

Security in EGEE

EGEE

- Slides based on an EGEE document:
- P Hobson, March 2008

Global Security Architecture

FOR WEB AND LEGACY SERVICES

EU Deliverable DJRA3.3

Document identifier: **EGEE-JRA3-TEC-602183-DJRA3.3-v-1-2**

Date: **2005-09-08**

Activity: **JRA3: Global Security Architecture**

Document status: **FINAL**

Document link: **<https://edms.cern.ch/document/602183/>**

X509 Security

Single sign-on provided by Proxy Certificates

Shibboleth is an alternative browser-centric infrastructure for security which is becoming “grid aware”

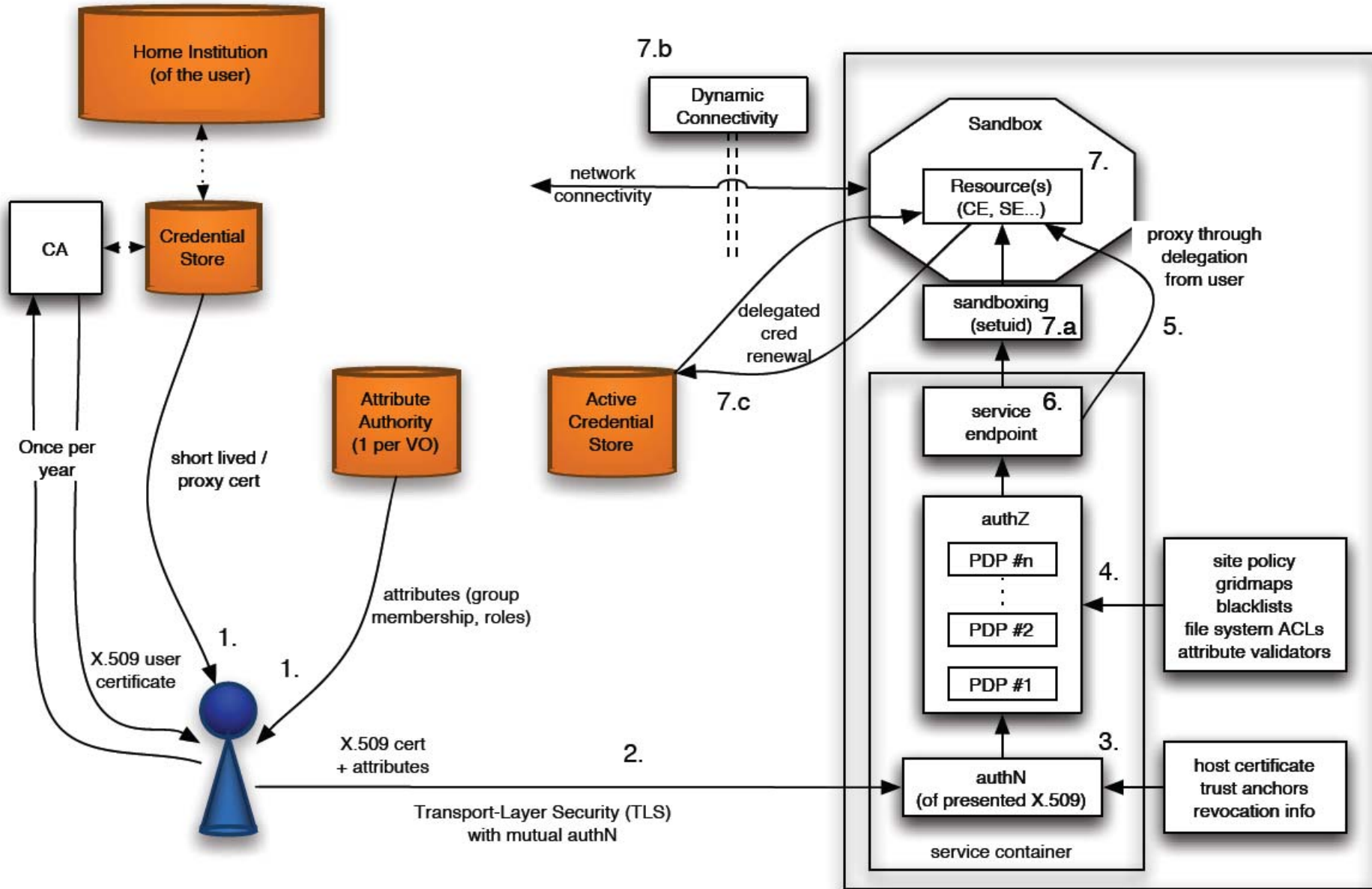
M. Myers et al. RFC2560: X.509 Internet Public Key Infrastructure Online Certificate Status Protocol (OCSP). <http://www.ietf.org/rfc/rfc2560.txt>.

