Хухлаев Е.В.

БЕЗОПАСНОСТЬ ГРИД-ДИСПЕТЧЕРА, РЕАЛИЗОВАННАЯ СРЕДСТВАМИ ГРИД-СЛУЖБ*

Институт прикладной математики им. М.В.Келдыша РАН; Россия, 125047, Москва, Миусская пл. 4; тел. (095)250-78-15, e-mail: huh@keldysh.ru

Представлено на международную конференцию
«Распределенные вычисления и Грид-технологии
в науке и образовании»
29 июня - 2 июля 2004 г.
г.Дубна, Россия

1. Введение. Концепция среды распределенных вычислений Грид (Grid) [1, 2] становится все более популярной, позволяя потенциально получить из географически распределенных ресурсов за счет программных решений и с помощью коммерческого сетевого оборудования очень большие вычислительные мощности, намного превосходящие те, которыми располагают современные суперкомпьютерные архитектуры.

Нами разрабатывается система централизованного управления заданиями в Грид, которую мы называем Грид-диспетчером. Роль и место Грид-диспетчера в контексте задачи организации распределенных вычислений подробно рассмотрены в статье [3] (в этой статье Грид-диспетчер именуется Метадиспетчером).

Проект Грид-диспетчера исходит из представления о Грид как о совокупности узлов. Узел – группа компьютеров (в локальной сети), находящаяся под управлением локального монитора ресурсов, в качестве которого используются различные системы управления пакетной обработкой (СУПО) [4]. Совокупность узлов в Грид объединена некоторой общей информационной инфраструктурой, позволяющей планировать размещение заданий на вычислительных ресурсах узлов Грид. Однако каждый узел обладает автономией и предоставляет в распоряжение Грид только ту часть своих вычислительных ресурсов и на таких условиях, которые приемлемы для управляющей этим узлом СУПО. Функциональность, предоставляемая пользователю Грид-диспетчером, близка к функциональности СУПО. По существу, Грид-диспетчер – это СУПО более высокого уровня (см. рис.1).

Грид-диспетчер реализуется средствами Globus Toolkit 3 (GT3) [5, 6, 7] как комплекс Грид-служб и клиентских компонент. Система Globus была выбрана в качестве базовой при разработке Грид-диспетчера, потому что (помимо всего прочего) она становится стандартом де-факто в Грид.

Помимо инструментария для подготовки собственных Грид-служб, реализующих стандартные интерфейсы, в состав GT3 входит ряд уже готовых Грид-служб, выполняющих запуск заданий в локальных СУПО (GRAM), безопасную и надежную передачу файлов (GridFTP), информационное обслуживание (MDS) и многое другое.

В работе кратко описывается функциональность и архитектура Грид-диспетчера (п.2) и рассмотрены вопросы безопасности в контексте реализации Грид-диспетчера средствами GT3 (п.4). В связи с этим изложена система безопасности GT3 (п.3).

* *Работа выполнена при поддержке Российского фонда фундаментальных исследований (проекты 02-01-00282, 04-07-90299).*

