

NORDUGRID

*Grid Solution For Wide Area
Computing and Data Handling*



Know**ARC**

Overview of the security capabilities of ARC

Aleksandr Konstantinov, Weizhong Qiang
(presented by Balázs Kónya)

NorduGrid collaboration

EGEE'09 Conference

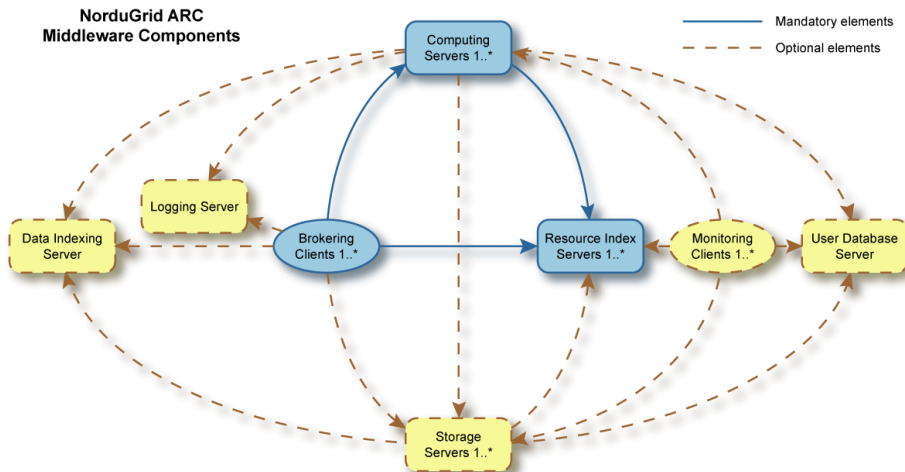
Barcelona, Spain, 22 September 2009

Outline

- The Advanced Resource Connector
- Security within pre-WS services
- The new security framework (HED)
- New security services

- Separate talk: arcproxy client

ARC Today



❖ Reliable, efficient and easy-to handle open source middleware, in production since 2002

❖ Best suits high-throughput distributed computing

❖ Totally independent, very portable code base

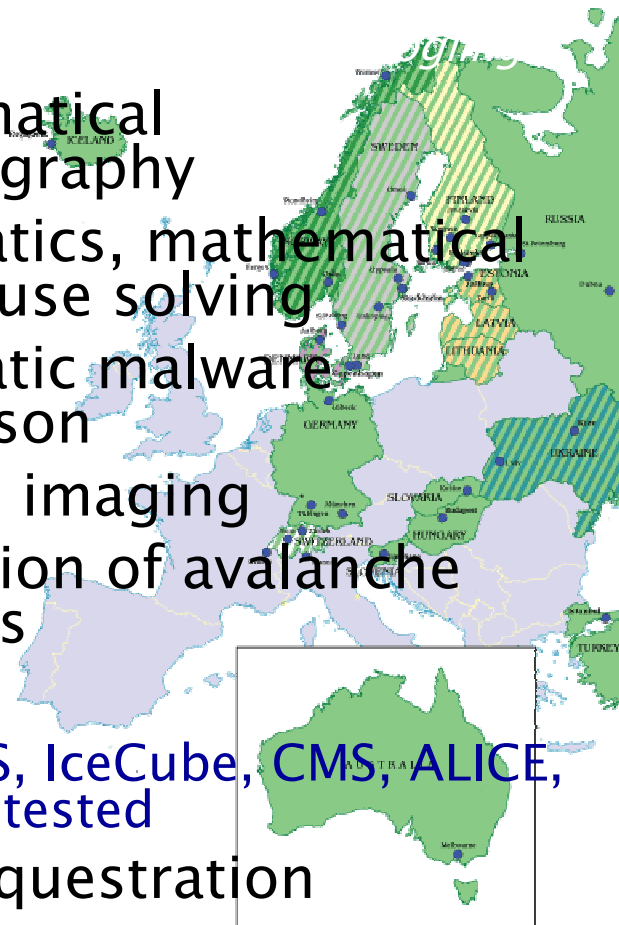
❖ GSI-based

- **Clear separation of cluster and grid layer**
 - No grid layer on the nodes (unless required by users)
 - Powerful input/output grid data handling by the front-end
 - Dramatically increases CPU utilization
 - Automatically allows for data caching
 - ARC frontend: all grid related operations
 - ARC infosys: efficient, reliable, distributed, dynamic
- **Resource discovery and brokering encapsulated in the client**
 - No single point of failure, ARC clients act as “agents”
 - Redundancy, mobility, scalability
 - Based on a powerful client API, ARCLIB

