SelfCert (в версии Microsoft Office 2003 и старше вызов этой программы возможен через меню Пуск | Программы | Microsoft Office | Средства Microsoft Office | Цифровой сертификат для проектов VBA) выполнить следующее:
   - 5.1. создать самоподписанный сертификат для субъекта с именем, совпадающим с фамилией и инициалами студента;
   - 5.2. включить в отчет о лабораторной работе
     - 5.2.1. сведения о хранилище сертификатов, в которое помещается самоподписанный сертификат.

   Включить в электронную версию отчета
     - 5.2.2. копии экранных форм, полученных при выполнении п. 5.1.
6. Ознакомиться с разделом 2 «Создание списка доверенных сертификатов» скопированного в п. 2 документа.
7. С помощью мастера списка доверия сертификатов, автоматически активизируемого при вызове утилиты командной строки MakeCTL без параметров, выполнить следующее:
   - 7.1. создать файл со списком доверенных сертификатов, созданных при выполнении п.п.4-5 и предназначенных для подписывания кода;
   - 7.2. создать другой файл со списком доверенных сертификатов, созданных при выполнении п.п. 4-5 и предназначенных для шифрования файлов;
   - 7.3. включить в отчет о лабораторной работе

7.3.1. сведения о назначении, способах получения и хранения списков отозванных сертификатов.

Если программа MakeCTL не установлена, то скопировать ее из папки с описаниями лабораторных работ. Включить в электронную версию отчета

7.3.2. копии экранных форм, полученных при выполнении п. 7.

8. Ознакомиться с разделом 3 «Вычисление и проверка электронной цифровой подписи» скопированного в п. 2 документа.
9. С помощью мастера создания ЭЦП, автоматически активизируемого при вызове утилиты командной строки SignTool signwizard без параметров, выполнить следующее:
   9.1. вычислить ЭЦП для файлов со списками доверенных сертификатов, созданных при выполнении п.п. 7.1-7.2, с помощью закрытого ключа и сертификата, созданных при выполнении п. 4.1;
   9.2. вычислить ЭЦП для файлов с произвольными (несистемными) программой и библиотекой (DLL), с помощью секретного ключа и самоподписанного сертификата, созданных при выполнении п. 5.1;
   9.3. включить в отчет о лабораторной работе
      9.3.1. сведения о назначении и способах получения ЭЦП;
      9.3.2. ответ на вопрос, какие возможности утилиты SignTool sign не поддерживаются мастером создания электронной цифровой подписи;
      9.3.3. ответ на вопрос, под файлами каких типов может быть вычислена ЭЦП с помощью утилиты SignTool signwizard.

   Включить в электронную версию отчета

      9.3.4. копии экранных форм, полученных при выполнении п.9.
10. Освоить средства проверки ЭЦП под файлами различных типов:
   10.1. получить сведения о правильности ЭЦП и составе списков доверенных сертификатов, созданных при выполнении п.п. 7.1-7.2 и подписанных при выполнении п. 9.1 (с помощью двойного щелчка на имени соответствующего файла);
   10.2. получить сведения о правильности и параметрах ЭЦП под файлами, подписанными при выполнении п. 9.2 (с помощью вкладки Цифровые подписи окна свойств файла);
   10.3. проверить ЭЦП под файлами, указанными в п.п. 10.1-10.2, с помощью утилиты командной строки SignTool verify (с указанием различных опций при вызове этой утилиты);
   10.4. включить в отчет о лабораторной работе
      10.4.1. сведения о способах проверки ЭЦП и получения ее параметров;
      10.4.2. ответ на вопрос, как происходит добавление издателя сертификата к списку доверенных сертификатов издателей и на что это оказывает влияние (при ответе на этот вопрос могут потребоваться сведения, полученные при выполнении п.п. 12 и 13).

   Включить в электронную версию отчета

      10.4.3. копии экранных форм, полученных при выполнении п. 10.
11. Ознакомиться с разделом 4 «Управление сертификатами» скопированного в п. 2 документа.
12. С помощью утилиты командной строки CertMgr выполнить следующее:
   12.1. добавить списки доверенных сертификатов, созданных при выполнении п. 7 и подписанных при выполнении п.9, в системное хранилище Trust;
   12.2. включить в отчет о выполнении лабораторной работы
      12.2.1. сведения о назначении и основных функциях утилиты CertMgr.

   Включить в электронную версию отчета

12.2.2. протокол работы в режиме командной строки, полученный при выполнении п. 12.1-12.2 (с помощью системного меню окна командной строки и буфера обмена).

13. С помощью менеджера управления сертификатами, автоматически активизируемого при вызове утилиты CertMgr без параметров, выполнить следующее:
    13.1. освоить способы отбора сертификатов с требуемым назначением;
    13.2. освоить способы просмотра характеристик сертификатов;
    13.3. на примере файлов с сертификатами, созданными при выполнении п. 4, освоить работу с мастером импорта сертификатов;
    13.4. освоить работу с мастером экспорта сертификатов;
    13.5. освоить процедуру удаления сертификата, не удаляя их окончательно;
    13.6. включить в отчет о лабораторной работе ответы на вопросы:
        13.6.1. все ли возможности утилиты CertMgr поддерживаются менеджером сертификатов;
        13.6.2. как еще может быть начат диалог с менеджером сертификатов;
        13.6.3. как может быть получена информация о составе списка доверенных издателей сертификатов.

