



ViPNet Publication Service

Форматы хранения опубликованных данных

© ОАО «ИнфоТеКС», 2019

ФРКЕ.00113-04 90 03

Версия продукта 4.6.6

Этот документ входит в комплект поставки ViPNet Publication Service, и на него распространяются все условия лицензионного соглашения.

Ни одна из частей этого документа не может быть воспроизведена, опубликована, сохранена в электронной базе данных или передана в любой форме или любыми средствами, такими как электронные, механические, записывающие или иначе, для любой цели без предварительного письменного разрешения ОАО «ИнфоТеКС».

ViPNet® является зарегистрированным товарным знаком ОАО «ИнфоТеКС».

Все названия компаний и продуктов, которые являются товарными знаками или зарегистрированными товарными знаками, принадлежат соответствующим владельцам.

ОАО «ИнфоТеКС»

127287, г. Москва, Старый Петровско-Разумовский проезд, д. 1/23, стр. 1, 2 этаж

Телефон: +7 (495) 737-6192, 8-800-250-0260 — бесплатный звонок из России (кроме Москвы)

Веб-сайт: <https://infotecs.ru>

Служба технической поддержки: hotline@infotecs.ru

Содержание

Введение.....	4
О документе.....	5
Соглашения документа.....	5
Обратная связь.....	6
Глава 1. Формат размещения данных на LDAP-серверах AD DS и AD LDS.....	7
Сертификаты пользователей.....	8
Публикация в AD DS	8
Публикация в AD LDS	8
Сертификаты издателей.....	12
Публикация в AD LDS	12
Списки аннулированных сертификатов сетей ViPNet	13
Списки аннулированных сертификатов сторонних сетей	14
Глава 2. Формат размещения данных на FTP-сервере	15
Сертификаты издателей.....	16
Сертификаты пользователей.....	17
Списки аннулированных сертификатов сетей ViPNet	18
Списки аннулированных сертификатов сторонних сетей	19
Приложение А. Глоссарий	20



Введение

О документе	5
Обратная связь	6

О документе

При организации системы защищенного документооборота возникает потребность в публикации сертификатов и [списков аннулированных сертификатов \(CRL\)](#) (см. глоссарий, стр. 21) в едином хранилище для общего доступа к ним всех участников документооборота. Такое хранилище можно организовать на основе [службы домена Active Directory \(AD DS\)](#) (см. глоссарий, стр. 20), [службы Active Directory облегченного доступа к каталогам \(AD LDS\)](#) (см. глоссарий, стр. 20) или на FTP-сервере.

Данный документ входит в комплект поставки программы ViPNet Publication Service и описывает формат размещения данных в хранилищах. Также в документе приводится информация об обеспечении доступа к опубликованным данным из клиентских приложений.

Соглашения документа

Ниже перечислены соглашения, принятые в этом документе для выделения информации.

Таблица 1. Обозначения, используемые в примечаниях




Обозначение	Описание
	Внимание! Указывает на обязательное для исполнения или следования действие или информацию.
	Примечание. Указывает на необязательное, но желательное для исполнения или следования действие или информацию.
	Совет. Содержит дополнительную информацию общего характера.

Таблица 2. Обозначения, используемые для выделения информации в тексте

Обозначение	Описание
Название	Название элемента интерфейса. Например, заголовок окна, название поля, кнопки или клавиши.
Клавиша+Клавиша	Сочетание клавиш. Чтобы использовать сочетание клавиш, следует нажать первую клавишу и, не отпуская ее, нажать вторую клавишу.
Меню > Подменю > Команда	Иерархическая последовательность элементов. Например, пункты меню или разделы на панели навигации.
Код	Имя файла, путь, фрагмент текстового файла (кода) или команда, выполняемая из командной строки.