ARC enabled Applications

- Biophysics
- Biochemistry
- Computational chemistry
- Quantum chemistry
GAMESS
- Molecular dynamics
GAUSSIAN, DALTON, MOLDEN
- Bioinformatics
Taverna
BLAST, HMMER
eQTL
- Language studies
- Solid state physics
- Computational physics

- Mathematical crystallography
- Informatics, mathematical logic clause solving
- Automatic malware comparison
- Medical imaging
- Simulation of avalanche dynamics
- HEP
ATLAS, IceCube, CMS, ALICE, LHCb tested
- CO2 sequestration
- Other materials sciences



Security within production ARC

- Protocols
- Authorization
- Delegation

production ARC – protocols

- Uses X.509 for authentication of users
- Uses communication protocols which provide data integrity and protection
 - GridFTP
 - Used for most communications
 - Including communication with Computing Element (job submission!)
 - HTTPS
 - Third-party proprietary protocols
 - Data management – RLS, LFC
- Unprotected communication
 - LDAP
 - Used by Information System

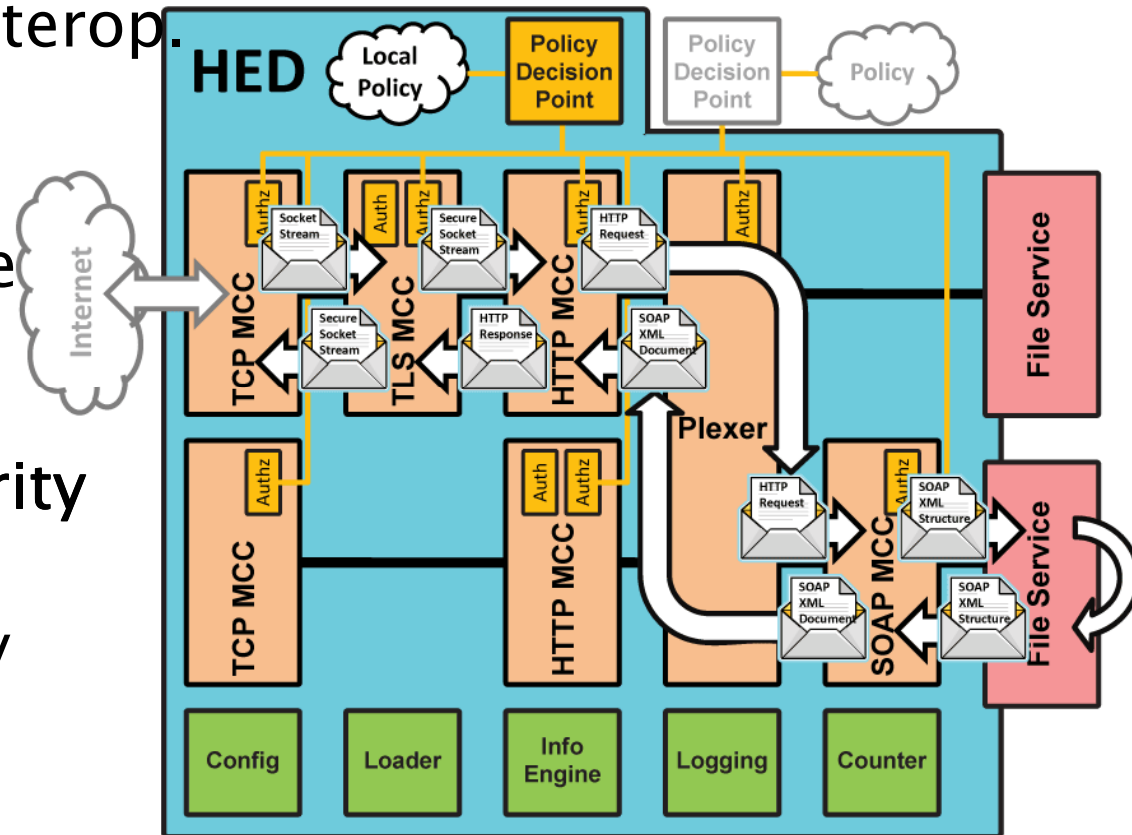
production ARC – authorization

- Relatively thin layer integrated into communication stack
- Strongly coupled with delegation
- Based on information stored in X.509 certificate
- Simple hard-coded and configurable authorization rules
 - DN of X.509
 - VOMS attributes
 - External plugin/executable
 - LCAS framework
- Some services implement own authorization based on internal information
 - Hard-coded rules
 - GACL polices

