Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
Информатики и радиоэлектроники

УДК 004.428.4

Анохина
Александра Евгеньевна

РЕПОЗИТОРИЙ СЕРТИФИКАТОВ ОТКРЫТОГО КЛЮЧА И АТРИБУТНЫХ СЕРТИФИКАТОВ НА ОСНОВЕ СЛУЖБЫ КАТАЛОГОВ LDAP

АВТОРЕФЕРАТ
на соискание степени магистра информатики и вычислительной техники

по специальности 1-40 81 01 Информатика и технологии разработки программного обеспечения

Научный руководитель

Сиротко Сергей Иванович

Кандидат физ.-мат. наук, доцент

Библиотека БГУИР

Минск 2018

КРАТКОЕ ВВЕДЕНИЕ

Инфраструктура открытых ключей решает такие важные задачи, как обеспечение конфиденциальности информации, обеспечение целостности информации, обеспечение аутентификации пользователей и используемых ими ресурсов, обеспечение возможности подтверждения совершенных пользователями действий с информацией.

Одним из ключевых понятий ИОК является электронная цифровая подпись (ЭЦП). Без ЭЦП не возможен электронный документооборот, целостность и конфиденциальность цифровой информации.

Сертификат открытого ключа – это данные пользователя и его открытый ключ, скреплённые электронной подписью удостоверяющего центра. Выпуская сертификат открытого ключа, удостоверяющий центр тем самым подтверждает, что лицо, поименованное в сертификате, владеет закрытым ключом, который соответствует этому открытому ключу.

Атрибутный сертификат связывает атрибуты прав доступа с владельцем сертификата. Поскольку атрибутный сертификат не содержит открытого ключа, то его используют вместе с сертификатом открытого ключа. Аутентификация субъекта осуществляется при помощи сертификата открытого ключа, а связывание атрибутов с данным субъектом – посредством атрибутного сертификата. Атрибутные сертификаты позволяют управлять доступом на основе определенных принципов, ролей, должностей.

Важно разработать удобное и надежное место хранения сертификатов, а также оптимальные способы работы с хранилищем.

Хранилище данных представляет собой банк данных определенной структуры. Главное назначение хранилища – обеспечивать быстрое выполнение произвольных аналитических запросов.

Каталоги, как правило, содержат статические и редко изменяемые элементы, так как каталоги изначально оптимизированы для очень быстрого отклика на запросы поиска и чтения данных.

Каталоги являются очень специфическими системами хранения данных. Их удобно использовать для иерархически скомпонованных объектов. Каталоги могут быть реплицированы между несколькими серверами для удобного доступа и распределения нагрузки. Текстовая информация очень хорошо подходит для каталогов, так как легко поддается поиску, но данные могут быть представлены и в любой другой форме.

Очень удобно использовать каталоги для управления пользовательскими аккаунтами, машинами, схемами доступа, приложениями и многим другим, поскольку механизмы управления чаще всего только считывают данные из

Библиотека БГУИР

центрального хранилища. В то же время каталоги очень гибко настраиваются для любого уровня контроля доступа, позволяя ограничивать доступ к информации разными способами.

Каталоги часто используются для хранения информации о пользователях или реальных объектах.

LDAP – это протокол, определяющий методы, посредством которых осуществляется доступ к данным каталога. Он также определяет и описывает, как данные представлены в службе каталогов. Наконец, он определяет, каким образом данные загружаются (импортируются) и выгружаются (экспортируются) из службы каталогов.

LDAP характеризуется как сервис "один раз записал – много раз прочитал". Другими словами, от данных, обычно хранящихся в каталоге LDAP, не ожидается, чтобы они менялись при каждом доступе.

Данная работа исследует способы организации хранилищ данных, определяет наиболее подходящий вариант для хранения сертификатов и описывает разработанное программное средство для работы с репозиторием сертификатов открытого ключа и атрибутных сертификатов на основе каталога LDAP.