Обратная связь

Дополнительная информация

Сведения о продуктах и решениях ViPNet, распространенные вопросы и другая полезная информация собраны на сайте ОАО «ИнфоТеКС»:

- Информация о продуктах ViPNet <https://infotecs.ru/product/>.
- Информация о решениях ViPNet <https://infotecs.ru/resheniya/>.
- Часто задаваемые вопросы <https://infotecs.ru/support/faq/>.
- Форум пользователей продуктов ViPNet <https://infotecs.ru/forum/>.

Контактная информация

Если у вас есть вопросы, свяжитесь со специалистами ОАО «ИнфоТеКС»:

- Единый многоканальный телефон:
+7 (495) 737-6192,
8-800-250-0-260 — бесплатный звонок из России (кроме Москвы).

- Служба технической поддержки: hotline@infotecs.ru.

Форма для обращения в службу технической поддержки через сайт
<https://infotecs.ru/support/request/>.

Консультации по телефону для клиентов с расширенной схемой технической поддержки:
+7 (495) 737-6196.

- Отдел продаж: soft@infotecs.ru.

Если вы обнаружили уязвимости в продуктах компании, сообщите о них по адресу security-notifications@infotecs.ru. Распространение информации об уязвимостях продуктов ОАО «ИнфоТеКС» регулируется политикой ответственного разглашения
<https://infotecs.ru/disclosure.php>.

1

Формат размещения данных на LDAP-серверах AD DS и AD LDS

Сертификаты пользователей	8
Сертификаты издателей	12
Списки аннулированных сертификатов сетей ViPNet	13
Списки аннулированных сертификатов сторонних сетей	14

Сертификаты пользователей

Публикация в AD DS

Для успешной публикации имя владельца сертификата не должно содержать один и тот же атрибут более одного раза.

Публикация сертификатов представляет собой запись сертификата в атрибут `userCertificate` объекта класса `user`, который является учетной записью пользователя домена Active Directory. Если на момент записи атрибут `userCertificate` уже содержит другой ранее опубликованный сертификат, то он будет замещен вновь опубликованным.

Сертификат должен быть в DER-кодировке. При публикации не происходит создания каких-либо вспомогательных объектов, только поиск подходящей учетной записи пользователя и запись в нее сертификата. При поиске подходящей учетной записи используется таблица сопоставления атрибутов учетной записи и атрибутов имени владельца публикуемого сертификата. С таблицей сопоставления можно ознакомиться, запустив мастер создания публикации в программе ViPNet Publication Service (см. документ «ViPNet Publication Service. Руководство администратора», раздел «Публикация в AD DS»).

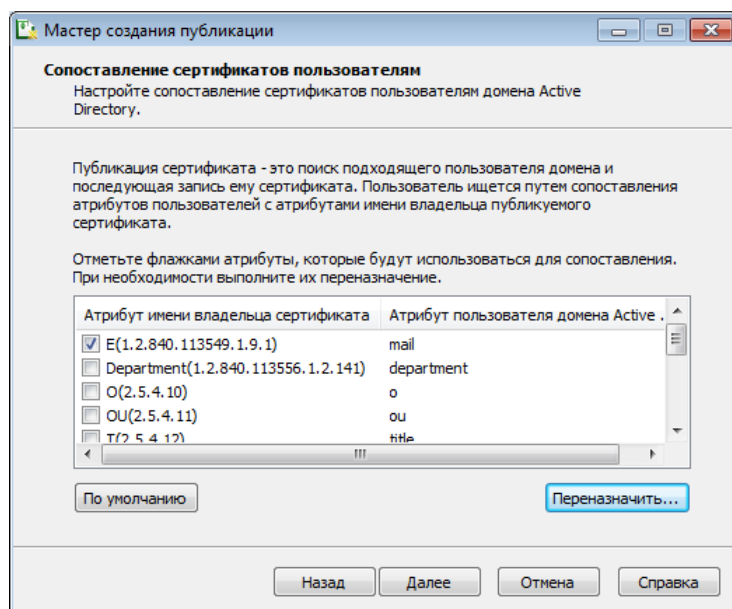


Рисунок 1: Сопоставление сертификатов пользователям Active Directory

Публикация в AD LDS

Для хранения сертификатов используются вспомогательные объекты класса `inetOrgPerson`. Сертификат хранится в его атрибуте `userCertificate`. При публикации сертификата создается иерархия вспомогательных [контейнеров](#) (см. глоссарий, стр. 21). Иерархия контейнеров нужна для

