



Enabling Grids for E-science

Аутентификация, авторизация и безопасность в Грид

Олешко С.Б.

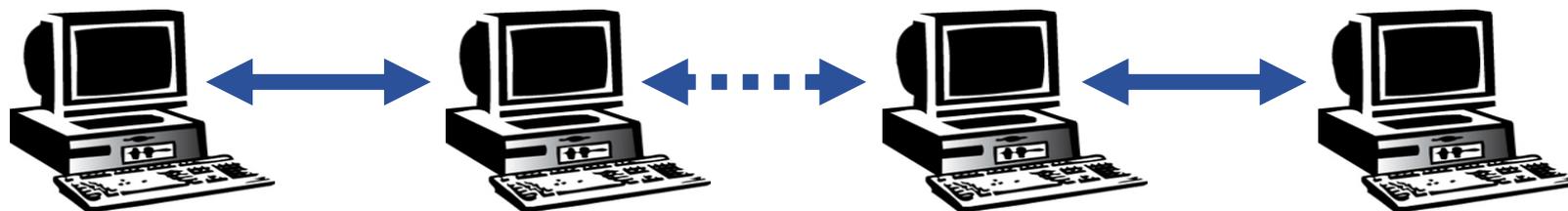
*Петербургский институт ядерной физики
г.Гатчина*

www.eu-egee.org



Information Society

- **Объект (защиты):**
 - Пользователь, программа или компьютер
- **Параметры доступа**
 - Некоторые данные, обеспечивающие доказательства идентичности объекта
- **Аутентификация**
 - Проверка идентичности объекта защиты
- **Авторизация**
 - Определение множества прав и привилегий для объекта защиты
- **Конфиденциальность**
 - Шифрование сообщений для того чтобы только получатель мог его расшифровать
- **Целостность**
 - Гарантия того, что сообщение не было изменено во время передачи



Пользователь

Ресурс

- Как Пользователь может получить безопасный доступ к Ресурсу, не являясь зарегистрированным пользователем промежуточных узлов или хотя бы самого Ресурса?
- Как Ресурс узнает, кто такой Пользователь?
- Как определять права Пользователя и как определить какой доступ ему разрешён?

- **Опасность атак с других узлов**
 - Большие распределённые кластеры – идеальная мишень для атак злоумышленников (“отказ в обслуживании”)
- **Незаконное или ненадлежащее распространение данных и доступ к конфиденциальной информации**
 - Огромные доступные ресурсы хранения данных могут быть использованы, например для хранения “пиратской информации”
 - Всё больше пользователей обладают данными, которые требуют являются конфиденциальными (медицина)
- **Опасность, связанная с проникновением вирусов, сетевых червей и т.п.**
 - Высокоскоростные сети являются более быстрым источником распространения, чем обычный Интернет

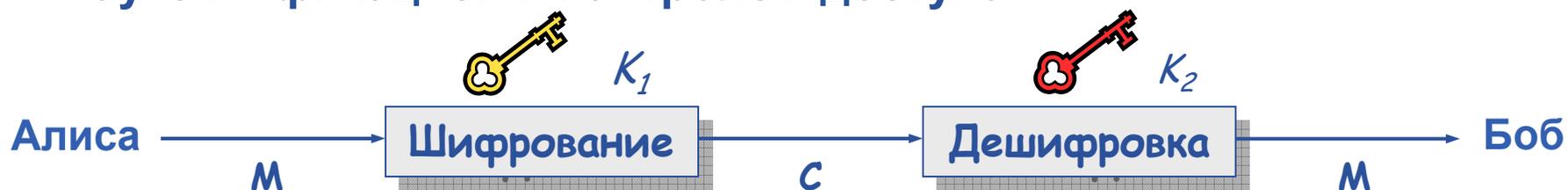
Три основных аспекта безопасности:

Privacy – Обмен сообщениями должен быть приватным.
(доступность передаваемых данных только участникам диалога)