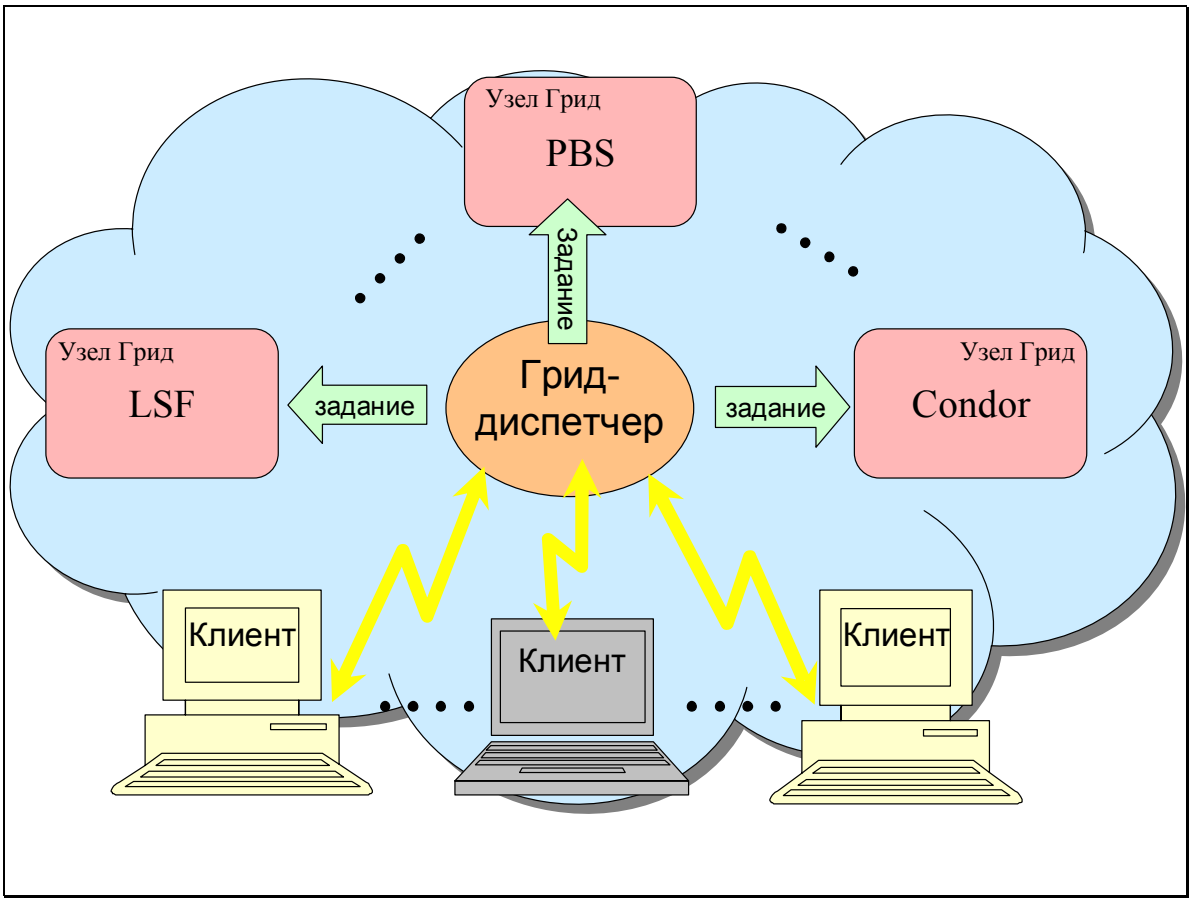

Рис.1. Грид-диспетчер в Грид

2. Функциональность и архитектура Грид-диспетчера. Функциональность Грид-диспетчера включает команды запуск задания (submit), получение информации о состоянии задания (status), снятие задания (cancel) и некоторые другие. Команда submit имеет на входе описание задания и возвращает ярлык задания, предъявляемый при вызове остальных команд управления.

Архитектура Грид-диспетчера показана на рис.2.

Грид-диспетчер состоит из планировщика и комплекса Грид-служб, выполняющихся на управляющем хосте Грид (хосте Грид-диспетчера), и клиентских компонент, выполняющихся на других хостах Грид. В комплекс входят:

- интерфейсная утилита (клиент GT3), направляющая запросы клиентов (пользователей и администраторов) Грид-диспетчеру;
- грид-служба приема запросов;
- ресурсный агент (клиент GT3), выполняющийся на каждом узле, и передающий информацию о ресурсах узла Грид-диспетчеру;
- ресурсная грид-служба, принимающая сообщения от агентов;
- управляющая компонента (клиент GT3), занимающаяся запуском заданий и управлением ими в узлах GT3 по командам планировщика.

Организация вычислительной сети Грид-диспетчера базируется на средствах GT3:

- На управляющем хосте Грид (хосте Грид-диспетчера) устанавливается сервер GT3, в рамках которого выполняются грид-службы Грид-диспетчера.
- В каждом узле Грид выделяется шлюзовой компьютер, на котором устанавливается сервер GT3. Грид-службы сервера обслуживают СУПО, управляющую узлом. Кроме того, на узле запускается ресурсный агент (клиент GT3), взаимодействующий с СУПО.

- На каждом клиентском хосте устанавливается инфраструктура GT3, достаточная для выполнения интерфейсной утилиты.

