Реализация алгоритма обновления списков аннулированных сертификатов удостоверяющего центра

С.И. Носков, А.П. Медведев

Иркутский государственный университет путей сообщения

Аннотация: Важнейшей проблемой в использовании электронной подписи является актуализация списков аннулированных сертификатов. В настоящий момент не существует единого решения, позволяющего автоматизировать этот процесс. В данной работе приведен один из вариантов решения этой задачи на примере комплексного использования возможностей операционной системы, средств криптографии и стандартных библиотек управления сертификатами.
Ключевые слова: защита информации, программное обеспечение, списки аннулированных сертификатов.

Инфраструктура открытых ключей (PKI), представляющая собой набор средств, служб и компонентов поддержки криптозадач на основе пары закрытого и открытого ключей в настоящее время стала неотъемлемой частью большинства современных производственных процессов [1]. Как показано в статье [2], процесс применения цифровой подписи базируется на PKI, и, хотя сама инфраструктура PKI [3] и алгоритм формирования списков отозванных сертификатов [4] имеют ряд недостатков, важно, чтобы на всех этапах жизни ключа выполнялись все условия её правильного функционирования. При этом одним из необходимых условий для осуществления процесса подписания электронных документов, а также в качестве подтверждения актуальности электронной подписи, является актуализация корневых сертификатов и списков аннулированных сертификатов (CRL-файлов), выпускаемых удостоверяющим центром [5]. Ввиду достаточно короткого времени актуальности (вплоть до нескольких часов) списков аннулированных сертификатов процесс их актуализации зачастую сопряжен с существенными временными трудозатратами, как правило, прямо пропорциональными числу рабочих мест (защищаемых узлов) в организации, а, следовательно, с фактором, который необходимо учитывать при планировании численности подразделения [6]. Как показано в

© Электронный научный журнал «Инженерный вестник Дона», 2007–2025

[7], одной из ключевых задач при организации процесса автоматизации управления электронной подписью и внедрения PKI в домене предприятия также является процесс своевременного обновления списков аннулированных сертификатов. При этом для систем, основанных на сертификатах со списками их отзыва, в обязательном порядке требуется разработка метода распространения CRL-файлов [8].

Список аннулированных сертификатов представляет собой файл с цифровой подписью, выпускаемый удостоверяющими центрами для идентификации сертификатов, запрещенных к использованию, срок действия которых при этом еще не истек. Физически список содержит в себе серийные номера сертификатов ключей проверки электронной подписи, к которым по той или иной причине утрачено доверие (например, в случае компрометации). Стоит отметить, что электронная версия сертификата ключа проверки электронной подписи, выпускаемая удостоверяющим центром, обычно представляет собой файл с расширением .cer формата X.509, содержащий в себе всю необходимую информацию о точках распространения списков аннулированных сертификатов. Особенности работы с сертификатами формата X.509 наглядно показаны в статье [9].

Несмотря на то, что вопросам автоматизации проверки сертификатов уделено внимание в отдельных работах [10], [11], общего решения указанной задачи автоматизации рассылки и установки списков аннулированных сертификатов на текущий момент не существует, а процесс обновления CRL-файлов зачастую сводится к их установке вручную силами специалистов по защите информации, что создает для них дополнительную нагрузку. Однако, решение подобной задачи существует и будет особенно актуальным для автоматизированных рабочих мест и информационных систем, где процесс подписания файлов происходит в непрерывном режиме.

© Электронный научный журнал «Инженерный вестник Дона», 2007–2025

В данной работе предложен алгоритм автоматизации обновления списков аннулированных сертификатов, основыванный на личном сертификате пользователя. В качестве примера реализации подобного подхода выбран язык программирования C# и криптопровайдер КриптоПро CSP. Примеры кода приведены для операционных систем семейства Windows.

Процесс обновления списков аннулированных сертификатов можно условно разделить на 3 этапа:

– очистка старых списков CRL;

– составление ресурсных ссылок для загрузки файлов CRL;

– загрузка и установка файлов CRL.

Все манипуляции с файлами CRL необходимо выполнять с правами администратора. Проверить наличие прав администратора можно с помощью следующего кода:

```
public static bool IsAdministrator()
    {var identity = WindowsIdentity.GetCurrent();
     var principal = new WindowsPrincipal(identity);
     return principal.IsInRole(WindowsBuiltInRole.Administrator);}
```

Далее стоит обратить внимание на существование двух типов хранилищ CRL-файлов в операционных системах семейств Windows и Linux. Хранилище m* (machine) относится ко всем пользователям системы, в то время как хранилище u* (user) – только к пользователю, от имени которого производилась установка. При удалении CRL-файлов необходимо произвести указанные действия для обоих хранилищ: mCA и uCA. Применение приведенного ниже алгоритма к обоим типам хранилищ гарантирует полное удаление CRL-файлов.