обеспечения возможности публикации множества сертификатов на одного пользователя, а также для упрощения навигации по содержимому хранилища средствами простых неспециализированных инструментов, например оснастки **Редактирование ADSI**.

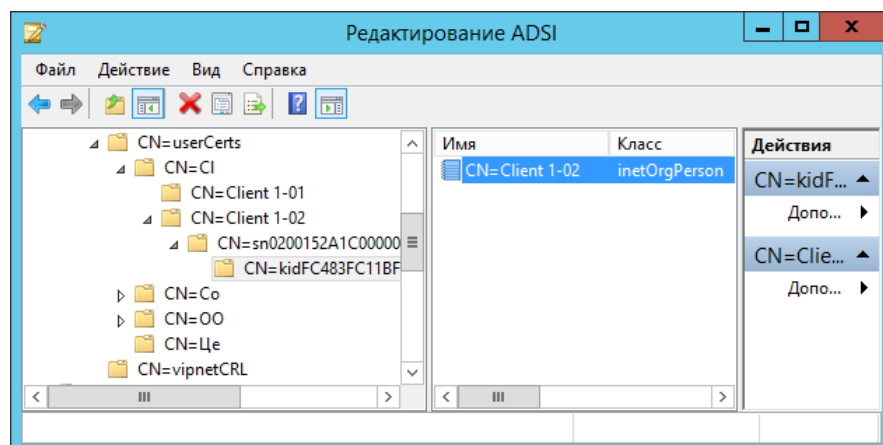


Рисунок 2. Структура хранения сертификата при публикации в AD LDS

Несмотря на то, что атрибут `userCertificate` может хранить несколько значений (сертификатов), эта возможность не используется, и атрибут всегда хранит только одно значение. Сделано это для того, чтобы упростить реализацию и повысить скорость выполнения поиска сертификатов на клиентской стороне.

Принцип формирования вспомогательных контейнеров следующий.

На верхнем уровне находится контейнер, имя которого представляет собой первые 2 символа атрибута `CN` имени владельца сертификата. Имя контейнера сокращается до одного символа, если имя атрибута состоит из одного символа. Если имя пользователя не включает в себя атрибут `CN`, то в качестве замены используется атрибут `Pseudonym`. Если имя пользователя не включает в себя ни один из перечисленных атрибутов, сертификат не будет опубликован. Этот уровень иерархии нужен для упрощения непосредственного анализа содержимого базы с помощью низкоуровневых инструментов вроде оснастки **Редактирование ADSI** и утилиты `LDP.EXE`.

На уровень ниже находится контейнер, имя которого представляет собой отображаемое имя владельца сертификата. Отображаемое имя — это атрибут `CN` или `Pseudonym`, в зависимости от того, который из них представлен в имени владельца сертификата.

На уровень ниже находится контейнер, хранящий серийный номер публикуемого сертификата в следующем формате:

Имя контейнера = "sn" + Шестнадцатичное представление серийного номера.

Например, `sn14080C2713080000100172139A32C801`.

На уровень ниже находится контейнер, хранящий идентификатор ключа проверки электронной подписи публикуемого сертификата в следующем формате:

Имя контейнера = "kid" + Шестнадцатичное представление идентификатора.

Например, `kid59646083885801A4ACDC0497BD721097A1C5BD70`.

Этот контейнер не будет создан в том случае, если идентификатор ключа проверки электронной подписи не указан в сертификате.

