ПЕРСОНАЛЬНЫЕ И СЕРВИСНЫЕ СЕРТИФИКАТЫ ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ГРИД-СЕТЯХ

Р. М. Томашевский, Н. В. Серикова

ВВЕДЕНИЕ

ГРИД-структуры объединяют автономные системы – от персональных компьютеров до суперкомпьютеров. Они дают компаниям и разработчикам возможность совместно использовать процессорные ресурсы и данные, невзирая на географические границы и принадлежность к той или иной организации. Соответствующая технология позволяет преобразовывать вычислительную инфраструктуру в интегрированную повсеместную виртуальную среду.

ГРИД – согласованная, открытая и стандартизованная среда, которая обеспечивает гибкое, безопасное, скоординированное разделение ресурсов в рамках виртуальной организации [1].

Использование ГРИД-технологий позволяет: организовать эффективное использование ресурсов для небольших заданий, с утилизацией временно простаивающих компьютерных ресурсов; осуществлять распределенные супервычисления, для решения сложных задач, которые требуют огромных процессорных ресурсов и памяти.

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 [2]. Необходимо также решать вопросы аутентификации и авторизации пользователей для выделения им полномочий на использование ресурсов других университетов и организаций. Решение этих вопросов основано на использовании персональных и сервисных сертификатов, выдачу которых осуществляет центр выдачи сертификатов, который и является гарантом соблюдения правил информационной безопасности в ГРИД-сетях.

СТРУКТУРА И ПРИНЦИПЫ ФУНКЦИОНИРОВАНИЯ ЦЕНТРА ВЫДАЧИ ПЕРСОНАЛЬНЫХ И СЕРВИСНЫХ СЕРТИФИКАТОВ

Центр выдачи персональных и сервисных сертификатов (центр сертификации) – это компонент ГРИД-сети, отвечающий за управление криптографическими ключами пользователей и служб. Информация о службах

ГРИД-сети хранится в виде сервисных сертификатов. Открытые ключи и другая информация о пользователях хранится центрами сертификации в виде цифровых персональных сертификатов формата X.509 [3].

Сервисные сертификаты необходимы для аутентификации служб ГРИД-сети между собой и их корректной работы. Персональные сертификаты пользователей используются для авторизации пользователей в ГРИД-сети и запуск заданий в этой сети от имени пользователя.

Центр выдачи сертификатов выполняет следующие функции:

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

Центр выдачи сертификатов решает проблемы связанные с авторизацией пользователей в ГРИД-сетях. Подписывая электронный сертификат пользователя, центр сертификации, тем самым, дает пользователю набор прав на использование ГРИД. Выдавая полномочия на использование ресурсов ГРИД-сети только тем пользователям, которые имеют на это разрешение, центр выдачи сертификатов решает вопросы, связанные с обеспечением конфиденциальности и целостности данных. Неавторизованный пользователь не может получить доступ к службам ГРИД и нарушить их функционирование. Таким образом, допуск к ГРИД получают только пользователи с определенным набором прав.

ГРИД-СЕТЬ ФАКУЛЬТЕТА РАДИОФИЗИКИ И ЭЛЕКТРОНИКИ

Для создания ГРИД-сети факультета Радиофизики и Электроники использовался программный пакет промежуточного уровня UNICORE [4]. Платформа UNICORE написана на языке Java, что обеспечивает межплатформенную переносимость и совместимость с различными операционными системами. Выигрыш, который получает пользователь UNICORE – однородный доступ к разного рода системам, а значит и больше возможностей по получению ресурсов.

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 при помощи центра выдачи персональных и сервисных сертификатов.

Центр выдачи персональных и сервисных сертификатов факультета Радиофизики и Электроники состоит из двух частей:

•отдельного клиентского модуля для генерации запроса на сертификат;

•web-интерфейса серверной части для подписи сертификата.

Клиентская часть центра выдачи сертификатов была реализована в виде отдельного модуля, написанного на языке программирования Java с использованием криптографических библиотек [5]. Клиентская часть центра выдачи сертификатов позволяет пользователю:

•создать хранилище для пары закрытый/открытый ключ и сертификата в формате jks (стандартный тип хранилища для хранения ключей и сертификатов в пакете UNICORE);

•сгенерировать пару открытый/закрытый ключ длиной 1024 бит;

•создать запрос на сертификат в формате X.509;

•экспортировать запрос на сертификат для подписи в центр сертификации;

•импортировать подписанный сертификат в хранилище для дальнейшего использования в составе пакета UNICORE.

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.

К web-интерфейсу 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.

Администратору, в отличие от пользователя, доступен гораздо больший функционал. Администратор может:

- подписать или нет сертификат пользователя, тем самым разрешить или запретить пользователю использовать ресурсы ГРИД-сети;
- 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. Foster I., Kesselman C., Tuecke S. The Anatomy of the Grid: Enabling Scalable Virtual Organizations // International J. of Supercomputer Applications and High Performance Computing. -2001. - T. 15, No 3. -P. 200-222.
7. Таненбаум Э. Компьютерные сети. 4-ое издание. Питер, 2003.
8. Шнайер Б. Прикладная криптография. 2-е издание-1995
9. Интернет-адрес: www.unicore.eu/documentation
10. Интернет-адрес: www.bouncycastle.org

АНАЛИЗ И МОДЕЛИРОВАНИЕ ДАННЫХ ИНЕРЦИАЛЬНОГО КОМПЛЕКСА ОРИЕНТАЦИИ И НАВИГАЦИИ

М. А. Чертков, Л. В. Калацкая

ВВЕДЕНИЕ

Современные достижения в области информационных технологий существенно расширяют возможности подвижных объектов различного назначения. Значительную роль в этом процессе играет решение задач ориентации и навигации объектов. Системы, решающие эти задачи, объединяются в информационно-управляющие комплексы ориентации и навигации (КОН) [1].

Как правило, в роли устройств определения местоположения в пространстве выступают инерциальная и спутниковая системы навигации [2-3]. Важно учесть в этом случае способы хранения и алгоритмы обработки