    Включить в электронную версию отчета
        13.6.4. копии экранных форм, полученных при выполнении п. 13.
14. Ознакомиться с разделом 5 «Получение сертификата в удостоверяющем центре» скопированного в п. 2 документа.
15. С помощью оснастки «Сертификаты» выполнить следующее:
    15.1. освоить использование основных функций, доступных с помощью этой оснастки (просмотр хранилищ сертификатов, запрос, просмотр, импорт, экспорт, удаление и поиск сертификатов, просмотр списков отозванных сертификатов);
    15.2. включить в отчет о лабораторной работе ответы на вопросы:
        15.2.1. при каких условиях возможен запрос сертификата с помощью оснастки «Сертификаты»;
        15.2.2. какие дополнительные возможности имеет оснастка «Сертификаты» по сравнению с менеджером сертификатов (п.п. 12-13).

    Включить в электронную версию отчета
        15.2.3. копии полученных при выполнении п. 15 экранных форм
16. Предъявить преподавателю электронную версию отчета о лабораторной работе с копиями использовавшихся экранных форм и соответствующими им номерами пунктов задания (4.5.2, 5.2.2, 7.3.2, 9.3.4, 10.4.3, 12.2.2, 13.6.4, 15.2.3). После принятия результатов работы преподавателем удалить документ Microsoft Word «СИСТЕМНЫЕ ПРОГРАММЫ ДЛЯ РАБОТЫ С СЕРТИФИКАТАМИ» из индивидуальной папки студента, в которую было произведено копирование при выполнении п. 2.
17. Включить в отчет о лабораторной работе
    17.1. ответы на контрольные вопросы, выбранные в соответствии с номером варианта и приложением.
18. Подготовить отчет о выполнении лабораторной работы, который должен включать в себя:
    18.1. титульный лист;
    18.2. сведения, полученные при выполнении работы, и ответы на вопросы с указанием соответствующих пунктов задания (4.5.1, 5.2.1, 7.3.1, 9.3.1, 9.3.2, 9.3.3, 10.4.1, 10.4.2, 12.2.1, 13.6.1, 13.6.2, 13.6.3, 15.2.1, 15.2.2);:
    18.3. ответы на контрольные вопросы.
19. Предъявить отчет о выполнении лабораторной работы (в твердой копии) преподавателю.

Контрольные вопросы

1. Назовите основные свойства и типы устройств аутентификации.
2. Как используются в системах аутентификации генераторы одноразовых паролей на основе счетчиков?
3. Как используются в системах аутентификации генераторы одноразовых паролей на основе внутренних часов?
4. Какие существуют методики применения PIN-кодов?
5. Как проводится регистрация пользователей с устройствами аутентификации?
6. В чем может заключаться защита от угроз при регистрации пользователей с устройствами аутентификации?
7. В чем достоинства и недостатки программных реализаций устройств аутентификации?
8. В чем достоинства и недостатки открытых и закрытых протоколов удаленной аутентификации?
9. Как происходит прямая аутентификация в ОС Windows?
10. Какими могут быть атаки на протокол прямой аутентификации в ОС Windows?
11. Как происходила непрямая аутентификация в ОС Windows NT?
12. Как обеспечивается защищенное взаимодействие сервера и контроллера домена в ОС Windows при непрямой аутентификации?
13. Как происходит непрямая аутентификация в ОС Windows 2000?
14. Как может быть обеспечена защита базовых секретов, используемых для аутентификации компьютеров?
15. Назовите протоколы аутентификации на основе асимметричной криптографии.
16. В чем заключается общая идея протокола SSL?
17. Из каких шагов состоит стандартный вариант протокола SSL?
18. Как обеспечивается дополнительная аутентификация клиента в протоколе SSL?
19. В чем назначение удостоверяющих центров (центров сертификации)?
20. Назовите основные элементы инфраструктуры открытых ключей.
21. Какая информация включается в сертификат открытого ключа в соответствии со стандартом X.509?
22. Где и как может осуществляться хранение личных (секретных, закрытых) ключей пользователей?

Варианты для выбора номеров контрольных вопросов

№	Номера вопросов	№	Номера вопросов	№	Номера вопросов
1	1, 9, 18	11	4, 10, 13	21	1, 8, 16
2	3, 10, 19	12	5, 9, 16	22	2, 17, 22
3	4, 12, 20	13	8, 15, 19	23	3, 11, 18
4	5, 13, 22	14	7, 14, 20	24	4, 14, 20
5	6, 14, 18	15	2, 12, 21	25	5, 15, 20
6	7, 11, 15	16	3, 15, 20	26	6, 12, 16
7	8, 12, 20	17	4, 9, 22	27	7, 11,17
8	1, 11, 17	18	5, 10, 19	28	8, 18, 22
9	2, 10, 21	19	6, 16, 20	29	1, 10, 19
10	3, 12, 22	20	7, 10, 20	30	2, 17, 22