BAR Security

JRA4 F2F, Cambridge, 8 May 2005

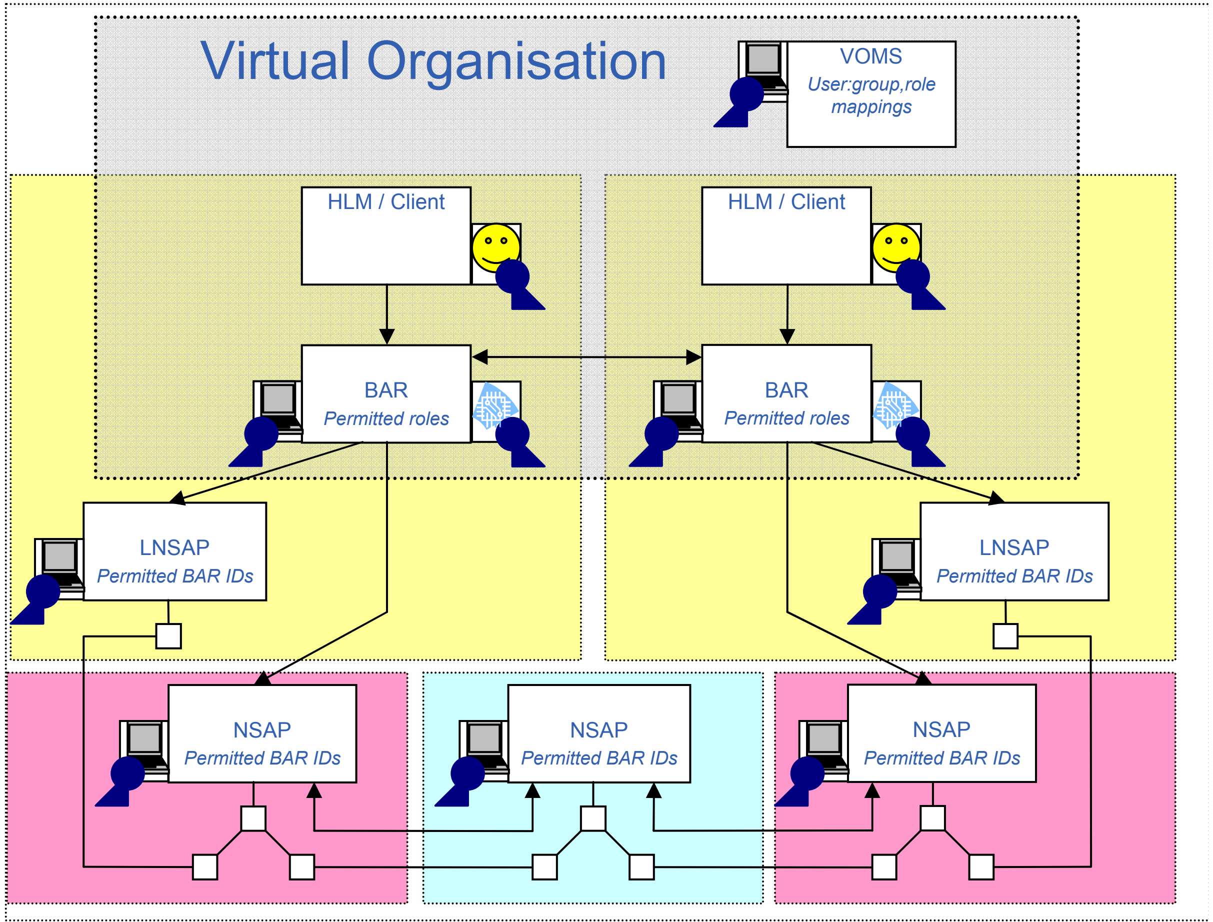
Alistair K Phipps (A.Phipps@ed.ac.uk)

University of Edinburgh

Architecture

- **Two separate levels of authentication / authorisation, allowing user to use standard grid credentials but not requiring networks to use VOMS**

- **EGEE VO:**
  - HLM – BAR north interface
- **Networks:**
  - BAR south interface – (L)NSAP