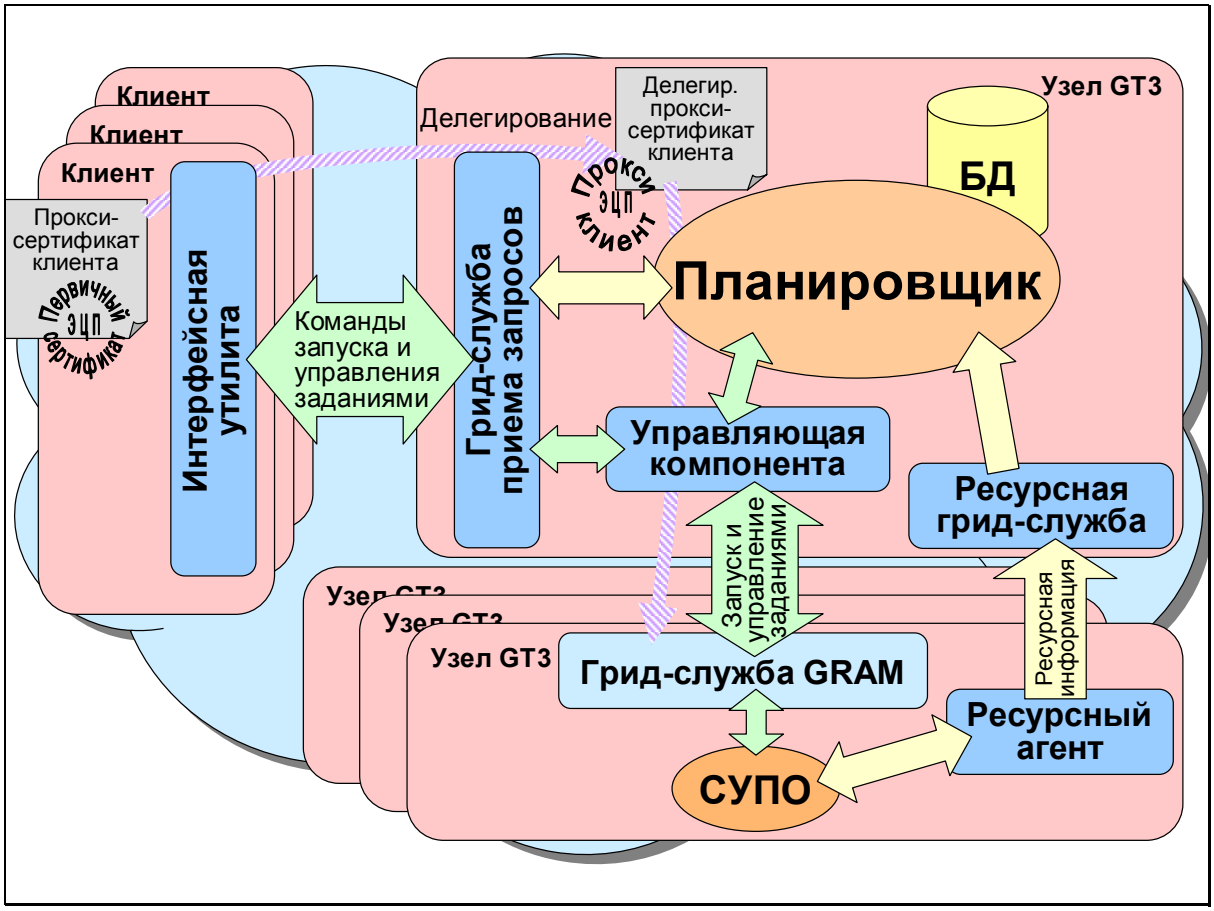

Рис. 2. Архитектура Грид-диспетчера

Центральной компонентой Грид-диспетчера является планировщик, к которому поступает вся информация от грид-служб. Планировщик, руководствуясь некоторой стратегией и полученной информацией о состоянии ресурсов и принятых заданиях, в определенные моменты времени направляет (с помощью управляющей компоненты) то или иное задание в выбранный целевой узел.

Вопросы стратегии планирования выходят за пределы настоящей работы. Некоторые подходы к этим вопросам рассмотрены в [8]. Далее (п. 4) мы осветим только проблемы безопасности грид-служб Грид-диспетчера. Предварительно необходимо привести некоторые сведения о системе безопасности GT3 GSI (Grid Security Infrastructure).

3. Система безопасности GT3. GT3 GSI [9] основана на PKI (инфраструктуре открытых ключей). Все участники вычислительной среды (пользователи, вычислительные процессы и ресурсы) владеют X.509 сертификатами открытых ключей (далее – сертификат или СОК), используемыми для аутентификации (выяснения «who is who»). В сертификате, подписанном ЭЦП удостоверяющего центра (Certificate Authority), что гарантирует его подлинность, указаны идентификатор владельца (как правило, собственное имя - distinguished name) и соответствующий открытый ключ (именно это связывает владельца с ключом), срок действия и назначение сертификата. Авторизация (предоставление участнику прав на доступ к ресурсам) выполняется в соответствии с результатами аутентификации и политики авторизации, принятой для данного ресурса.

Персональные сертификаты в формате X.509 выдаются на длительный срок в результате сложной и дорогостоящей процедуры установления личности субъекта. Применение СОК для аутентификации предполагает использование закрытого ключа пользователя, который обычно хранится в зашифрованном виде на системе пользователя и защищен паролем, который надо предъявлять при каждом его использовании.

