Литература

1. *Rabiner L.* A Tutorial on Hidden Markov Models and Selected Applications in Speech Recognition // IEEE Press. 1988. С. 257–286.
2. *Young S., Evermann G., Gales M., Hain T., Kershaw D., Liu X., Moore G., Odell J., Ollason D., Valtchev V.* / The HTK Book (for HTK Version 3.4). 2006.
3. *Wessel F., Schluter R., Macherey K., Ney H.* Confidence Measures for Large Vocabulary Continuous Speech Recognition // IEEE Transactions on Speech and Audio Processing. 2001. Вып. 3. гл. 9.

СОЗДАНИЕ ЦЕНТРА АУТЕНТИФИКАЦИИ И АВТОРИЗАЦИИ ПОЛЬЗОВАТЕЛЕЙ В ГРИД-СЕТЯХ НА ОСНОВЕ ПАКЕТА UNICORE

Р. М. Томашевский, Н. В. Серикова

ВВЕДЕНИЕ

ГРИД – согласованная, открытая и стандартизованная среда, которая обеспечивает гибкое, безопасное, скоординированное разделение ресурсов в рамках виртуальной организации.

На основе технологии ГРИД осуществляется интегрирование региональных и даже национальных вычислительных компьютерных центров для создания объединенных интернациональных ресурсов, предназначенных для решения крупных научно-технических задач. В ГРИД предполагается интегрирование больших объемов географически удаленных компьютерных ресурсов.

Наряду с проблемой объединения компьютеров в единую ГРИД-сеть, существуют проблемы обеспечения информационной безопасности при использовании ГРИД-сетей, разнесенных на большие расстояния. Становится острым вопрос обеспечения конфиденциальности и целостности данных [1]. Необходимо также решать вопросы аутентификации и авторизации пользователей для выделения им полномочий на использование ресурсов других университетов и организаций. Решением этих вопросов является создание центра выдачи сертификатов, который будет являться гарантом соблюдения правил информационной безопасности.

UNICORE – ОСНОВА ПОСТРОЕНИЯ ГРИД-СЕТИ ФАКУЛЬТЕТА РАДИОФИЗИКИ И ЭЛЕКТРОНИКИ

Для создания ГРИД-сети факультета радиофизики и электроники использовался программный пакет промежуточного уровня UNICORE [2]. UNICORE – одна из немногих оригинальных платформ, которая не использовала Globus Toolkit [3].

UNICORE (UNiform Interface to COmputing REsources) предоставляет ученым и инженерам ресурсы суперкомпьютерных центров, объединенных в ГРИД, и делает их доступными через Интернет. Выигрыш, который получает пользователь UNICORE – однородный доступ к разного рода системам.

UNICORE дает возможность пользователю подготовить или изменить задание с использованием графического интерфейса на рабочей станции с платформой Unix или Windows. Задания могут быть запущены на любую из платформ UNICORE ГРИД, и далее пользователь может осуществлять мониторинг и управление запущенными заданиями, используя часть интерфейса, называемую монитором заданий.

Для каждого задания, пользователь определяет нужную исполнительную систему и требования к ресурсам для каждой задачи. Пользовательский интерфейс проверяет, могут ли ресурсные запросы быть удовлетворены исполнительной системой, и разрешает запуск только в том случае, если запрос действительно может быть выполнен. Чтобы перезапустить задание на другой системе, пользователь просто меняет исполнительную систему.

UNICORE состоит из следующих основных компонент:

- шлюз (Gateway) аутентифицирует запросы на связь, используя сертификаты приложений и серверов;
- интерфейс целевой системы TSI осуществляет запуск задачи на целевой системе от имени пользователя;
- UNICORE/X запрашивает данные XUUDB для авторизации пользователя и транслирует абстрактные задания и ресурсные запросы в зависящие от платформы команды и опции. Затем задания передаются в TSI на выполнение;
- база данных XUUDB содержит таблицы пользовательских сертификатов и их логины, а также управляет доступом к ресурсам UNICORE.

Центр выдачи сертификатов, отвечающий за выдачу сертификатов пользователям для доступа к ресурсам ГРИД, в UNICORE не реализован. UNICORE поставляется с демо-версией сертификатов, которые необходимы только для первичной настройки ГРИД-сети. Для дальнейшего использования UNICORE сертификаты служб должны быть заменены.