В самом низу размещается объект класса `inetOrgPerson`, который содержит сертификат, а также некоторые атрибуты имени владельца сертификата. Атрибуты имени владельца могут быть использованы при поиске опубликованных сертификатов по атрибутам имени владельца. Атрибуты сохраняются в объекте `inetOrgPerson` в соответствии со следующей таблицей.

Таблица 3. Сопоставление атрибутов в имени владельца сертификата и AD LDS

Название атрибута в имени владельца сертификата (OID атрибута)	Название атрибута в AD LDS (OID атрибута)
cn (2.5.4.3)	cn(2.5.4.3)
pseudonym(2.5.4.65)	pseudonym(2.5.4.65)
o(2.5.4.10)	o(2.5.4.10)
c(2.5.4.6)	c(2.5.4.6)
l(2.5.4.7)	l(2.5.4.7)
OU(2.5.4.11)	ou(2.5.4.11)
serialNumber(2.5.4.5)	serialNumber(2.5.4.5)
E(1.2.840.113549.1.9.1)	mail(0.9.2342.19200300.100.1.3)
ST(2.5.4.8)	st(2.5.4.8)
postalAddress(2.5.4.16)	postalAddress(2.5.4.16)
t(2.5.4.12)	title(2.5.4.12)
department(1.2.840.113556.1.2.141)	department(1.2.840.113556.1.2.141)
unstructuredName(1.2.840.113549.1.9.2)	unstructuredName(1.2.840.113549.1.9.2)
OGRN(1.2.643.100.1)	oGRN(1.2.643.100.1)
SNILS(1.2.643.100.3)	sNILS(1.2.643.100.3)
INN(1.2.643.3.131.1.1)	iNN(1.2.643.3.131.1.1)
SN(2.5.4.4)	sn(2.5.4.4)
G(2.5.4.42)	givenName(2.5.4.42)

Атрибуты `department`, `unstructuredName` и `Pseudonym` не являются частью схемы по умолчанию. Они определены в файлах расширения схемы, поставляемых в составе программы ViPNet Publication Service.

Кроме перечисленных выше атрибутов имени, в объект `inetOrgPerson` при публикации сохраняются: имя издателя сертификата, серийный номер сертификата, идентификатор ключа проверки электронной подписи. При публикации эти поля сертификата сохраняются соответственно в атрибуты `infotecsCertIssuer`, `infotecsCertSerialNumber`, `infotecsCertSubjectKeyIdentifier`. Все 3 атрибута являются индексными, поэтому их можно

использовать для быстрого поиска опубликованных сертификатов. Определения этих атрибутов находятся в файлах расширения схемы, поставляемых в составе программы ViPNet Publication Service.

Сертификаты издателей

Публикация в AD LDS

Сертификаты издателей публикуются так же, как и сертификаты пользователей, за исключением того, что для хранения сертификата вместо атрибута `userCertificate` используется атрибут `cACertificate`.

Списки аннулированных сертификатов сетей ViPNet

Каждый [список аннулированных сертификатов](#) (см. глоссарий, стр. 21) хранится в отдельном контейнере, имя которого представляет собой номер сети ViPNet, для которой издан CRL. Для хранения списка используется объект класса `cRLDistributionPoint`. Сам список непосредственно хранится в атрибуте `certificateRevocationList`.

Имя объекта `cRLDistributionPoint` зависит от способа формирования расширения [Authority Key Identifier](#) (см. глоссарий, стр. 20). Возможны варианты:

- 1 В качестве расширения указан идентификатор ключа проверки электронной подписи издателя.

Имя объекта = "kid" + Шестнадцатичное представление идентификатора.

Пример: kidBE5FB4BC7096CC236CBFD60909851345CCA43B39

- 2 Идентификатора нет, но указан серийный номер сертификата ключа проверки электронной подписи издателя.

Имя объекта = "isn" + Шестнадцатичное представление серийного номера.