Специфика выполнения заданий в Грид состоит в том, что задание, инициированное изначально пользователем (или другим заданием) требует подключения других ресурсов и входа в другие системы. Для устранения угрозы компрометации закрытого ключа пользователя необходимо обеспечить функцию единого входа (Single-Sign-On – однократного предъявления первичного закрытого ключа), исключающую передачу (пусть даже и безопасную) ключа на другие системы.

Для реализации функции единого входа в GT3 применяется безопасное делегирование прав (Delegation) на базе т.н. прокси-сертификата [10] (заместителя), действующего от имени владельца исходного сертификата.

3.1. Прокси-сертификат подписывается посредством первичного закрытого ключа или ключа другого прокси-сертификата. Прокси-сертификат имеет ограниченный срок действия (обычно не более 24 часа) и ограниченное (по сравнению с исходным) назначение сертификата. Тем самым прокси-сертификат ограничивает права его владельца, снижая угрозу безопасности.

Дополнительные расширения прокси-сертификата позволяют проследить всю цепочку сертификатов вплоть до исходного сертификата (см. рис. 3), что позволяет легко проверить его валидность. Закрытый ключ прокси-сертификата хранится незашифрованным. Поэтому прокси-сертификат пригоден для непосредственного использования в вычислительной среде Грид.

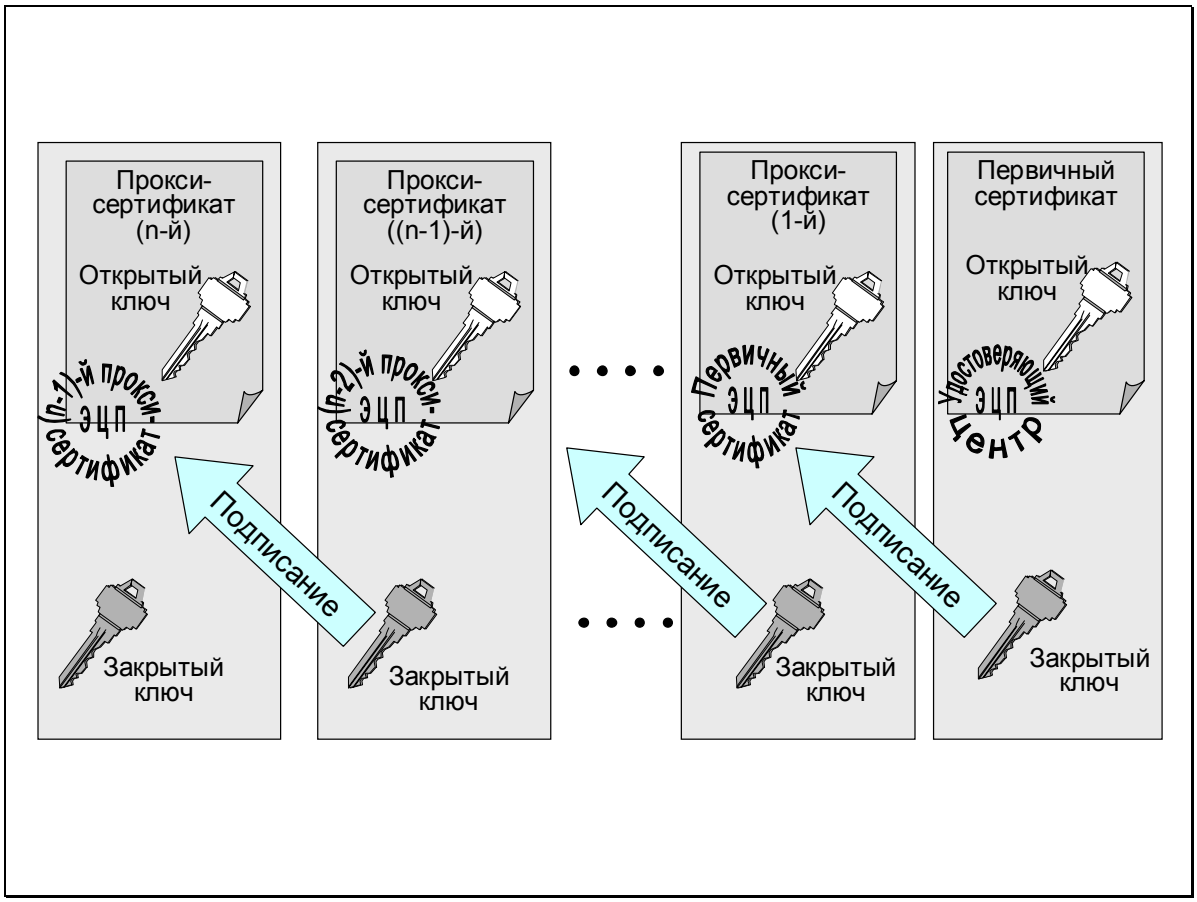

Рис. 3. Цепочка прокси-сертификатов

В GT3 прокси-сертификат пользователя (предъявляющего первичный закрытый ключ) выписывается стандартными средствами.