СОЗДАНИЕ ЦЕНТРА ВЫДАЧИ СЕРТИФИКАТОВ ФАКУЛЬТЕТА РАДИОФИЗИКИ И ЭЛЕКТРОНИКИ

Сертификаты в ГРИД имеют строгий, определенно заданный формат, структура которого регламентируется форматом X.509. Формат X.509

тесно связан с инфраструктурой открытых ключей (PKI – Public Key Infrastructure), в рамках которой сертификаты данного формата применяются [4, 5].

Центр выдачи сертификатов – это компонент ГРИД-сети, отвечающий за управление криптографическими ключами пользователей. Открытые ключи и другая информация о пользователях хранится центрами сертификации в виде цифровых сертификатов формата X.509.

Центр выдачи сертификатов выполняет следующие функции:

1. регистрирует электронные цифровые подписи;
2. создает по обращению пользователей закрытые и открытые ключи ЭЦП;
3. приостанавливает и возобновляет действие сертификатов ключей подписей, а также аннулирует их;
4. ведет реестр сертификатов ключей подписей, обеспечивает актуальность реестра и возможность свободного доступа пользователей к реестру;
5. выдает сертификаты ключей подписей в виде электронных документов с информацией об их действительности.

Центр выдачи сертификатов факультета радиофизики и электроники состоит из двух частей:

- отдельного клиентского модуля для генерации запроса на сертификат;
- web-интерфейса серверной части для подписи пользовательского сертификата.

Клиентская часть центра выдачи сертификатов была реализована в виде отдельного модуля, написанного на языке программирования Java с использованием криптографических библиотек [6,7]. Клиентская часть центра выдачи сертификатов получила название RFE Key Store 1.0. Интерфейс программы RFE Key Store приведен на рис. 1.

Клиентская часть центра выдачи сертификатов позволяет пользователю:

- создать хранилище для пары закрытый/открытый ключ и сертификата пользователя в формате jks (стандартный тип хранилища для хранения ключей и сертификатов в пакете UNICORE;
- сгенерировать пару открытый/закрытый ключ длиной 2048 бит;
- создать запрос на сертификат в формате X.509;
- экспортировать запрос на сертификат для подписи в центр сертификации;
- импортировать подписанный сертификат в хранилище пользователя для дальнейшего использования в составе пакета UNICORE.