Пример: isn0200F010A000000060549CE2A543C801

В свойстве `description` объекта `cRLDistributionPoint` сертификата хранится также имя издателя, который выпустил CRL. Этот атрибут многострочный, поэтому имя издателя хранится как одна из его строк. Перед значением имени издателя добавляется префикс «issuerName:». Это нужно на случай, если в описание [точки распространения](#) (см. глоссарий, стр. 22) будет добавлено еще что-то.

Пример значения атрибута `description`:

issuerName:C=RU,L=Ростов-на-Дону,T=Администратор,CN=Rosta Administrator

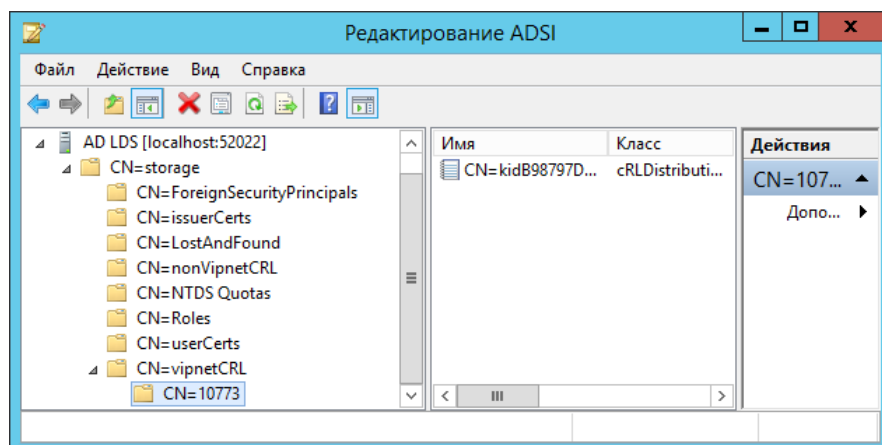


Рисунок 3. Структура хранения CRL сетей ViPNet на LDAP-сервере

Списки аннулированных сертификатов сторонних сетей

Каждый список аннулированных сертификатов хранится в отдельном контейнере, имя которого представляет собой один из predetermined атрибутов имени издателя. Выбор выполняется по следующему правилу: если в имени издателя задан CN, то имя контейнера = CN. Если в имени издателя задан Pseudonym, то имя контейнера = Pseudonym. Далее, аналогично для атрибутов: OU и O.

Имя объекта `cRLDistributionPoint` зависит от способа формирования расширения [Authority Key Identifier](#) (см. глоссарий, стр. 20). Возможны варианты:

- 1 В качестве расширения указан идентификатор ключа проверки электронной подписи издателя.

Имя объекта = "kid" + Шестнадцатичное представление идентификатора.

Пример: kidBE5FB4BC7096CC236CBFD60909851345CCA43B39

- 2 Идентификатора нет, но указан серийный номер сертификата ключа проверки электронной подписи издателя.

Имя объекта = "isn" + Шестнадцатичное представление серийного номера.

Пример: isn0200F010A000000060549CE2A543C801

В свойстве `description` объекта `cRLDistributionPoint` сертификата хранится также имя издателя, который выпустил CRL. Этот атрибут многострочный, поэтому имя издателя хранится как одна из его строк. Перед значением имени издателя добавляется префикс «issuerName:». Это нужно на случай, если в описание [точки распространения](#) (см. глоссарий, стр. 22) будет добавлено еще что-то.