- Full identity delegation – X.509 Proxy Certificates
 - Used by Computing Element to retrieve and store data on behalf of original user
 - No additional restrictions put into Proxy Certificates
 - Delegation performed as part of GSI handshake
 - Embedded into GridFTP protocol
 - Support for renewal of delegated credentials
 - Support for MyProxy service (for renewal)

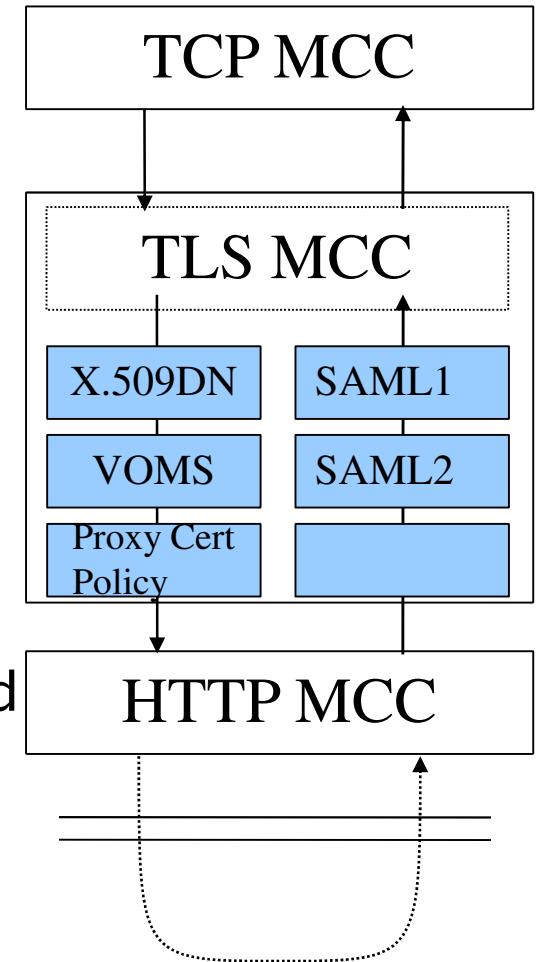
HED ing towards a better ARC

- WS interfaces
- Standard-based interoperability
- Better modularity
- Extensibility
- Self-sufficient core components
- Portability
- Re-designed security
- User-friendly
- Developer-friendly



Modular approach

- New ARC services and clients are based on modular approach
 - Message Chain Component (MCC)
 - Protocol layer module
 - Data Management Component (DMC)
 - Full data protocol(s)
 - ARC Client Component (ACC)
 - Job submission and control modules
 - Security Handler Component (SHC)
 - Security related attributes collection and handling
 - Policies and Attributes evaluation
 - WS-Security support