© Электронный научный журнал «Инженерный вестник Дона», 2007–2025

Алгоритм удаления CRL-файлов

Процесс очистки происходит с помощью вызова утилиты certmgr.exe, входящей в состав дистрибутива криптопровайдера КриптоПро CSP.

```
Process proc = new Process();
proc.StartInfo.FileName = "certmgr.exe";
proc.StartInfo.RedirectStandardError = true;
proc.StartInfo.Arguments = " -delete -crl -all -store uCA";
System.Diagnostics.ProcessStartInfo processStartInfo =
new System.Diagnostics.ProcessStartInfo(proc.StartInfo.FileName,
proc.StartInfo.Arguments);
int exitCode = 0;
```

Скрытие окон командной строки в процессе выполнения кода возможно реализовать с помощью следующего подхода:

```
proc.StartInfo.WindowStyle = ProcessWindowStyle.Hidden;
processStartInfo.RedirectStandardError = true;
processStartInfo.RedirectStandardOutput = true;
processStartInfo.CreateNoWindow = true;
processStartInfo.UseShellExecute = false;
```

Запуск процесса:

```
System.Diagnostics.Process process =
System.Diagnostics.Process.Start(processStartInfo);
process.WaitForExit();
exitCode = process.ExitCode;
```

Аналогичным образом очищается хранилище mCA:

```
Process proc2 = new Process();
proc2.StartInfo.FileName = pathCertMgr;
proc2.StartInfo.RedirectStandardError = true;
proc2.StartInfo.Arguments = " -delete -crl -all -store mCA";
System.Diagnostics.ProcessStartInfo processStartInfo2 =
new System.Diagnostics.ProcessStartInfo(proc2.StartInfo.FileName,
proc2.StartInfo.Arguments);
int exitCode2 = 0;
proc2.StartInfo.WindowStyle = ProcessWindowStyle.Hidden;
processStartInfo2.RedirectStandardError = true;
```

© Электронный научный журнал «Инженерный вестник Дона», 2007–2025

```
processStartInfo2.RedirectStandardOutput = true;
processStartInfo2.CreateNoWindow = true;
processStartInfo2.UseShellExecute = false;
System.Diagnostics.Process process2 =
System.Diagnostics.Process.Start(processStartInfo2);
process2.WaitForExit();
exitCode2 = process2.ExitCode;
```

Проверяется, успешно ли завершился процесс (вернул ли процесс код 0):

```
if ((exitCode == 0) && (exitCode2 == 0))
{MessageBox.Show("CRL успешно удалены!");}
```

Алгоритм загрузки CRL-файлов

Каждый сертификат ключа проверки электронной подписи содержит в себе ссылки на точки распространения CRL-файлов. Достаточно объединить их в единый массив, после чего поочередно скачать и установить в систему. Для этой цели необходимо воспользоваться классом X509Certificate2. Работа с объектами класса X509Certificate2 была наглядно показана в [2].

Импортируется сертификат и создается массив ссылок точек распространения CRL-файлов:

```
X509Certificate2 x509 = new X509Certificate2();
byte[] rawData = ReadFile(Directory.GetCurrentDirectory() + "\\Cert.cer");
x509.Import(rawData);
string[] links = X509Certificate2Extensions.GetCrlDistributionPoints(x509);
for (int i = 0; i < links.Length; i++)
    links[i] = links[i].Substring(0, links[i].LastIndexOf('.') + 4);
```

Производится загрузка CRL-файлов (в качестве адреса используется ссылка из созданного ранее массива):

```
client.DownloadFile(links[i], Directory.GetCurrentDirectory() + "\\CRL\\" + i + ".CRL");
```

Алгоритм установки CRL-файлов в систему

Для установки CRL-файлов можно воспользоваться стандартной утилитой certutil.exe, входящей в состав большинства дистрибутивов операционных

© Электронный научный журнал «Инженерный вестник Дона», 2007–2025

систем семейства Windows. В приведенном ниже коде переменная fullName содержит полный адрес до CRL-файла:

```
Process proc = new Process();
proc.StartInfo.FileName = "certutil.exe";
proc.StartInfo.RedirectStandardError = true;
proc.StartInfo.Arguments = " -addstore CA " + "\"" + fullName + "\"";
System.Diagnostics.ProcessStartInfo processStartInfo =new
System.Diagnostics.ProcessStartInfo(proc.StartInfo.FileName,
proc.StartInfo.Arguments);
int exitCode = 0;
proc.StartInfo.WindowStyle = ProcessWindowStyle.Hidden;
processStartInfo.RedirectStandardError = true;
processStartInfo.RedirectStandardOutput = true;
processStartInfo.CreateNoWindow = true;
processStartInfo.UseShellExecute = false;
System.Diagnostics.Process process =
System.Diagnostics.Process.Start(processStartInfo);
process.WaitForExit();
exitCode = process.ExitCode;
```

Заключение

Таким образом, в работе наглядно показано, как при помощи совместного использования возможностей операционной системы, элементов дистрибутива криптопровайдера и библиотек управления сертификатами возможно с высокой эффективностью автоматизировать процесс обновления списков аннулированных сертификатов. Приведенные алгоритмы могут быть использованы как в качестве самостоятельного приложения, так и при разработке отдельных элементов программного обеспечения управления механизмами цифровой подписи.