Пример: issuerName:C=RU,L=Ростов-на-Дону,T=Администратор,CN=Rosta Administrator

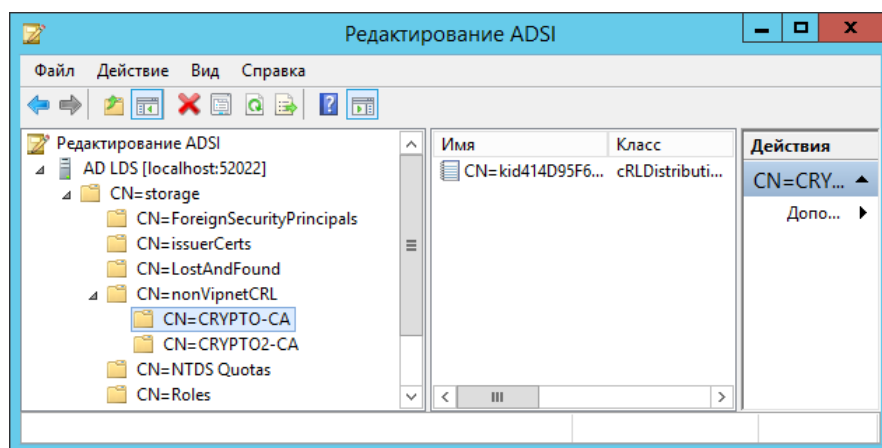


Рисунок 4. Структура хранения CRL сторонних сетей на LDAP-сервере

2

Формат размещения данных на FTP-сервере

Сертификаты издателей	16
Сертификаты пользователей	17
Списки аннулированных сертификатов сетей ViPNet	18
Списки аннулированных сертификатов сторонних сетей	19

Сертификаты издателей

Каждый [сертификат издателя](#) (см. глоссарий, стр. 21) или список аннулированных сертификатов хранятся в отдельных каталогах, имена которых формируются по определенным правилам.

Для сертификатов издателей каталоги формируются на основе идентификатора ключа проверки электронной подписи (если он указан в сертификате).

Имя каталога = «kid» + Шестнадцатеричное представление идентификатора.

Пример: kid131890B2951899E62159569AE7D542AA3766ED3B

Внутри каталога размещаются файлы с именами:

- 1 `subject` — бинарный файл. Хранит имя владельца сертификата в формате ASN.1 в кодировке DER. Фактически в этом поле находится значение поля Subject (Субъект) сертификата. Файл предназначен для упрощения поиска нужного сертификата по известному атрибуту имени владельца.
- 2 `issuer.crt` — бинарный файл. Хранит сертификат издателя в кодировке DER.

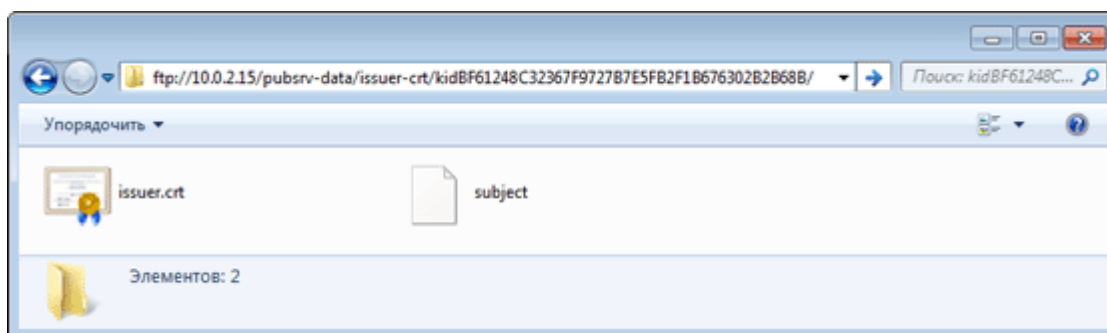


Рисунок 5. Структура хранения сертификатов издателей на FTP-сервере

Сертификаты пользователей

Сертификаты пользователей используют в целом ту же схему хранения, что и сертификаты издателей. Отличия в следующем:

- 1 Сертификат пользователя хранится в файле с именем `user.crt`.
- 2 Для успешной публикации сертификат пользователя должен иметь расширение Subject Key Identifier. Фактически это означает, что имя папки с сертификатом пользователя всегда имеет следующий вид: `kid131890B2951899E62159569AE7D542AA3766ED3B`.