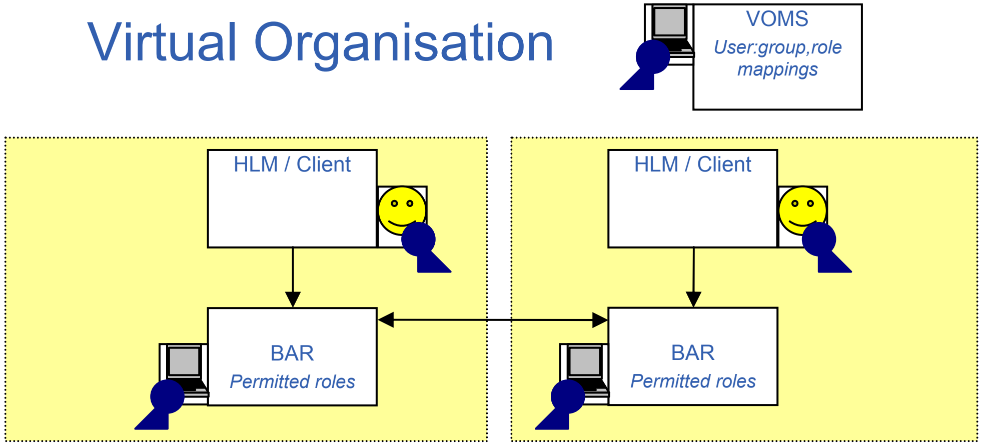


Implementation

- **Authentication:**
  - X.509v3 certificates used to identify users and hosts
  - CAs as roots of trust
  - EGEE domain:
    - EU Grid PMA approved CAs
  - Networks domain:
    - EU Grid PMA approved CAs recommended, but not mandatory
- **Authorisation:**
  - EGEE domain (for users):
    - Attribute certificates issued by VOMS; VOMS root of trust
  - Networks domain (for BARs):
    - List of authorised BAR DNs stored at each NSAP instance
- **Transport-Level Security (TLS) used – provides integrity and confidentiality protection**
- **Standard implementation provided by JRA3 modules (org.glite.security.util-java, org.glite.security.trustmanager)**
- **Checks on certificates include expiry date, CRLs, roots of trust (CA trusted, VOMS trusted) - will not mention these further**

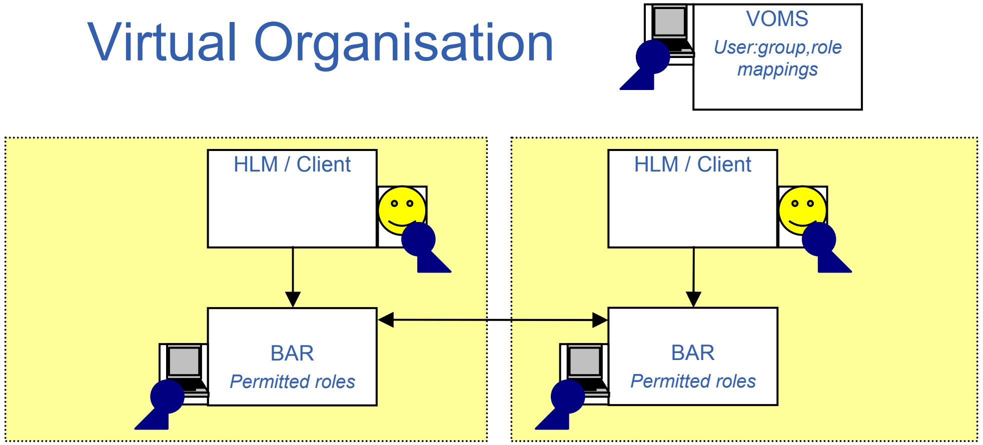
HLM-BAR Security (1)

- Security between HLM and BAR is based on use of standard grid user credentials (not JRA4 specific)
- User has X.509v3 certificate
- Generates Proxy, including Attribute Certificate from VOMS describing authorised roles (voms-proxy-init)
- Proxy delegated to HLM
- All of this is JRA1/JRA3 domain