Integrity – Целостность данных, т.е. неизменность передаваемых данных

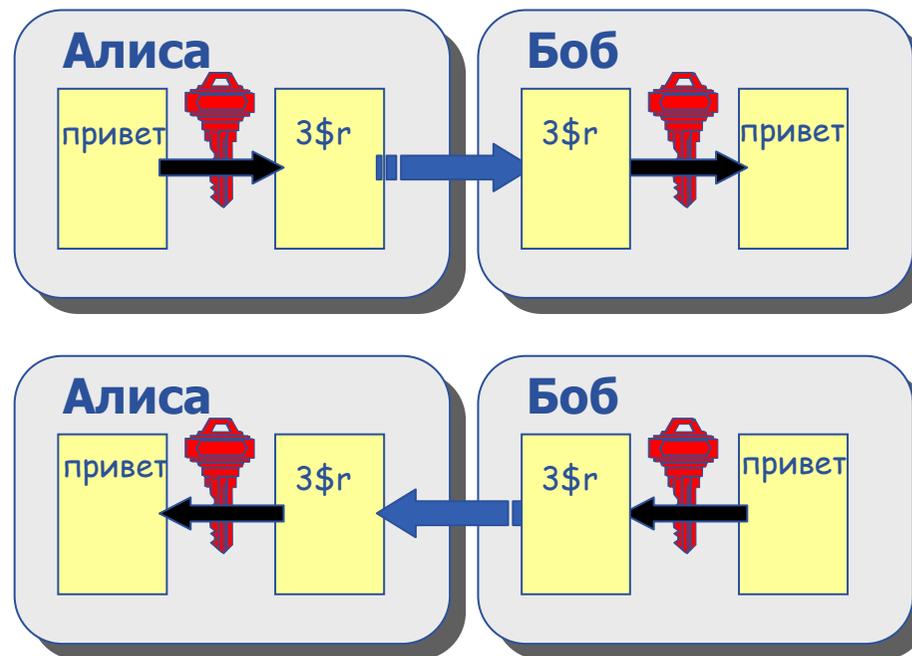
Authentication – Идентификация сторон, участвующих в диалоге
(проверка подлинности объекта)

- Криптография – математическая дисциплина, которая занимается вопросами информационной безопасности и связанными с ней проблемами, особенно шифрованием, аутентификацией и контролем доступа

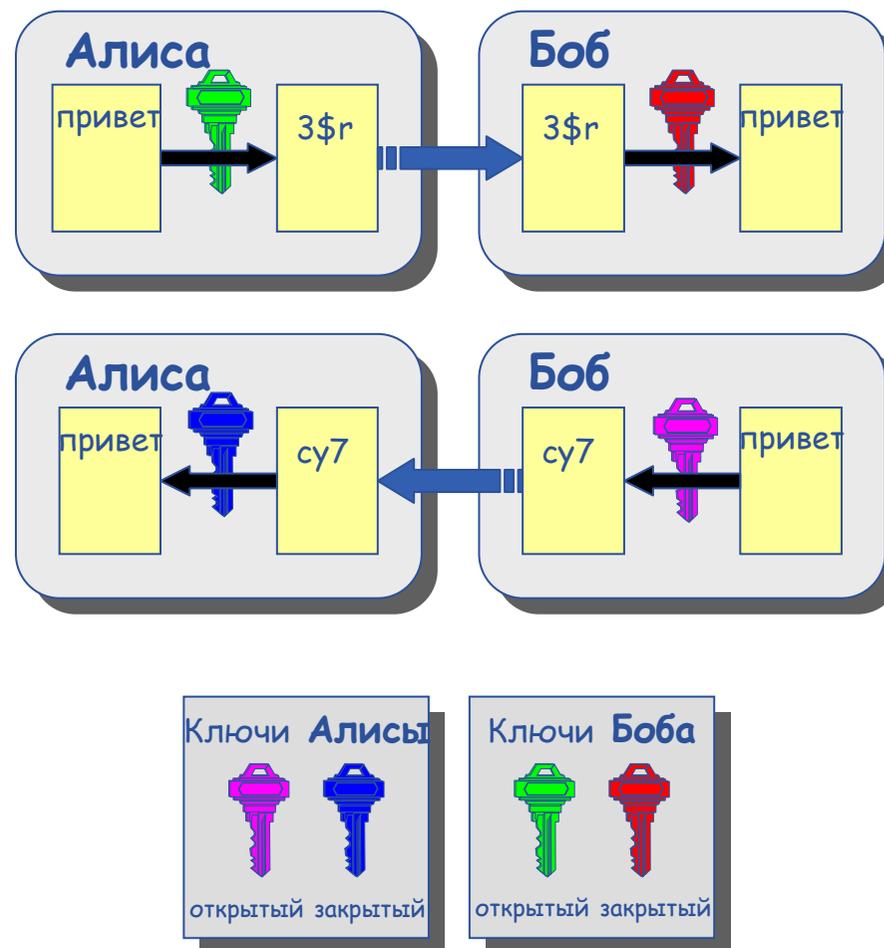


- Исходное сообщение: M
- Зашифрованное сообщение: C
- Шифрование с ключом K_1 : $E_{K_1}(M) = C$
- Дешифровка с ключом K_2 : $D_{K_2}(C) = M$
- Алгоритмы
 - Симметричный: $K_1 = K_2$
 - Несимметричный: $K_1 \neq K_2$