Unified security offered by HED

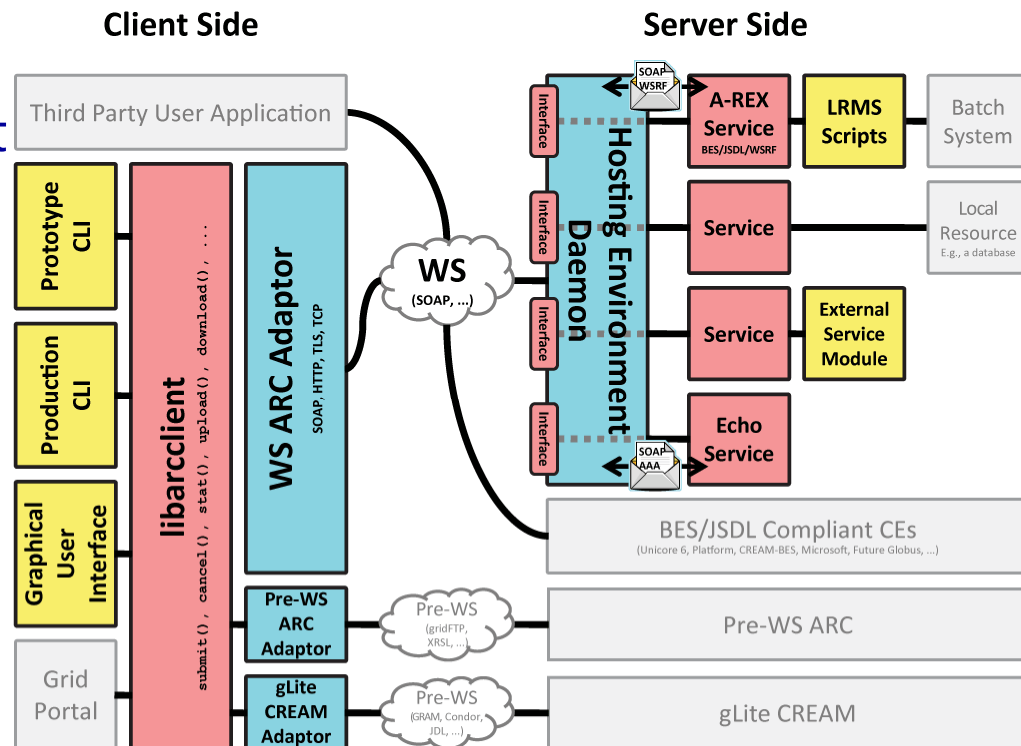
- Every service developed in HED gets generic security infrastructure
 - Information collected and processed at protocol levels
 - Authorization decisions based on protocol specific information
 - Authorization configuration fully depends on deployment
- Every service can implement own authorization
 - Through pluggable modules
 - Using direct support to ARC policy evaluation library
 - ARC policy language
 - Partial XACML

Unified security offered by HED

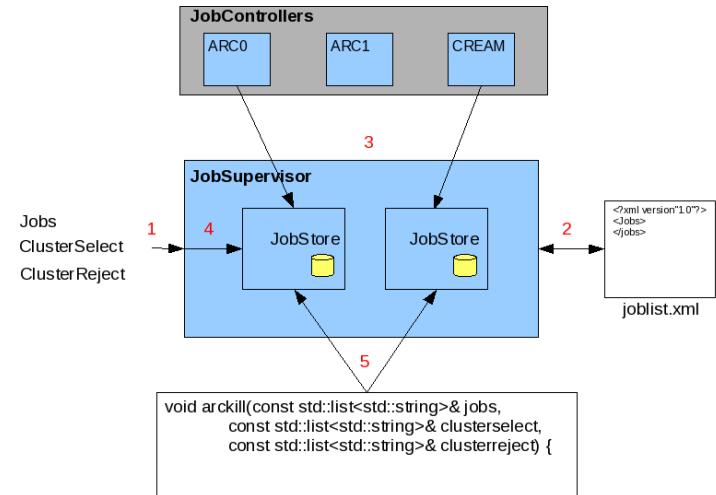
- Services which implement own authorization
 - A-REX – BES compliant Grid Computing Element
 - per Grid Job authorization policies
 - Storage system (multiple services)
 - per stored entity authorization policies
 - Inter-service trust relationship
- Information filtering (GLUE2 documents over WSRF)
 - Each node in XML document may have policy attached
 - Document is pre-filtered by matching policies to authentication tokens provided by client

• A-REX

- The flagship HED service implementing a Computing Element (CE)
- JSDL/BES/GLUE2 with ARC extensions
- Available as part of the 0.8 production ARC release
- Based on the good-old Grid-Manager
- Comes with all the production-triggered improvements