3.2. Делегирование [10] — передача части прав (определенных назначением сертификата) на ограниченный срок, необходимое для выполнения действий от имени участника (клиента) на другой вычислительной установке. Права подтверждаются владением сертификатом (т.е. соответствующим закрытым ключом). Делегирование заключается не в пересылке закрытого ключа (вместе с сертификатом), а в подписывании клиентом нового (делегированного) прокси-сертификата, который и применяется для выполнения действий от имени клиента (см. рис. 4).

В клиентской компоненте GT3 достаточно указать, какой вид делегирования (полноправное или ограниченное) применить. Грид-служба может получить делегированный сертификат и распоряжаться им.

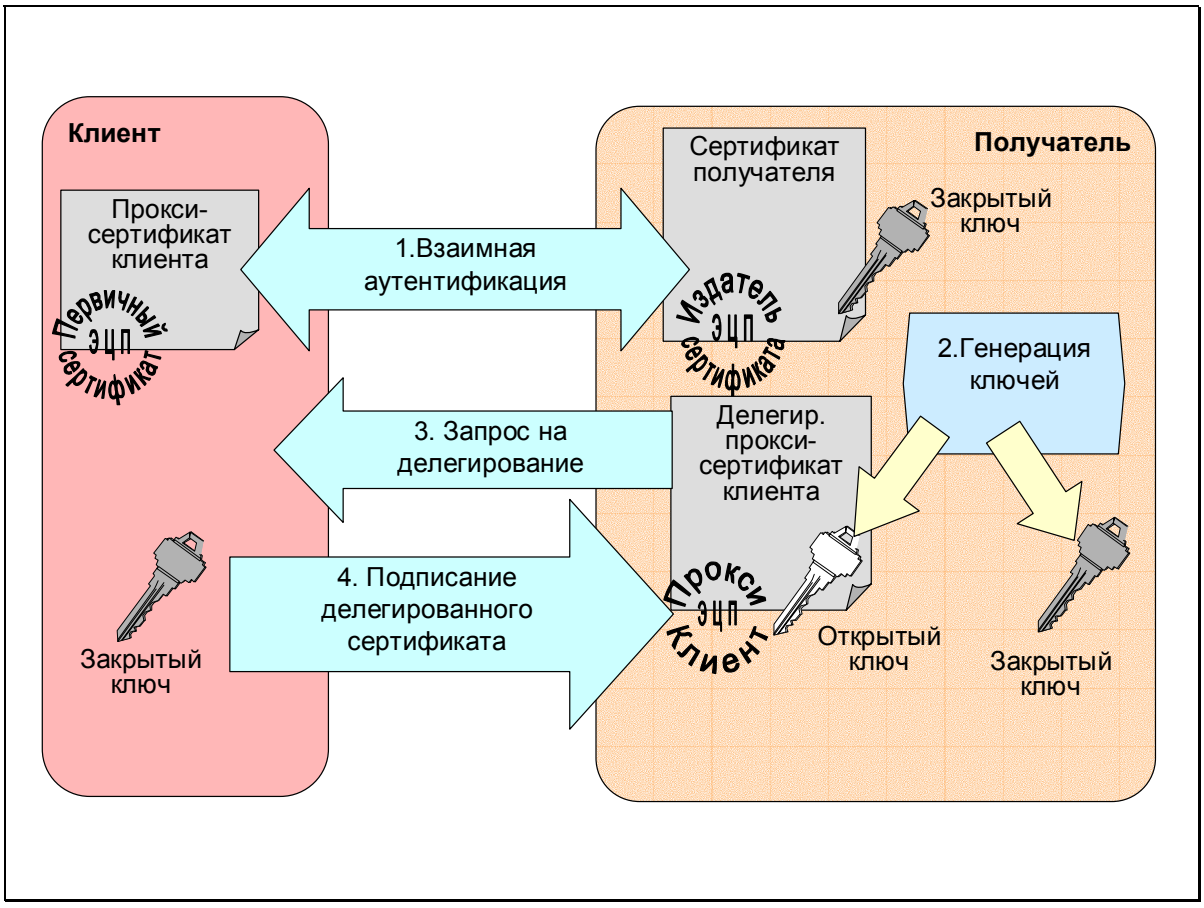

Рис. 4. Делегирование прав

3.3. GRIM-сертификаты. Чтобы снизить возможный ущерб от компрометации, серверные компоненты GT3 (например, контейнеры грид-служб) выполняются без привилегий системы. Таких компонент на одном сервере может быть, вообще говоря, несколько. Каждая из них для аутентификации должна владеть сертификатом. Нецелесообразно (долго и дорого), а иногда и невозможно, получать для каждой компоненты отдельный серверный сертификат. Поэтому в GT3 принят следующий подход: На сервере имеется единственный серверный сертификат, закрытый ключ которого доступен только системе. Любая компонента, выполняющаяся под несистемной учетной записью (account), может получить (посредством привилегированной утилиты GT3 globus-grim) GRIM-сертификат. Это – прокси-сертификат, подписанный закрытым ключом серверного сертификата, и