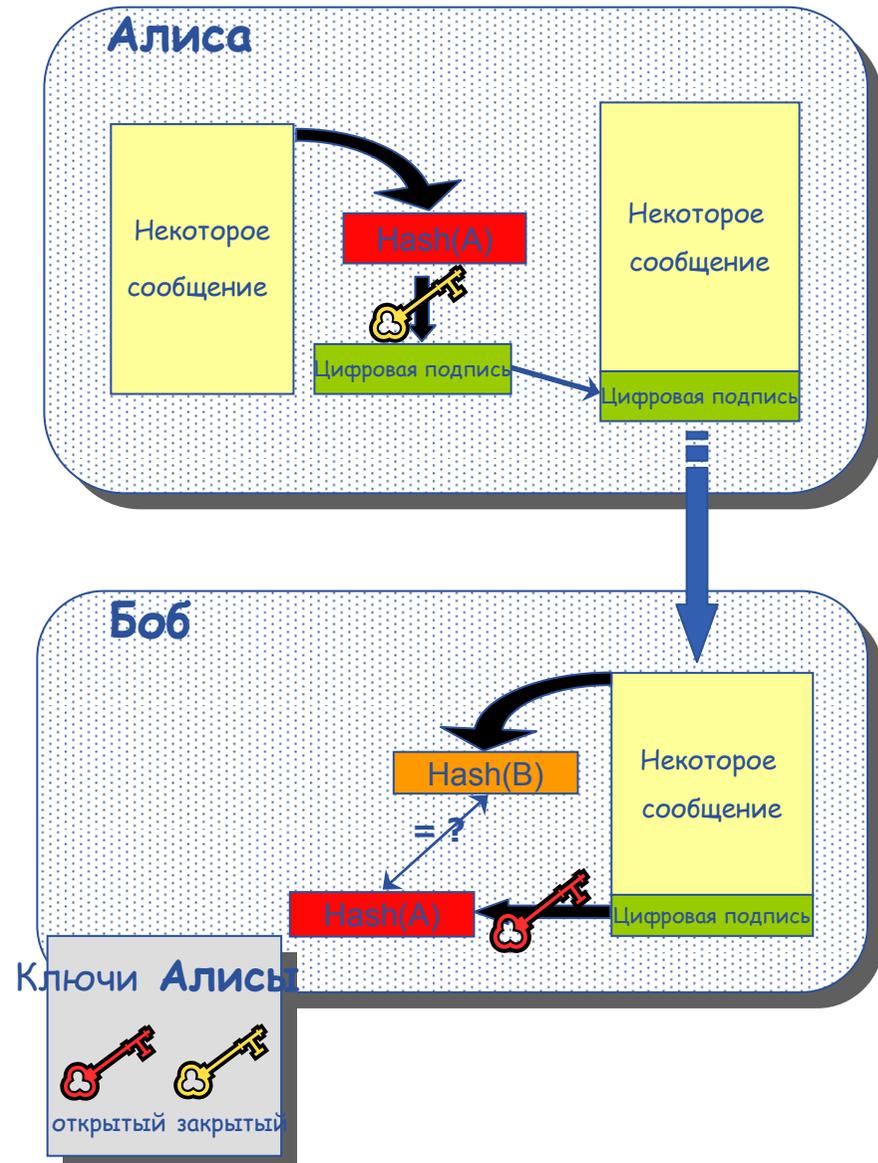
- Один и тот же ключ используется для шифрования и дешифровки
- Преимущества
 - Скорость
- Недостатки
 - Как безопасно передать ключ?
- Примеры
 - DES
 - 3DES
 - Rijndael (AES)
 - Blowfish
 - Kerberos



- У каждого пользователя 2 ключа: *открытый* и *закрытый*
 - “невозможно” вычислить значение закрытого ключа по открытому
 - сообщение, зашифрованное одним ключом может быть расшифровано *только* при помощи другого
- Нет необходимости обмениваться секретной информацией
 - отправитель зашифровывает при помощи *открытого* ключа получателя
 - получатель расшифровывает при помощи своего *закрытого* ключа
- Примеры
 - Diffie-Hellman (1977)
 - RSA (1978)



- Алиса вычисляет **дайджест** (hash) сообщения
- Алиса зашифровывает дайджест, используя свой **закрытый** ключ: зашифрованное значение и есть **цифровая подпись**
- Алиса отправляет подписанное сообщение Бобу
- Боб получает сообщение и вычисляет значение дайджеста
- Боб расшифровывает цифровую подпись при помощи **открытого** ключа Алисы и **сравнивает** его с вычисленным значением дайджеста
- Если оба значения равны, то сообщение не было изменено при передаче



- **Использование цифровой подписи Алисы безопасно, если:**
 1. **Закрытый ключ Алисы остался секретным**
 2. **Боб знает её открытый ключ**
- **Но как Боб может быть уверен, что открытый ключ, который он знает, на самом деле принадлежит Алисе, а не кому-то, кто выдаёт себя за неё?**
 - Нужна некоторая третья сторона, которая будет гарантировать соответствие между открытым ключом и объектом, которому он принадлежит
 - Обе стороны, и Алиса и Боб должны доверять этой третьей стороне

Эта третья сторона называется Сертификационный Центр - Certification Authority (CA).

