Outline

- Globus Alliance & Globus Toolkit
- The Grid “problem”
- Globus Security Infrastructure (GSI)
- Public Key Credentials + Proxy-Certificates
- SSL, GSSAPI/GSI and Delegation
- Kx509: Kerberos => PK
- Pkinit: PK => Kerberos
- GridLogon: username/password/OTP => PK
- Futures and Conclusion
The Globus™ Alliance
Making Grid computing a reality

- Argonne, UC, USC/ISI, EPCC, PDC, NCSA
- Close collaboration with many scientific and commercial Grid application and infrastructure projects
- Development and promotion of standard Grid protocols to enable interoperability and shared infrastructure
- Development and promotion of standard Grid software APIs and SDKs to enable portability and code sharing
- The Globus Toolkit® software: Open source software base for building Grid infrastructure and applications
There is a "bunch crossing" every 25 nsecs. There are 100 "triggers" per second. Each triggered event is ~1 MByte in size.

Physics data cache

Physicist workstations

Tier 1
France Regional Centre

Germany Regional Centre

Italy Regional Centre

FermiLab ~4 TIPS

Tier 0
CERN Computer Centre

~622 Mbits/sec

~1 TIPS

~100 MBytes/sec

~100 MBytes/sec

~0.25 TIPS

~1 MBytes/sec

~PBytes/sec

Online System

~20 TIPS

~622 Mbits/sec

or Air Freight (deprecated)

Tier 2
Caltech ~1 TIPS

Tier 2 Centre ~1 TIPS

Tier 4 Centre ~1 TIPS

Tier 4 Centre ~1 TIPS

Tier 4

Physicists work on analysis "channels". Each institute will have ~10 physicists working on one or more channels; data for these channels should be cached by the institute server.
• Each Organization is “independent”
• Each Organization has its own AuthN mechanisms
• Each Organization enforces its own access policy
• User needs to delegate rights to broker which may need to delegate to services
• QoS/QoP Negotiation and multi-level delegation
Grid Security Infrastructure (GSI)

- Based on standard PKI technologies
  - SSL protocol for authentication, message protection + GSSAPI-mechanism
  - CAs allow one-way, light-weight trust relationships (not just site-to-site)
- X.509 Certificates for asserting identity
  - for users, services, hosts, etc.
- Proxy Certificates
  - GSI extension to X.509 certificates for delegation, single sign-on
Grid Security Infrastructure (GSI)

- Use GSI as a standard mechanism for bridging disparate security mechanisms
  - Doesn’t solve trust problem, but now things talk same protocol and understand each other’s identity credentials
  - Basic support for delegation, policy distribution
- Translate from other mechanisms to/from GSI as needed
- Convert from GSI identity to local identity for authorization
Grid Identity, Local Policy

• In current model, all Grid entities assigned a PKI identity.
• User is mapped to local identities to determine local policy.
Use Delegation to Establish Dynamic Distributed System
X.509 Proxy Certificates

- GSI Extension to X.509 Identity Certificates
  - On RFC track
- Enables single sign-on
- Allow user to dynamically assign identity and rights to service
  - Can name services created on the fly and give them rights (i.e. set policy)
- What is effectively happening is the user is creating their own trust domain of services
  - Services trust each other with user acting as the trust root
Proxy Certificates

- **CN=Jane Doe**
- **Rights:** Can access file F1, Service S1, ...

**X.509 Id certificate**

**X.509 Proxy Delegation**

- **Create**

**X.509 Proxy certificate**

- **CN= Jane Doe/9874**
- **Use delegated rights to access resources.**

- **F1**
- **S1**
Goal is to do this with arbitrary mechanisms

- Compute Center
- Virtual Organization
- Rights
- X.509/SSL
- SAML Attribute
- Kerberos/WS-Security
Kerberos to GSI Gateway

- To use Kerberos, a Kerberos-to-GSI gateway translates Kerberos credentials to GSI credentials to allow local Kerberos users to authenticate on the Grid.
  - Kx509/KCA is an implementation of one such gateway.
- Sslk5/pkinit provide the opposite functionality to gateway incoming Grid credentials to local Kerberos credentials.
Local Identity, Grid Identity, Local Policy

- **KCA**
- **Kerberos Site**
- **Grid Identity**
- **Local Policy**
- **Map to local name**
- **SSLK5**
- **KRB5 Resources**
GridLogon: Credential Wallet/Converter

- GridLogon (MyProxy) allows users to store GSI credentials and retrieve them
  - With username/password or other credential
  - Integration with One-Time-Password (OTP) Systems
  - Can act as a credential translator from username/password to GSI
- Used by services that can only handle username and pass phrases to authenticate to Grid
  - Services limited by client implementations
    - E.g. web portals
- Also handle credential renewal for long-running tasks
GridLogon: Passphrase-X.509 Federation Service
One Time Passwords and Restricted Delegation

- User
- GridLogon
- OTP
- Restricted Delegation
- Grid Identity
- Restricted Delegation
- Local Policy
- Map to local name
- pkinit
- KRB5 Resources
- Restricted Delegation
GSI Implementation

Compute Center

Authz Callout

Virtual Organization

Access

Rights

SSL/WS-Security with Proxy Certificates

Services (running on user’s behalf)

Rights’

VO Users

Rights”

GridLogon

KCA

CAS or VOMS issuing SAML or X.509 ACs

Local Policy on VO identity or attribute authority

JET Workshop 2004

Globus Toolkit: Authentication and Credential Translation
Grid Evolution: Open Grid Services Architecture

- Goals
  - Refactor Globus protocol suite to enable common base and expose key capabilities
  - Service orientation to virtualize resources and unify resources/services/information
  - Embrace key Web services technologies for standard IDL, leverage commercial efforts

- Result = standard interfaces & behaviors for distributed system management built on Web services
  - Standardization within Global Grid Forum and OASIS
  - Open source & commercial implementations
Conclusion

- The Globus Toolkit is sophisticated, secure middleware
  - De-facto standard for Grid applications
- Multiple AuthN-mechanism support
  - Plus “translation” services
- Secure Delegation of Rights support
  - through use of proxy-certificate
- Next generation GT based on Web Services
  - Standardized in Global Grid Forum & OASIS
- Globus Toolkit provides a working, evolving implementation for “secure” Grid protocols
  - Downloaded 100k+ times already (www.globus.org)