удостоверяющий, что его владелец имеет на данном сервере права данной учетной записи. В состав контейнера входит обработчик, обеспечивающий автоматическое обновление GRIM-сертификата по истечении срока действия.

3.4. Авторизационные файлы. В GT3 безопасный доступ к ресурсам управляется авторизационными файлами грид-служб, в которых перечислены различительные имена клиентов. Доступ к грид-службе получают только те клиенты, чье различительное имя (извлекаемое из предъявляемого сертификата) зарегистрировано в ее авторизационном файле. Каждому различительному имени соответствует в этом файле локальное имя, которое грид-служба может использовать для дальнейшей авторизации. В типовом случае – это имя локальной учетной записи пользователя (account), с правами которой выполняются процессы, запускаемые на сервере от имени клиента. Например, грид-служба запуска заданий GT3 GRAM запускает с этими правами персональный грид-контейнер (UHE – user host environment), грид-службы которого и занимаются безопасным обслуживанием всех заданий клиента.

4. Система безопасности Грид-диспетчера. Безопасность Грид-диспетчера достигается применением средств (утилит и API) системы безопасности GT3.

4.1. Аутентификация и делегирование.

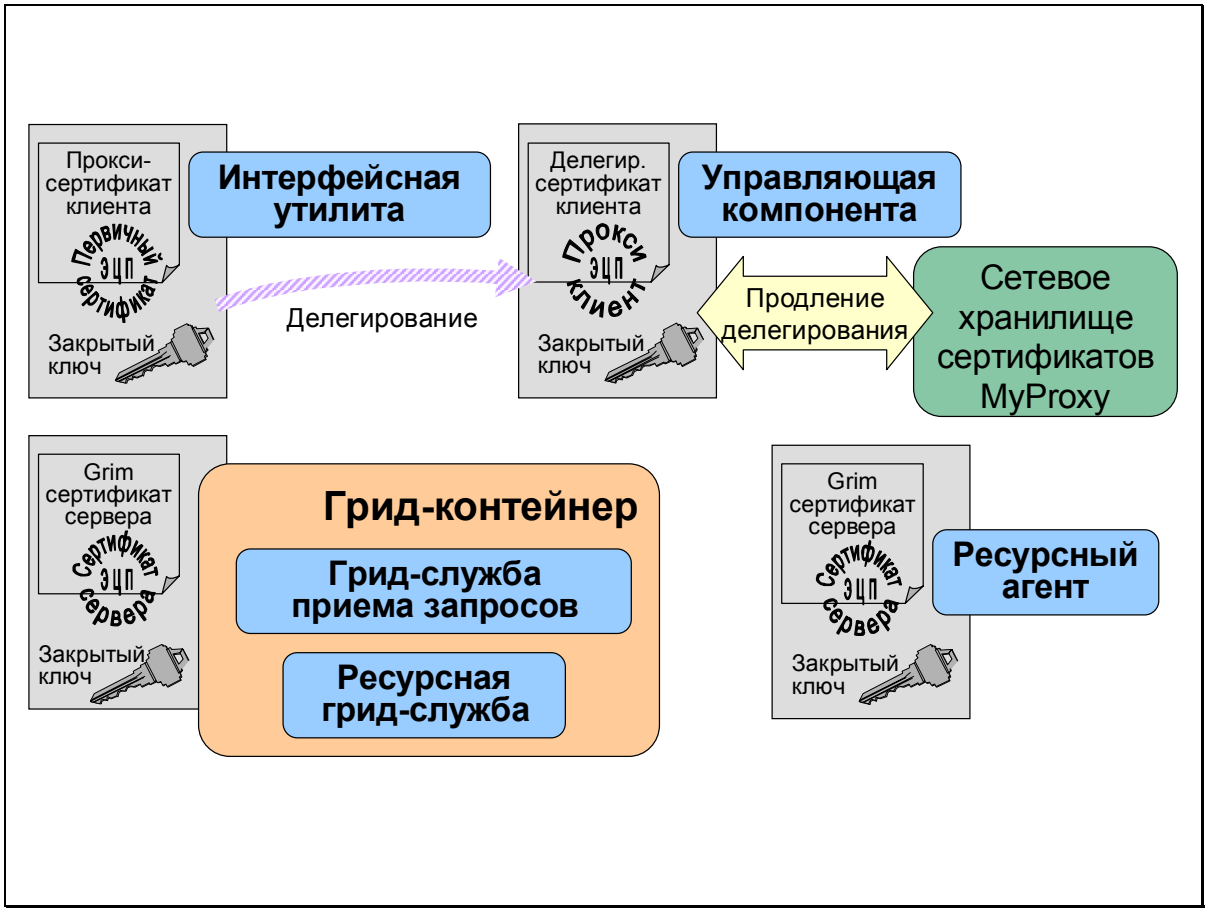

Рис.5. Аутентификация и делегирование в Грид-диспетчере

Для взаимной аутентификации каждая компонента должна предъявить X509 сертификат.

Интерфейсная утилита выполняется на установке клиента-пользователя и предъявляет стандартный прокси-сертификат клиента, делегируемый грид-службе приема запросов. Делегированный сертификат сохраняется в базе данных планирования, а при запуске и управлении заданием на целевом узле GT3 от имени

владельца задания предъявляется управляющей компонентой, как клиентом GT3. Использование сетевого хранилища сертификатов MyProxy [11] позволяет продлевать при необходимости срок делегирования без обращения к владельцу задания (см. рис.6).

Контейнер с грид-службами для аутентификации использует GRIM-сертификат.

Ресурсный агент, выполняющийся на узле GT3, также может воспользоваться GRIM-сертификатом.