- выдаёт цифровые сертификаты (содержат открытый ключ и идентификационную информацию) для пользователей, программ и машин (подписанные цифровой подписью CA)
- при этом проверяет соответствие представленных персональных данных и объекта
 - Но как это сделать, если сертификационный Центр в Москве, а пользователь – в Санкт-Петербурге?
 - Возникает сообщество Ответственных за Регистрацию Registration Authority (RA)

Пользователь создаёт пару ключей
Открытый / Закрытый



Закрытый ключ
шифруется на
локальном диске

На подпись передается
открытый ключ



Для подписи необходимо
удостоверение личности,
которое предъявляется RA



Подписанный открытый ключ
передается пользователю

Корневой
сертификат
CA

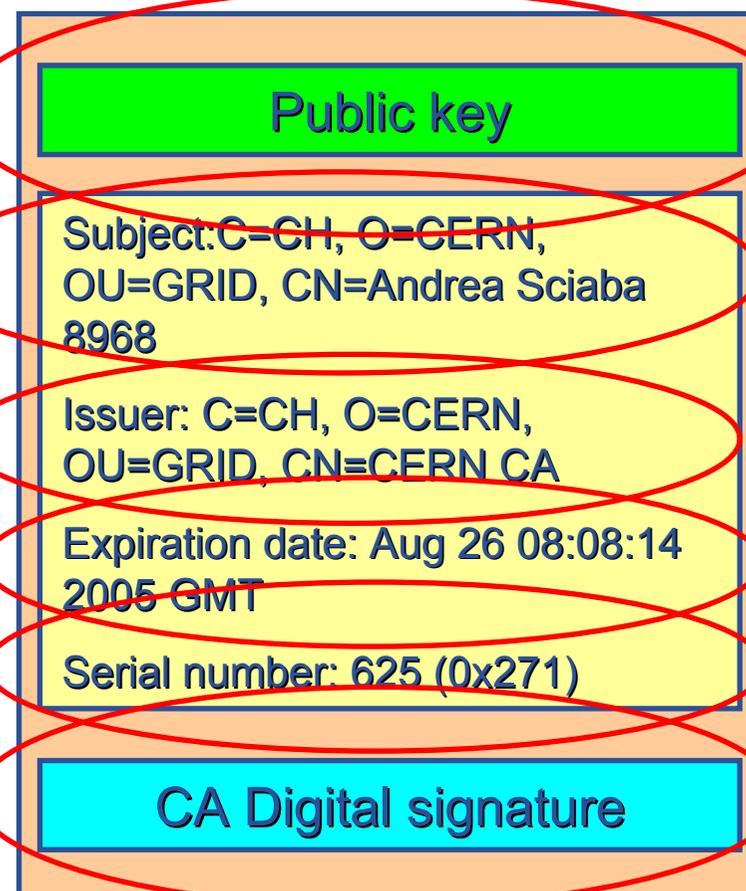
Центр
сертификации

CA подписывает
открытый ключ с
помощью своего
корневого
сертификата и
информирует
пользователя

X.509 сертификат содержит:

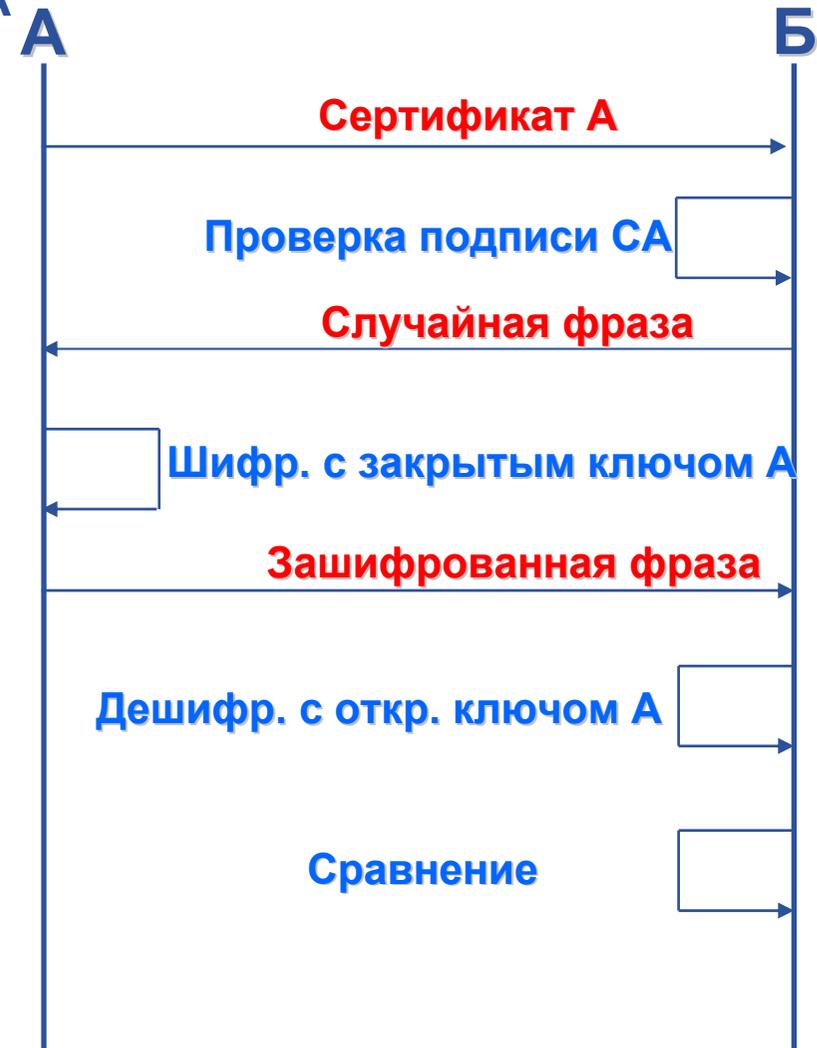
- открытый ключ владельца;
- данные владельца;
- информация о СА;
- срок действия;
- серийный номер;
- цифровая подпись СА