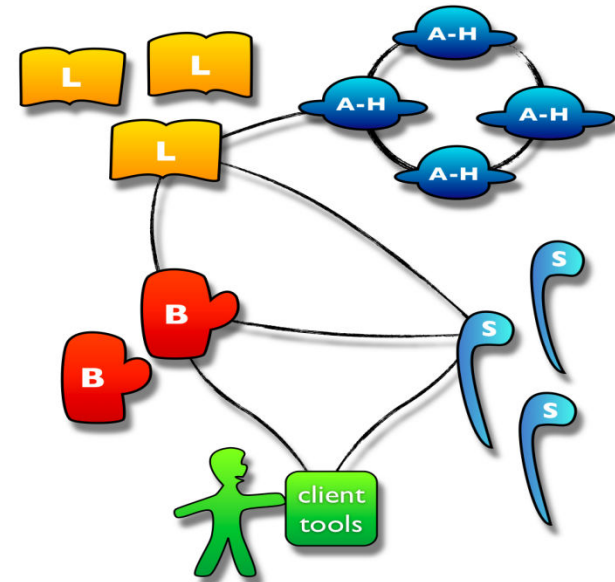


- Libarcclient (including libarcdata2) and arc* utils
 - Implemented in C++ but comes with Python and JAVA wrappers
 - Modular, plugin-based
 - with powerful *existing* plugins for pre-WS ARC, gLite, Unicore services, variety of brokering algorithms
 - Backward compatible with previous ARC servers
 - Available on Windows, MAC-OSXGrid



Fruits of the non-intrusive development

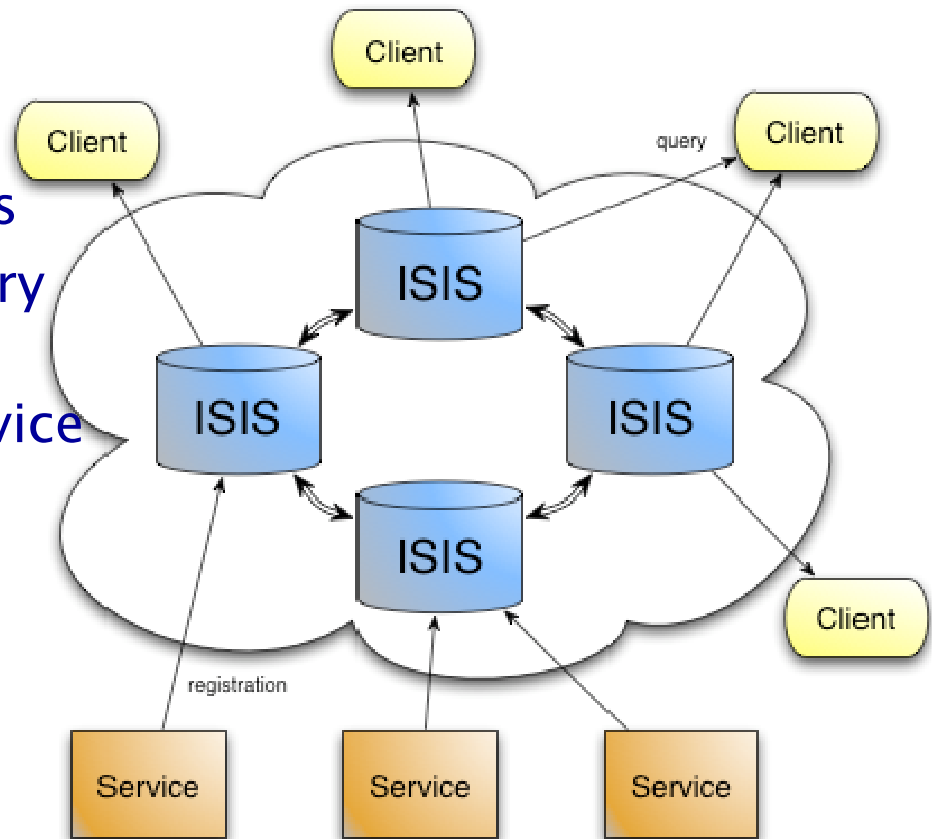
- Chelonia distributed storage solution implemented within HED
 - Global namespace
 - Supports collections and sub-collection to any depth
 - Automatic replication
- **A-Hash**: a replicated database to store metadata;
- **Librarian**: handles
 - metadata and hierarchy of collections and files
 - the location of replicas
 - health data of the Shepherd services
- **Bartender**: high-level interface for the users and for other services
- **Shepherd**: manages storage services, and provides a simple interface for storing files on storage nodes



Watch online www.youtube.com/watch?v=NEUWzGHHGhc
or see the demo live at EGEE09 in Barcelona

- **ISIS**

- P2P information system backbone
- stores service registrations
- WS interface to insert/query registration info
- a new generation ARC service implemented within HED