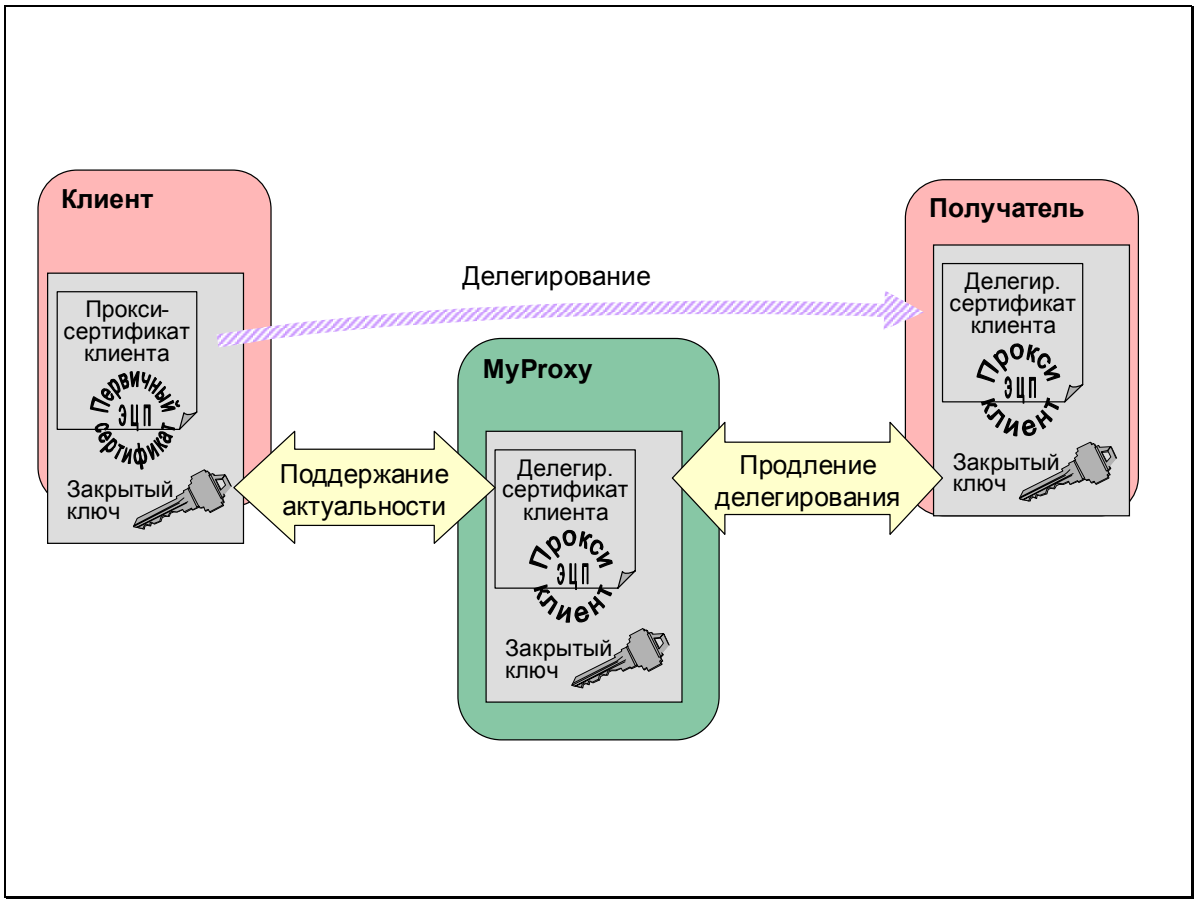

Рис.6. Сетевое хранилище сертификатов MyProxy

4.2. Авторизация. В авторизационном файле грид-службы приема запросов перечисляются различительные имена зарегистрированных клиентов Грид-диспетчера. Локальное имя интерпретируется грид-службой как роль клиента («пользователь» или «администратор»).

В авторизационном файле ресурсной грид-службы перечисляются различительные имена узлов, обслуживаемых Грид-диспетчером, а соответствующие локальные имена идентифицируют узлы в базе данных планирования.

Авторизационные файлы грид-служб GRAM этих узлов (входящие в ресурсную информацию узла), позволяют планировщику направлять задание только в те узлы, на которых авторизован владелец задания.

Л И Т Е Р А Т У Р А

1. *I.Foster, C.Kesselman,* Editors. The Grid: Blueprint for a New Computing Infrastructure. - 550 p. - Morgan Kauffmann, San Francisco, 1999. – Отдельные статьи доступны - http://www.globus.org/research/papers.html

2. *В.Н.Коваленко, Е.И.Коваленко, Д.А.Корягин, Э.З.Любимский, Е.В.Хухлаев.* Современное состояние и направления развития программного обеспечения GRID // Информационные технологии и вычислительные системы. № 4, 2003 г., с. 23-36
3. *В.Коваленко, Е.Коваленко, Д.Корягин, Э.Любимский, Е.Хухлаев.* Метадиспетчер: Управление заданиями в вычислительной Сети // Открытые системы, № 5-6, 2001. – с.22-28. – http://www.osp.ru/2001/05-06/022.htm
4. *В.Коваленко, Е.Коваленко.* Пакетная обработка заданий в компьютерных сетях // Открытые системы, № 7-8, 2000. – с. 10-19. – http://www.osp.ru/2000/07-08/010.htm