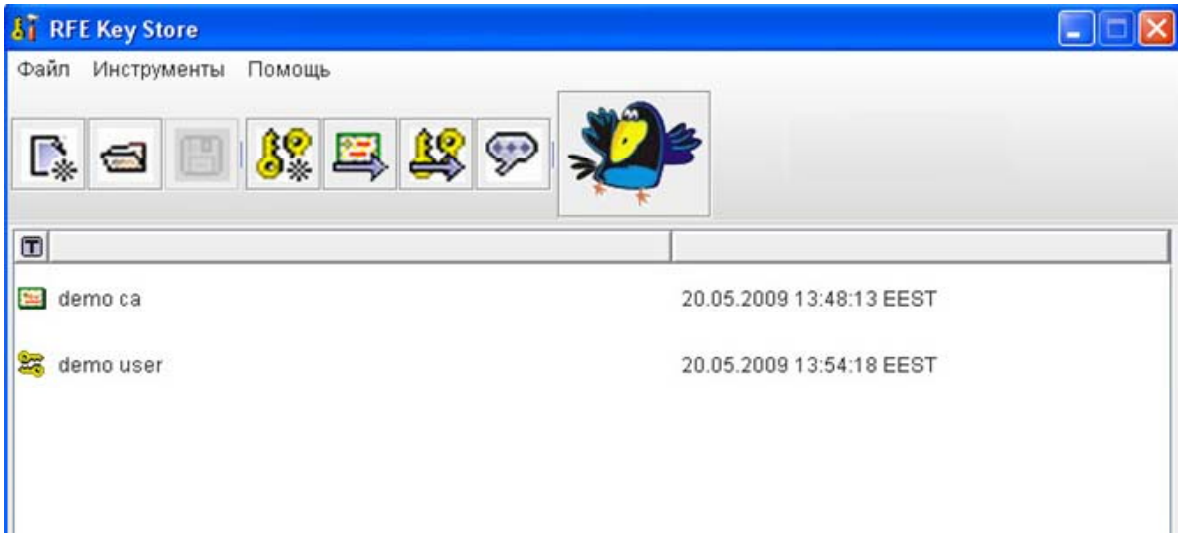

Рис.1. Интерфейс программы RFE Key Store

Серверная часть центра выдачи сертификатов, также как и клиентская, была разработана на языке Java. Однако, в отличие от клиентской, была реализована в виде web-интерфейса для обеспечения доступа к ней из любой точки локальной сети, что значительно упрощает получение сертификата на допуск в ГРИД для пользователя. Серверная часть центра выдачи сертификатов получила название RFE DEMO CA.

К web-интерфейсу RFE DEMO CA можно подключиться двумя способами: как пользователь (для отправки запроса на сертификат), и как администратор, введя соответствующий логин и пароль.

При работе с web-сайтом пользователь может отправить запрос на сертификат, просмотреть списки выданных и отозванных сертификатов, получить более подробную информацию о том, как нужно генерировать запрос на сертификат. Пользователю также доступна полная инструкция с описанием шагов действия для получения допуска к ресурсам ГРИД.

Администратор может:

- подписать или нет сертификат пользователя, тем самым разрешить или запретить пользователю использовать ресурсы ГРИД-сети;
- отправить пользователю письмо, в котором указано был ли его сертификат одобрен или нет, а также полномочия и сроки действия сертификата пользователя;
- отозвать сертификат пользователя, при этом сертификат пользователя будет перемещен в список отозванных сертификатов;
- просмотреть все выданные или отозванные сертификаты;
- при необходимости продлить время действия того или иного сертификата.

Литература

1. *Таненбаум Э.* Компьютерные сети. 4-ое издание. Питер, 2003.
2. Интернет-адрес: www.unicore.eu
3. *Томашевский Р. М., Серикова Н. В.* Реализация GRID-сети под управлением ОС WINDOWS // Сборник работ 65-й науч. конф. студентов и аспирантов БГУ. Минск, 2008. С. 154–157.
4. *Шнайер Б.* Прикладная криптография. 2-е издание. 1995.
5. Интернет-адрес: www.securityportal.ru
6. *Ноутон П., Шилдт Г.* Java 2. Петербург, 2006.
7. Интернет-адрес: www.bouncycastle.org.

СИСТЕМА ПЕРЕДАЧИ ЭЛЕКТРОПИТАНИЯ ПО ОДНОМОДОВОМУ ОПТИЧЕСКОМУ ВОЛОКНУ

Р. А. Федоров, А. Л. Чиж, С. А. Малышев

ВВЕДЕНИЕ

Использование оптоволокна для приема/передачи информации от различных датчиков или удаленных приемопередающих модулей требует также прокладки медного кабеля для обеспечения их электропитания.

Эта технология дороже передачи электропитания по металлическим кабелям, но в некоторых приложениях ее применение может быть оправдано. Например, в системах с повышенным уровнем электромагнитных помех или в системах с агрессивными и взрывоопасными средами, где требуется обеспечить пожаро- и взрывобезопасность от искрения контактов и необходимо защищать металлические проводники от взаимодействия с компонентами среды. Системы передачи электропитания по оптоволокну очень важны в медицинском диагностическом оборудовании при осуществлении различного рода исследований, где используют зондирование организма человека. Возможно применение оптоволокна для обеспечения электропитанием распределенных датчиков в бортовой аппаратуре, при этом достигается значительное улучшение массогабаритных характеристик. Данная технология может использоваться также в различных системах, где технологически нет места для прокладки дополнительного кабеля питания, или его прокладка связана с большими материальными затратами (оборудование в шахтах, видеокамеры наблюдения).

1. АНАЛИЗ КОМПОНЕНТОВ СИСТЕМЫ И ЕЕ ФУНДАМЕНТАЛЬНЫЕ ОГРАНИЧЕНИЯ И ХАРАКТЕРИСТИКИ

В общем случае волоконно-оптическая система передачи состоит из удаленного и центрального модулей. Стандартная система (рис. 1а) со-