Литература

1. Котенко А.В., Нурдавлетова Д.Р., Сопов М.А. Структура инфраструктуры открытых ключей // Электронные средства и системы

© Электронный научный журнал «Инженерный вестник Дона», 2007–2025

управления. Материалы докладов международной научно-практической конференции, 2013 № 2, С. 18-22.

2. Носков С.И., Медведев А.П. Реализация алгоритмов управления электронной подписью // Инженерный вестник Дона, 2024, №10. URL: ivdon.ru/ru/magazine/archive/n10y2024/9586.

3. Ellison C., Schneier B. Ten Risks of PKI: What You're not Being Told about Public Key Infrastructure // Computer Security Journal, 2000, Vol. 16, No 1, pp. 1-8.

4. Колыбельников А.И. Новый алгоритм формирования списков отозванных сертификатов // Труды МФТИ, 2017, Т. 9, № 2, С. 111-116.

5. Корчагина Е. В., Андреева Н. А., Бутова Л. В., Рогов И. В. Анализ задач администратора программно-технических средств удостоверяющего центра // Актуальные проблемы деятельности подразделений УИС. Сборник материалов Всероссийской научно-практической конференции. В 2-х частях. Часть 1, 2019, С. 365-367.

6. Носков С.И., Медведев А.П. Регрессионное моделирование штатной численности подразделений по защите информации // Инженерный вестник Дона, 2024, № 6. URL: ivdon.ru/ru/magazine/archive/n6y2024/9283.

7. Шпак С. Установка цепочки серверов сертификации как часть внедрения pki в домене. Часть 3 // Системный администратор, 2008, №11, С. 66-69.

8. Menezes A.J., Paul C. van Oorschot, Vanstone S.A. Handbook of applied cryptography, 1999, 794 p.

9. Housley R., Ford W., Polk W., Solo D. Internet X.509 public key infrastructure certificate and crl profile // RFC 2459, 1999, pp. 1-129.

10. Ключенко А.А., Пестова С.Ю., Лисютенко Д.В. Автоматизация запросов на проверку сертификатов электронной подписи // Образование.

© Электронный научный журнал «Инженерный вестник Дона», 2007–2025

Транспорт. Инновации. Строительство. Сборник материалов III Национальной научно-практической конференции, 2020, С. 689-693.

11. Толох И. О., Михневич С. Ю., Сенкевич А. Ю. Сервис для проверки сертификатов электронных документов // Цифровая трансформация, 2023, Т. 29, № 4, С. 50-57.

References

1. Kotenko A.V., Nurdavletova D.R., Sopov M.A., Jelektronnye sredstva i sistemy upravlenija. Materialy dokladov mezhdunarodnoj nauchno-prakticheskoj konferencii, 2013 № 2, pp. 18-22.

2. Noskov S.I., Medvedev A.P. Inzhenernyj vestnik Dona, 2024, №10. URL: ivdon.ru/ru/magazine/archive/n10y2024/9586.

3. Ellison C., Schneier B. Computer Security Journal, 2000, Vol. 16, No 1, pp. 1-8.

4. Kolybel'nikov A.I. Trudy MFTI, 2017, T. 9, № 2, pp. 111-116.

5. Korchagina E. V., Andreeva N. A., Butova L. V., Rogov I. V. Aktual'nye problemy dejatel'nosti podrazdelenij UIS. Sbornik materialov Vserossijskoj nauchno-prakticheskoj konferencii. V 2-h chastjah. Chast' 1, 2019, pp. 365-367.

6. Noskov S.I., Medvedev A.P. Inzhenernyj vestnik Dona, 2024, №6. URL: ivdon.ru/ru/magazine/archive/n6y2024/9283.

7. Shpak S. Sistemnyj administrator, 2008, №11, pp. 66-69.

8. Menezes A.J., Paul C. van Oorschot, Vanstone S.A. Handbook of applied cryptography, 1999, 794 p.

9. Housley R., Ford W., Polk W., Solo D. RFC 2459, 1999, pp. 1-129.

10. Kljuchenko A.A., Pestova S.Ju., Lisjutenko D.V. Obrazovanie. Transport. Innovacii. Stroitel'stvo. Sbornik materialov III Nacional'noj nauchno-prakticheskoj konferencii, 2020, pp. 689-693.

11. Toloh I. O., Mihnevich S. Ju., Senkevich A. Ju. Cifrovaja transformacija, 2023, V. 29, № 4, pp. 50-57.

Дата поступления: 21.11.2024 Дата публикации: 3.01.2025

© Электронный научный журнал «Инженерный вестник Дона», 2007–2025