5. *T.Sandholm, R.Seed, J.Gawor.* Globus Toolkit 3 Core – A Grid Service Container Framework. Globus Project, 2003. - http://www-unix.globus.org/ogsa/docs/alpha/gt3_alpha_core.pdf
6. *I.Foster, C.Kesselman, S.Tuecke.* The Anatomy of the Grid: Enabling Scalable Virtual Organizations.// Intl. J. High-Performance Computing Applications, 15(3), pp.200-222, 2001. - ftp://ftp.globus.org/pub/globus/papers/anatomy.pdf
7. *I.Foster, C.Kesselman, J.Nick, S.Tuecke.* Grid Services for Distributed System Integration.// Computer, 35(6), pp.37-46, 2002. – Расширенная версия - ftp://ftp.globus.org/pub/globus/papers/physiology.pdf
8. *В.Н.Коваленко, Е.И.Коваленко, Д.А.Корягин, Э.З.Любимский, Е.В.Хухлаев, О.Н.Шорин.* Планирование ресурсов в Грид на основе локальных расписаний // Методы и средства обработки информации. М: МГУ им.М.В.Ломоносова. - 2003
9. *V. Welch, F. Siebenlist, I. Foster, J. Bresnahan, K. Czajkowski, J. Gawor, C. Kesselman, S. Meder, L. Pearlman, S. Tuecke.* Security for Grid Services. // Twelfth International Symposium on High Performance Distributed Computing (HPDC-12), IEEE Press, June 2003. - http://www.globus.org/Security/GSI3/GT3-Security-HPDC.pdf
10. *V. Welch, I. Foster, C. Kesselman, O. Mulmo, L. Pearlman, S. Tuecke, J. Gawor, S. Meder, F. Siebenlist.* X.509 Proxy Certificates for Dynamic Delegation. 3rd Annual PKI R&D Workshop, 2004. - http://www.globus.org/Security/papers/pki04-welch-proxy-cert-final.pdf
11. *J. Novotny, S. Tuecke, V. Welch.* An Online Credential Repository for the Grid: MyProxy. Proceedings of the Tenth International Symposium on High Performance Distributed Computing (HPDC-10), IEEE Press, August 2001. - http://www.globus.org/research/papers/myproxy.pdf