Структура сертификата X.509



Боб (Б) хочет аутентифицировать Алису (А)

- А посылает свой сертификат Б
- Он проверяет правильность сертификата и подпись (имеет PK CA).
- Б посылает А произвольную фразу (challenge) с просьбой зашифровать её закрытым ключом А.
- А шифрует пришедшие данные
- А отправляет ответ (response) Б.
- Б расшифровывает ответ А с помощью переданного ранее открытого ключа
- Б сравнивает результат с эталонной фразой. Если сравнение успешно, то А действительно владеет закрытым ключом, соответствующим сертификату.



- **В зависимости от способа получения сертификата он может быть получен в различных форматах:**
 - *.pem формат: 2 файла: userkey.pem – закрытый ключ, usersert.pem – подписанный сертификат)
 - *.p12 формат (PKCS12): один файл - для загрузки в браузер Mozilla/Netscape/FireFox
 - *.pfx формат: один файл - для загрузки в браузер Internet Explorer
- **Как правило, сертификат должен быть загружен в браузер (регистрация в ВО)**
- **Процедура экспорта/импорта зависит от типа используемого браузера и формата сертификата**
- **Сертификат имеет срок действия (от 2 недель до 1 года)**
- **По истечению срока действия он может быть продлён**

Проблемы:

Single sign-on

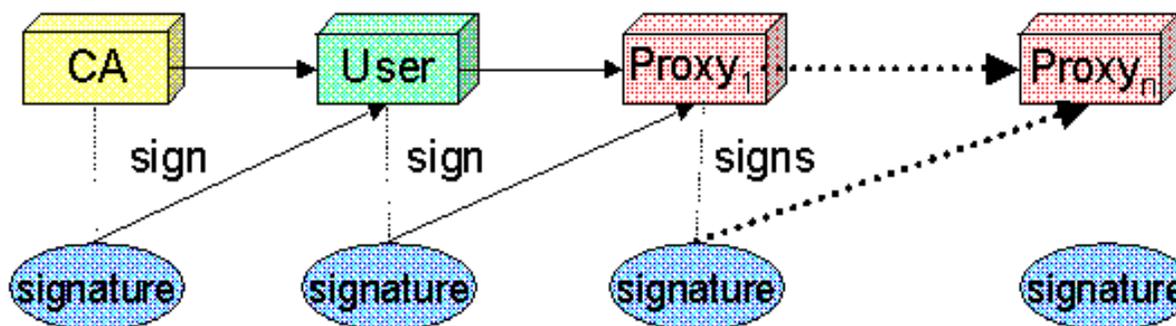
(однократное предъявление
первичного закрытого ключа)

Delegation

делегирование полномочий



Прoxy-сертификат (расширение X.509)



Применение проxy-сертификата для аутентификации избавляет пользователя от необходимости вводить свой пароль при каждом взаимодействии с сервисами.

Можно передавать свои проxy-сертификаты другим субъектам для выполнения операций от своего имени.

Ограниченное время действия и ограниченное назначение

- Проху сертификат имеет достаточно короткое время жизни (обычно не более 24 часов). А как быть, если заданию требуется больше времени для выполнения?
 - в HEP Data Challenges в LCG некоторые задания выполнялись до 2 суток
- Выход – создание специального сервиса для автоматического обновления сертификатов (**MyProxy server**)
- Проху-сертификат можно зарегистрировать на сервере Мурпроху и он будет обновляться в течение указанного периода времени (по умолчанию 7 суток)
- При этом соответствующий запрос будет проходить через Мурпроху server

- «Динамическое собрание одиночек и организаций, гибко, безопасно и координировано разделяющее ресурсы»
- Пользователь Грид **обязан** принадлежать к одной из ВО
 - ВО согласовывают доступ к Грид-узлам и ресурсам
 - Авторизация проверяется на ресурсе
- **ВО с технической точки зрения:** ресурс, перечисляющий Distinguished Names сертификатов пользователей конкретной ВО
- Реализационно ВО ведёт список своих членов на специальном сервере (LDAP Server)
 - **этот список распространяется на все узлы, где поддерживается эта ВО**
 - **сопоставляется с локальными пользователями, зарегистрированными на этом узле (обычно выполняется через файл grid-mapfiles)**

```
..
"/C=CH/O=CERN/OU=GRID/CN=Simone Campana 7461" .dteam
"/C=CH/O=CERN/OU=GRID/CN=Andrea Sciaba 8968" .cms
```