HED security modules

- Security Handler components
 - Security handlers are modules that are supposed to be embedded/configured into generic services in order to provide different security functionalities.
 - Available SCHs:
 - X.509 generic information extraction
 - VOMS information extraction
 - WS–Security extraction and insertion
 - X.509 Token Profile
 - Username Token Profile
 - SAML Token Profile (co-operate with an Attribute Authority service, such as VOMS SAML Service)

HED security modules

- Available SCHs (continued)
 - Local policy evaluation
 - Remote policy evaluation (call to remote policy decision service)
 - CHARON (ARC service)
 - ARGUS to be supported
 - X.509 proxy certificate policy evaluation
 - Consumption of SAML assertions (from SAML token, and SAML 2.0 SSO profile)

HED security: policies

- Supported policy expressions/languages
 - Lists of X.509 DNs – gridmap-like
 - Grid Access Control List (GACL)
 - Proprietary ARC policy language
 - XML based
 - Similar to XACML with simplification for (relative) user-friendliness
 - XACML policy language
 - Obligation is not supported

HED: new approach for delegation

- Still full identity delegation – X.509 Proxy Certificates
 - WS Port type for delegating credentials to service
 - Implemented by services which accept delegation
 - Support for proxy policies
 - According to RFC 3820
 - policyLanguage = id-ppl-anyLanguage
 - policy = ARC Policy XML document

New security services: Charon

- CHARON, ARC authorization service (policy evaluation service)
 - Accepts policy evaluation request
 - XACML request (XACML context schema)
 - Proprietary ARC request
 - Interoperation profile
 - SAML 2.0 profile of XACML 2.0 --- for XACML policy and request
 - Proprietary ARC profile --- for ARC policy and request
 - Returns evaluation result
 - Security handler (embedded in generic services) is supposed to contact Policy decision service

New security services: Fruitfly

- FruitFly short-lived credential service (SLCS service)
 - Accepts Shibboleth tokens
 - Generates short-lived X.509 credentials
 - SAML attribute assertion returned from Shibboleth IdP is embedded as certificate extension
 - The credential then can be used to access services which require X.509 credentials
 - Related *client* “arcslcs” that can be used to contact IdP (Shibboleth) and short-lived credential service to acquire X.509 credential
 - The client can/will also be capable to contact other SLCS service (like the gLite SLCS implementation) and the Confusa SLCS service (<https://slcstest.uninett.no/slcsweb/>)

New security services: DS

- Delegation service (DS)
 - Web Service for X.509 credential delegation
 - Standalone service
 - Functionality similar to Myproxy – but uses standard communication channel (SOAP)
 - Acts as intermediate for passing delegated credentials from client to service
 - Corresponding Security Handler Component to (almost) seamlessly
 - Delegate credentials to DS on client side
 - Fetch credentials from DS on service side

New security services: ARC-VOMS

- ARC-VOMS, an Attribute Authority (AA) service
 - Act as Attribute Authority to issue SAML attribute assertion
 - With the same interface as VOMS AA service
 - Reuse voms database as back-end database
 - Reuse voms admin service for managing the voms attributes
 - Configurable to adapt other database schema

New security services: ARC-VOMS

- Two ways of using AA service
 - SAML token security handler (embedded in generic services) is supposed to contact AA service to acquire SAML Token (assertion); and then SAML Token profile (WS-Security) can be supported.
 - Specific client is supposed to contact AA service to acquire SAML assertion; The assertion can be embedded into proxy certificate.

New security services: Shibbridge

- Service Provider service (Shibboleth-bridge)
 - Http layer service
 - In charge of Service Provider (SP) functionality of SAML 2.0 SSO profile
 - Act together with client interface (in charge of the functionality of user agent of SAML 2.0 SSO), and Shibboleth IdP (2.0)
 - SP service shares the same session with other services (one SP service per container)
 - SSL Client certificate authentication should be switched off
 - SAML attribute assertion can be used for access control
 - *Benefit:* Use community credential (Username/Passwd) as a replacement of X.509 cred.

Read more

- The new security framework
 - svn.nordugrid.org/trac/nordugrid/browser/arcl/trunk/doc/tech_doc/sec/arc-security-documentation.pdf
 - Soon available at <http://www.nordugrid.org/manuals.html>