Списки аннулированных сертификатов сетей ViPNet

При размещении CRL сетей ViPNet на FTP-сервере имя каталога формируется следующим образом:

Имя каталога = номер сети в десятичном формате + дефис + "kid" + Шестнадцатиричное представление идентификатора.

Пример: 4342-kidBE5FB4BC7096CC236CBFD60909851345CCA43B39

Внутри каталога размещаются файлы с именами:

- 1 issuer — бинарный файл. Хранит имя издателя в формате ASN.1 в кодировке DER. Файл предназначен для упрощения поиска нужного CRL по известному атрибуту имени издателя.
- 2 revokedCerts.crl — бинарный файл. Хранит CRL в кодировке DER.

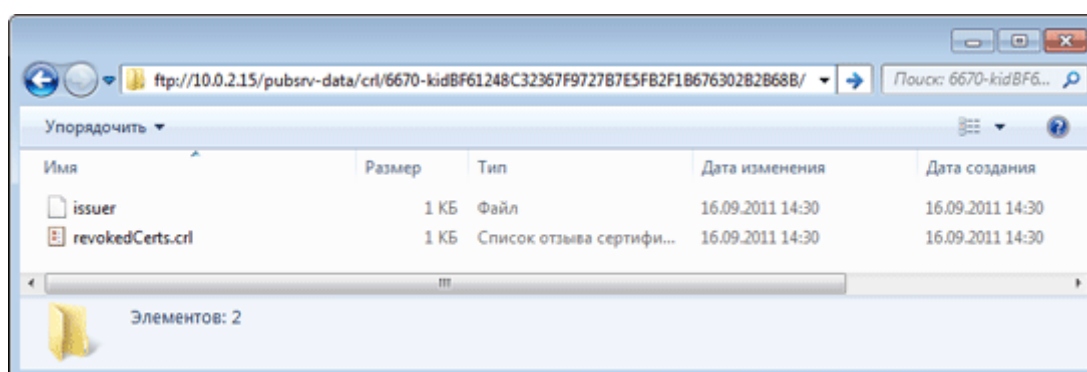


Рисунок 6. Структура хранения CRL сетей ViPNet на FTP-сервере

Списки аннулированных сертификатов сторонних сетей

При размещении CRL сторонних сетей на FTP-сервере имя каталога формируется следующим образом:

Имя каталога = IssuerDisplayName + дефис + "kid" + Шестнадцатиричное представление идентификатора.

IssuerDisplayName строится на основе одного из predetermined атрибутов имени издателя по следующему правилу: если в имени задан CN, то IssuerDisplayName = CN. Иначе, если в имени задан Pseudonym, то IssuerDisplayName = Pseudonym. Далее, аналогично для атрибутов: OU и O.

Пример: AtlasNW-App CA-kidBE5FB4BC7096CC236CBFD60909851345CCA43B39

Внутри каталога размещаются файлы с именами:

- 1 issuer — бинарный файл. Хранит имя издателя в формате ASN.1 в кодировке DER. Файл предназначен для упрощения поиска нужного CRL по известному атрибуту имени издателя.
- 2 revokedCerts.crl — бинарный файл. Хранит CRL в кодировке DER.