До VOMS

- Пользователь может быть членом только одной VO
- Все члены VO имеют одинаковые права
- Grid-mapfiles модифицируются только системой управления VO
- `grid-proxy-init`

С VOMS

- Пользователь может быть членом нескольких VO
 - Объединение прав
- VO может иметь группы
 - Различные права для каждой
 - Различные группы экспериментаторов
 - Связанные группы
- VO может иметь роли
 - Назначаются для особых целей
 - Напр. sysadmin
- При создании Proxy сертификата вводится дополнительный атрибут – имя VO
- `voms-proxy-init -voms gilda`

VOMS – используется сейчас в Грид EGEE

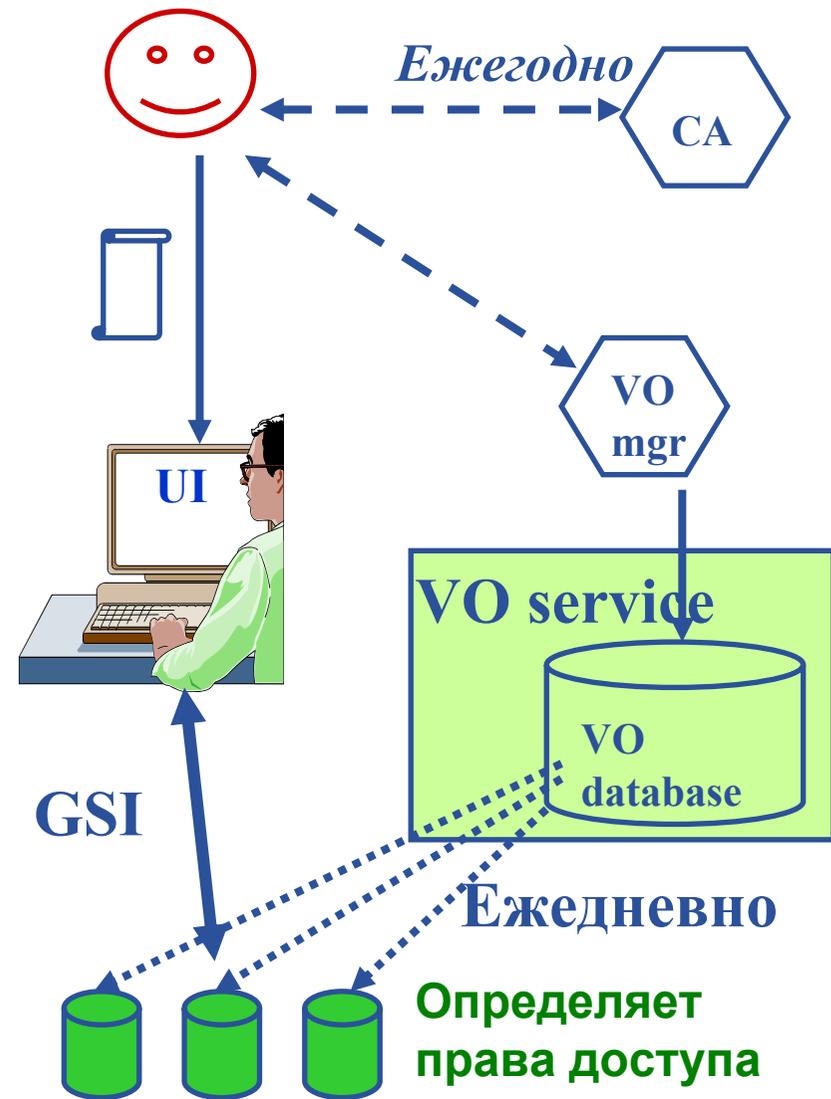
- Аутентификация основывается на использовании сертификатов стандарта **X.509**
 - Устанавливаются отношения доверия между **Certificate Authorities (CA)** и узлами, между CAs и пользователями
 - CAs выдаёт/подписывает (долгоживущие) **сертификаты**, идентифицирующие узлы и пользователей (аналог паспорта)
 - Широко используется в браузерах для аутентификации сайтов
 - Для того, чтобы уменьшить уязвимость, в Грид для идентификации пользователей используются (короткоживущие) **проxy** их сертификатов
- **Проxy сертификаты могут**
 - Быть **делегированы** сервису для того чтобы он мог действовать от имени пользователя
 - Включать **дополнительные атрибуты** (например информацию о VO для VOMS)
 - Быть зарегистрированными на **внешнем хранилище** (MyProxy)
 - Быть **обновлены** (в случае истечения срока действия)