Библиотека БГУИР

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Цель и задачи исследования.

Целью исследования является нахождение новых путей для организации репозитория сертификатов открытого ключа и атрибутных сертификатов и работы с ним.

Задачами исследования являются изучение данной предметной области, определение оптимального метода создания и работы с репозиторием сертификатов, разработка программного средства, обеспечивающего работу с репозиторием сертификатов.

Объектом исследования является репозиторий сертификатов. Предметом исследования – способы организации репозиториев.

Новизна полученных результатов.

Новизна способа организации репозитория сертификатов. Улучшение характеристик работы с сертификатами.

Разработанное программное средство не имеет общедоступных аналогов в Беларуси.

Положения, выносимые на защиту:

– краткий обзор предметной области;

– способы организации хранения данных, каталоги LDAP;

– разработанное программное средство, его архитектура, характеристики и область применения.

Апробация результатов диссертации.

На конференциях работа не была представлена.

Опубликованность результатов исследования.

Результаты работы не были опубликованы.

Структура и объем диссертации.

Диссертация имеет следующую структуру:

– перечень условных обозначений и терминов ;

– введение;

– глава 1 «Обзор предметной области»;

– глава 2 «Хранение данных»;

– глава 3 «Разработка программного обеспечения»;

Библиотека БГУИР

– заключение;

– список использованной литературы.

Объем диссертации –75 страниц, из них 15 иллюстраций, 1 таблица, 1 приложение (25 страниц).

Использовано 13 библиографических источников.

Библиотека БГУИР

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Основная часть работы состоит из 3 глав.

В первой главе представлен обзор предметной области, источников литературы по теме диссертации. Рассматриваются такие понятия, как инфраструктура открытых ключей, инфраструктура управления привилегий, протокол LDAP. Таким образом, закладывается основа для определения структуры хранимых данных, организации их хранения. Востребованность и новизна работы заключается в том, что общедоступных аналогов данного комплекса программных средств в Беларуси нет.

Вторая глава описывает типы хранилищ данных: файлы, базы данных, хранилища, каталоги. На основании анализа делается выбор в пользу LDAP, что обусловлено следующими причинами:

– данные, которые планируется хранить, будут редко изменяться;
– приоритетная операция чтения данных;
– LDAP – упрощенный вариант каталогов X.500;
– удобные средства работы с LDAP-серверами.

Третья глава содержит информацию о средствах разработки программного обеспечения, описывает разработанное программное средство, демонстрирует его работу, приводит основные характеристики. Результаты тестирования и экспериментов с разработанными программными средствами позволяют сделать вывод об его эффективности.

Библиотека БГУИР

ЗАКЛЮЧЕНИЕ

В рамках данной работы изучена предметная область инфраструктуры открытых ключей и инфраструктуры привилегий, рассмотрены виды хранилищ данных, разработано программное средство, позволяющее создавать репозиторий сертификатов и работать с ним.

Служба каталогов LDAP является оптимальным вариантом для реализации поставленной задачи. Основания для данного выбора:

– данные, которые планируется хранить, будут редко изменяться;

– приоритетная операция чтения данных;

– удобные средства работы с LDAP-серверами.

Разработанное программное средство представляет собой библиотеку и приложение, демонстрирующее функции библиотеки. Библиотека является кросплатформенной, лекго может использоваться в прикладных проектах. Также подготовлен комплект документов на данную библиотку.

Репозиторий может использоваться для хранения сертификатов открытых ключей и атрибутных сертификатов.

Сертификат открытого ключа позволяют подтвердить подлинность владельца ключа. Атрибутный сертификат связывает атрибуты прав доступа с владельцем сертификата.

Данное программное средство разработано согласно с требованиями и целями предприятия, внедрено в ЗАО "НТЦ Контакт" и пригодно к дальнейшему использованию.

Библиотека БГУИР