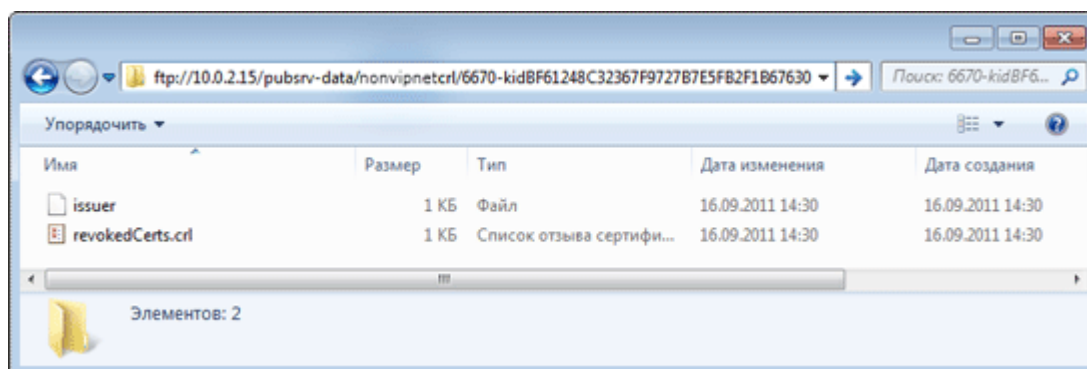


Рисунок 7. Структура хранения CRL сторонних сетей



Глоссарий

Active Directory (AD)

Служба каталогов, разработанная Microsoft для доменных сетей Windows. Эта служба интегрирована в большинство операционных систем Windows Server.

Active Directory является центром администрирования и обеспечения безопасности сети. Она служит для аутентификации и авторизации всех пользователей и компьютеров внутри сети доменного типа Windows. При помощи Active Directory задаются и применяются политики безопасности для всех компьютеров в сети, а также устанавливается или обновляется программное обеспечение на компьютерах сети. Active Directory хранит данные и настройки среды в централизованной базе данных.

AD LDS (Active Directory Lightweight Directory Services)

Служба Active Directory облегченного доступа к каталогам, работающая под управлением операционной системы Microsoft Windows Server 2008, Windows Server 2012.

Authority Key Identifier (идентификатор ключа центра сертификатов)

Данный параметр является информационным дополнением сертификата и его указание необязательно. Может принимать одно из значений:

- идентификатор ключа проверки электронной подписи издателя;
- серийный номер сертификата издателя плюс имя издателя.

Выбранный способ формирования этого параметра не рекомендуется изменять, пока действителен сертификат издателя, выпускающего списки аннулированных сертификатов (CRL) с данным параметром. Это обусловлено тем, что значение расширения отчасти определяет URL, по которому будет доступен опубликованный CRL.

FTP (File Transfer Protocol)

Стандартный протокол прикладного уровня для передачи файлов в компьютерных сетях. FTP позволяет подключаться к серверам FTP, просматривать содержимое каталогов и загружать файлы с сервера или на сервер.

LDAP (Lightweight Directory Access Protocol)

Упрощённая версия протокола доступа к каталогу стандарта X.500. LDAP является основным протоколом, используемым для доступа к Active Directory и AD LDS.

ViPNet Administrator

Набор программного обеспечения для администрирования сети ViPNet, включающий в себя серверное и клиентское приложения ViPNet Центр управления сетью, а также программу ViPNet Удостоверяющий и ключевой центр.

ViPNet Удостоверяющий и ключевой центр (УКЦ)

Программа, входящая в состав программного обеспечения ViPNet Administrator. Администратор УКЦ формирует и обновляет ключи для сетевых узлов ViPNet, а также управляет сертификатами и списками аннулированных сертификатов.

Контейнер

Объект службы каталогов (Active Directory, AD LDS) который может содержать в себе другие объекты.

Обновления, выпущенные в удостоверяющем центре «Верба-сертификат МВ»

Представляют собой файл в формате *.pse, который содержит сертификат издателя и актуальный список аннулированных сертификатов (CRL). Также pse-файл может содержать только сертификат издателя или только CRL.

Сервис публикации

ViPNet Publication Service. Программа, которая описывается в данном документе.

Сертификат издателя

Сертификат удостоверяющего центра, которым заверяются издаваемые сертификаты.

Список аннулированных сертификатов (CRL)

Список сертификатов, которые до истечения срока их действия были аннулированы или приостановлены администратором Удостоверяющего центра и потому недействительны на момент, указанный в данном списке аннулированных сертификатов.

Точка распространения данных

Источник, доступный по общеизвестным протоколам (например, HTTP или LDAP), используемый для размещения сформированной в удостоверяющем центре информации (сертификатов издателей и списков аннулированных сертификатов).