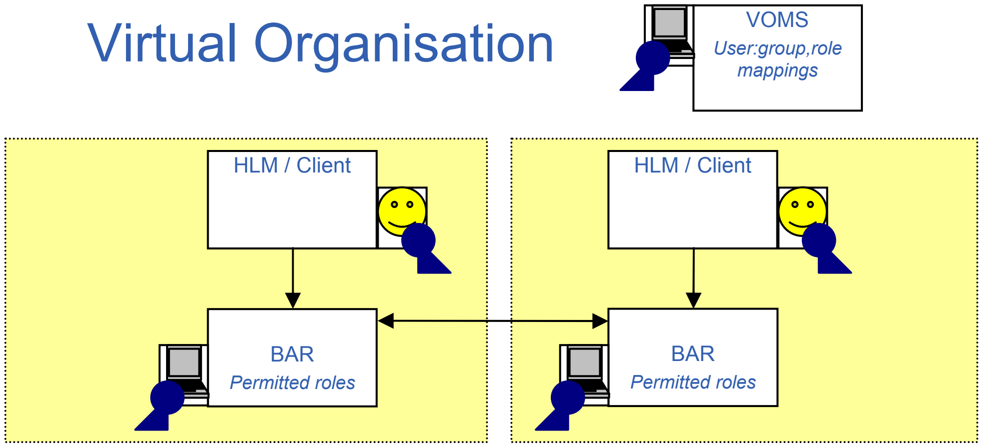
HLM-BAR Security (2)

- HLM contacts BAR and authenticates BAR based on BAR’s presented host certificate
- BAR authenticates HLM based on presented proxy certificate
- HLM sends request to BAR
- BAR authorises request if proxy contains attributes signed by VOMS with roles specified matching those authorised to make the request
- HLM delegates proxy to BAR



BAR-BAR Security

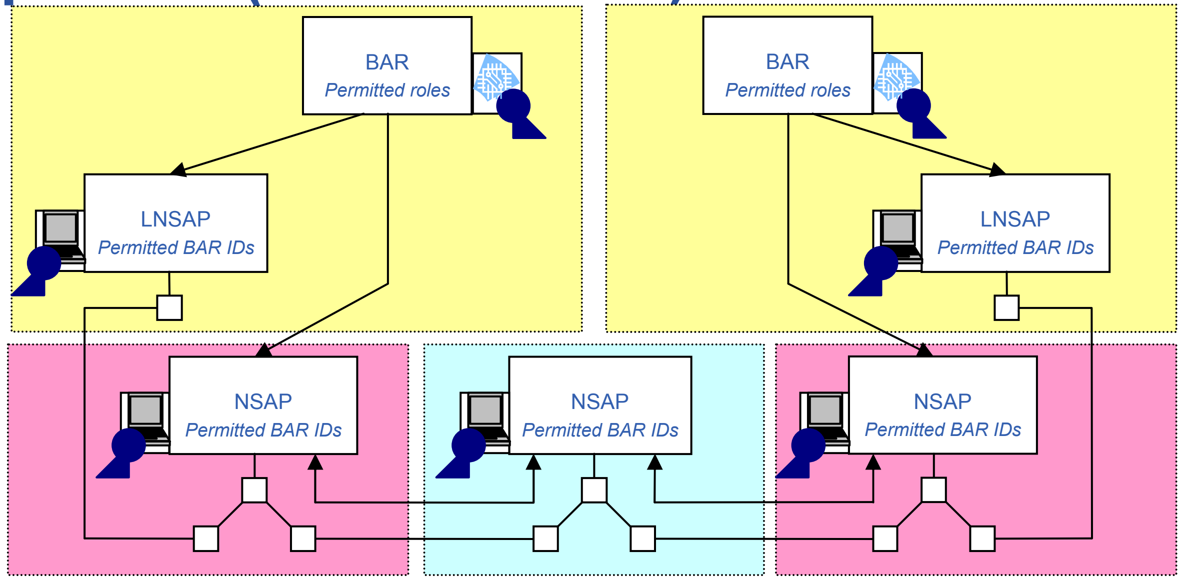
- BAR must contact remote BAR so remote BAR can set up remote LNSAP
- BAR acting as a client uses delegated user's proxy – security / request flow exactly as for HLM-BAR



Enabling Grids for E-sciencE

BAR-NSAP Security

- BAR connects to NSAP
- NSAP authenticates BAR based on presented service certificate
- BAR authenticates NSAP based on presented host certificate
- BAR sends request to NSAP
- NSAP checks BAR's service certificate Distinguished Name is on local list of allowed Distinguished Names for action requested (authorisation)



References

- **More details on the security architecture in BAR Security Architecture document in EDMS – currently being reviewed by JRA3:**
  - https://edms.cern.ch/document/571891
- **To be considered:**
  - Impact of Notification (NSAP->BAR, BAR->HLM)