• Аутентификация

- Пользователь получает сертификат от **Certificate Authorities (CA)**
- Соединяется с UI по SSH (UI – сервис пользовательского интерфейса)
- Загружает сертификат на UI
- “Входит” в Грид - создание проху
- GSI (Grid Security Infrastructure)

• Авторизация

- Пользователь вступает в VO
- VO согласовывает доступ к Грид-узлам и ресурсам
- Авторизация проверяется на ресурсе
- Права пользователя определяются информацией из его проху



- Расположен в Курчатовском институте
<http://ca.grid.kiae.ru/RDIG/>.
- Ознакомиться с правилами и процедурой можно на страничке
<http://ca.grid.kiae.ru/RDIG/certificates/obtain.html>.

Получение нового пользовательского сертификата, RDIG CA - Netscape

File Edit View Go Bookmarks Tools Window Help

http://ca.grid.kiae.ru/RDIG/requests/new_user_cert.html

Получение нового пользовательского с...

([список RA](#)). При этом пользователь должен иметь при себе удостоверение личности и заполненную бумажную форму.

Персональные данные владельца сертификата	
Имя: ваше имя (по-английски), например Ivan	<input type="text"/>
Фамилия: ваша фамилия (по-английски), например Petrov	<input type="text"/>
E-mail: адрес электронной почты, на который будут приходить все сообщения о вашем сертификате. Например vania@ru.net	<input type="text"/>
Контактный телефон: телефон (с кодом города), по которому с вами можно связаться. Например +7 (095) 123-45-67	<input type="text"/>
Параметры сертификата	
Common Name: ваши имя и фамилия (по-английски), например Ivan Petrov	<input type="text"/>
Организация: название организации, в которой вы работаете. Если названия вашей организации нет в списке, то вам сначала необходимо завести у себя Registration Authority. Как это сделать, написано в этой инструкции .	<input type="text"/> <ul style="list-style-type: none"> IHEP, ihep.su ITEP, itep.ru KIAM, keldysh.ru BINP, inp.nsk.su
<input type="button" value="Далее"/> <input type="button" value="Сброс"/>	

Document: Done (0.171 secs)

- Центр регистрации для виртуальных организаций
LCG

https://lcg-registrar.cern.ch/virtual_organization.html

- Центр регистрации для виртуальных организаций
РДИГ

http://rdig-registrar.sinp.msu.ru/virtual_organization.html

LCG Users Registration - Virtual Organization - Netscape

File Edit View Go Bookmarks Tools Window Help

http://lcg.web.cern.ch/LCG/users/registration/VO.html

Регистрация пользователей РДИГ LCG Users Registration - Virtual Organization

LCG home | Calendar | Meetings | Contact Us

LCG Users Registration

- Project Structure
- Project Planning
- Press&Media
- Documents
- Dissemination
- Jobs
- Activities
- LCG Users
 - User Registration
 - Users Support
 - Exp.Int.Supp
- LCG Sites
- LCG Operations

[Overview](#) • [Digital Certificates](#) • [Loading Certificates](#) • [Certificate Troubleshooting](#)
[Personal Information](#) • [Virtual Organization](#) • [Contact Registrar](#) • [Registration Form](#)

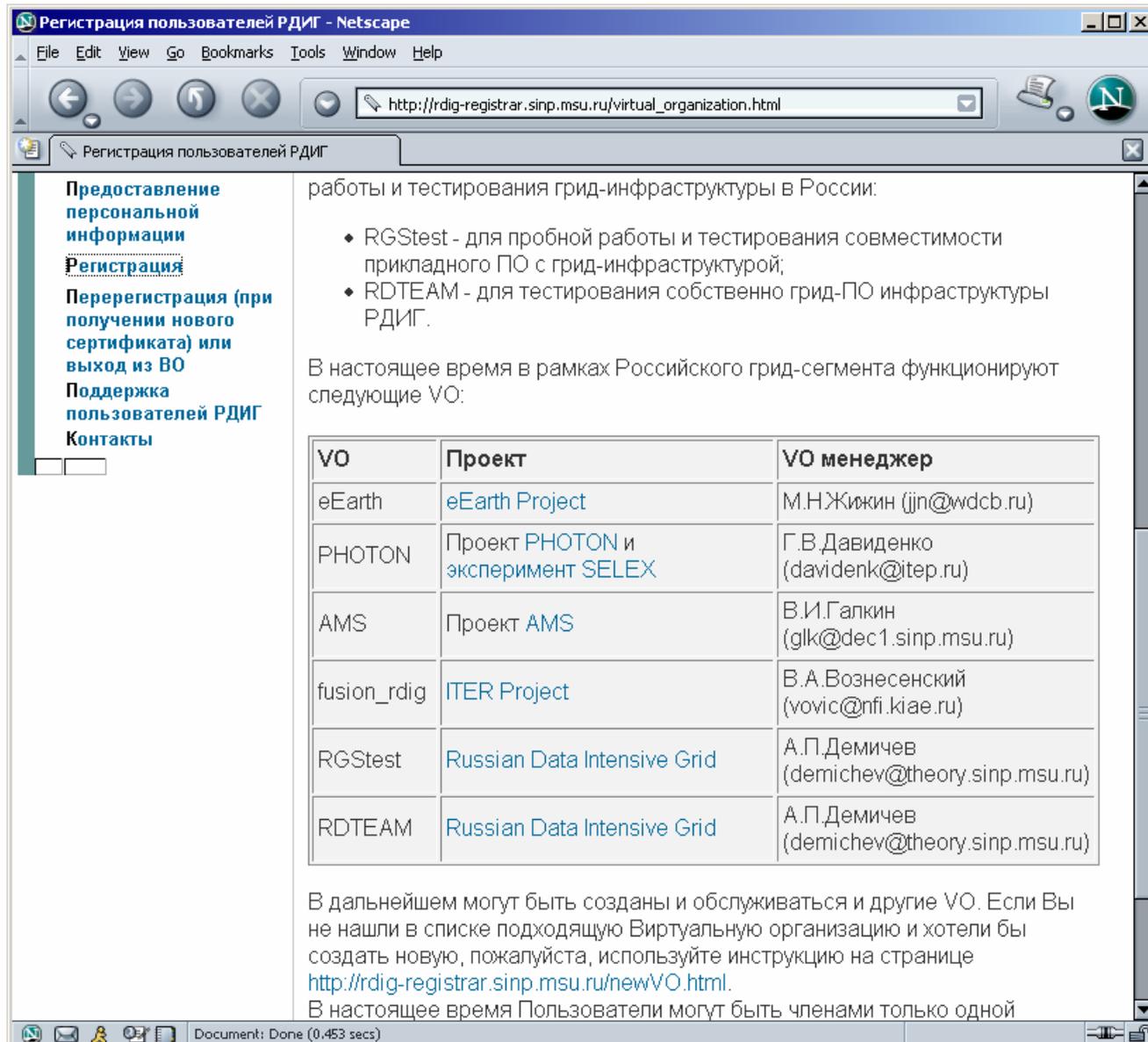
Virtual Organization

To use LCG resources you must be affiliated with one of the following Virtual Organizations (VO). You will be required to select your VO when you register and the information you supply will be forwarded to the VO administration and resource providers for validation before you complete the registration process.

Currently you can only be a member of **one** VO at a time. If you decide to change the VO you belong to, please send an email request from the registered address to project-lcg-registrar@cern.ch. You will be asked to confirm your request by the LCG Registrar. An email notification will inform you when you have been removed from the registration database and your previous VO. After this you should submit a new [registration form](#) selecting your new VO.

VO	LHC Affiliation
ALICE	ALICE experiment
ATLAS	ATLAS experiment
CMS	CMS experiment
DTEAM	Grid (LCG) Deployment Group
LHCB	LHCb experiment
SixTrack	Single Particle Tracking Code
VO	non-LHC Affiliation
BaBar	BaBar experiment
D0	D0 experiment
H1	H1 experiment

Document: Done (0.453 secs)



Регистрация пользователей РДИГ - Netscape

File Edit View Go Bookmarks Tools Window Help

http://rdig-registrar.sinp.msu.ru/virtual_organization.html

Регистрация пользователей РДИГ

Предоставление персональной информации
Регистрация
Перерегистрация (при получении нового сертификата) или выход из VO
Поддержка пользователей РДИГ
Контакты

работы и тестирования грид-инфраструктуры в России:

- RGStest - для пробной работы и тестирования совместимости прикладного ПО с грид-инфраструктурой;
- RDTEAM - для тестирования собственно грид-ПО инфраструктуры РДИГ.

В настоящее время в рамках Российского грид-сегмента функционируют следующие VO:

VO	Проект	VO менеджер
eEarth	eEarth Project	М.Н.Жижин (jln@wdcb.ru)
PHOTON	Проект PHOTON и эксперимент SELEX	Г.В.Давиденко (davidenk@itep.ru)
AMS	Проект AMS	В.И.Галкин (glk@dec1.sinp.msu.ru)
fusion_rdig	ITER Project	В.А.Вознесенский (vovic@nfi.kiae.ru)
RGStest	Russian Data Intensive Grid	А.П.Демичев (demichev@theory.sinp.msu.ru)
RDTEAM	Russian Data Intensive Grid	А.П.Демичев (demichev@theory.sinp.msu.ru)

В дальнейшем могут быть созданы и обслуживаться и другие VO. Если Вы не нашли в списке подходящую Виртуальную организацию и хотели бы создать новую, пожалуйста, используйте инструкцию на странице <http://rdig-registrar.sinp.msu.ru/newVO.html>.

В настоящее время Пользователи могут быть членами только одной

Document: Done (0.453 secs)