R. Housley et al. RFC3280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. <http://www.ietf.org/rfc/rfc3280.txt>.

S. Tuecke et al. RFC3820: Internet X.509 Public Key Infrastructure (PKI) Proxy Certificate Profile. <http://www.ietf.org/rfc/rfc3820.txt>.

V. Welch, T. Barton, K. Keahey, and F. Siebenlist. Attributes, Anonymity, and Access: Shibboleth and Globus Integration to Facilitate Grid Collaboration. In *4th Annual PKI R&D Workshop*, 2005.

Components of Security architecture



Collection of authorization policy

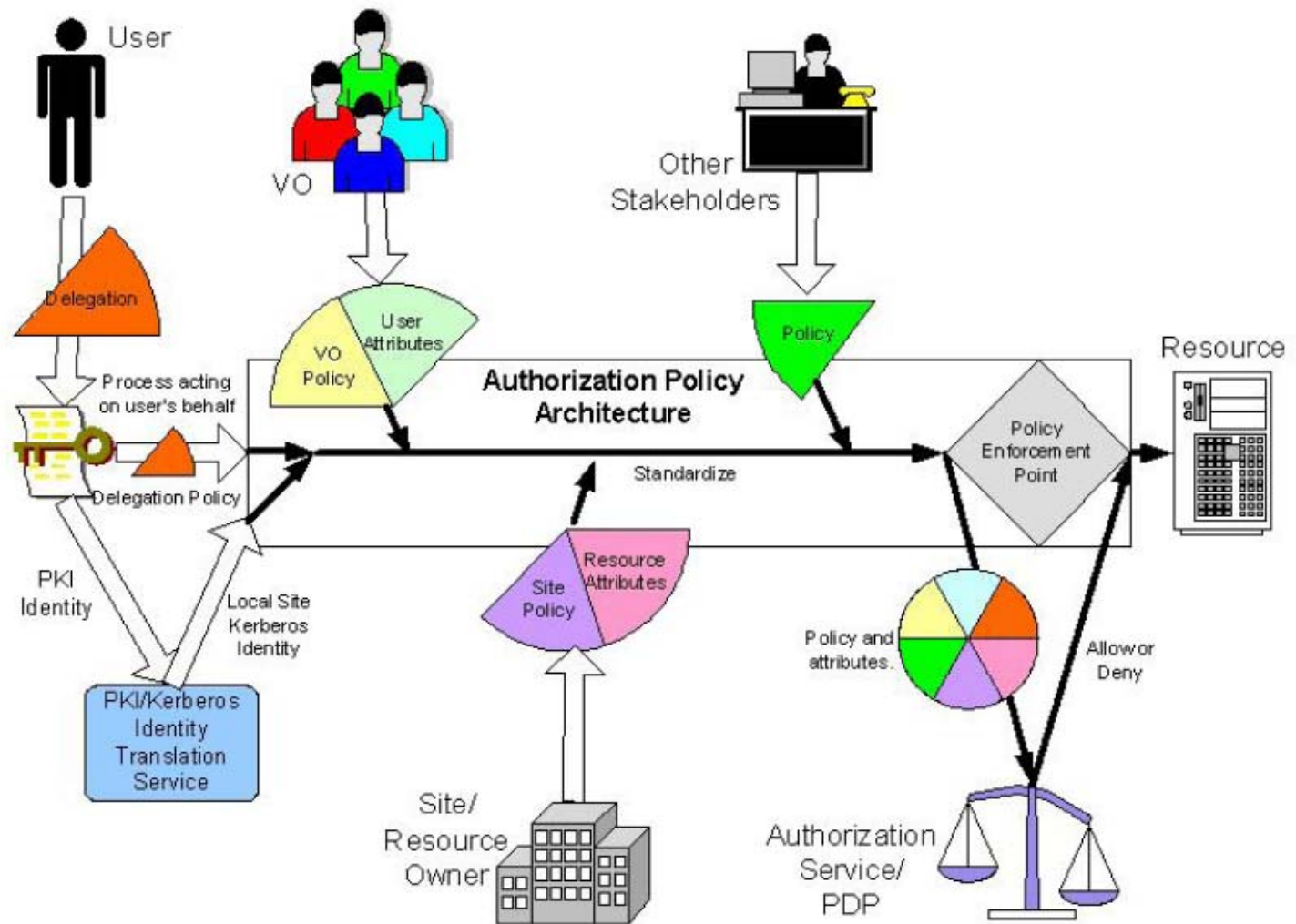


Figure 4: Conceptual view of a framework for collecting authorization policy from different stakeholders and combining them into a final authorization decision. Graphics from Globus Alliance and the security design team in the GGF OGSA working group.

Framework Concept

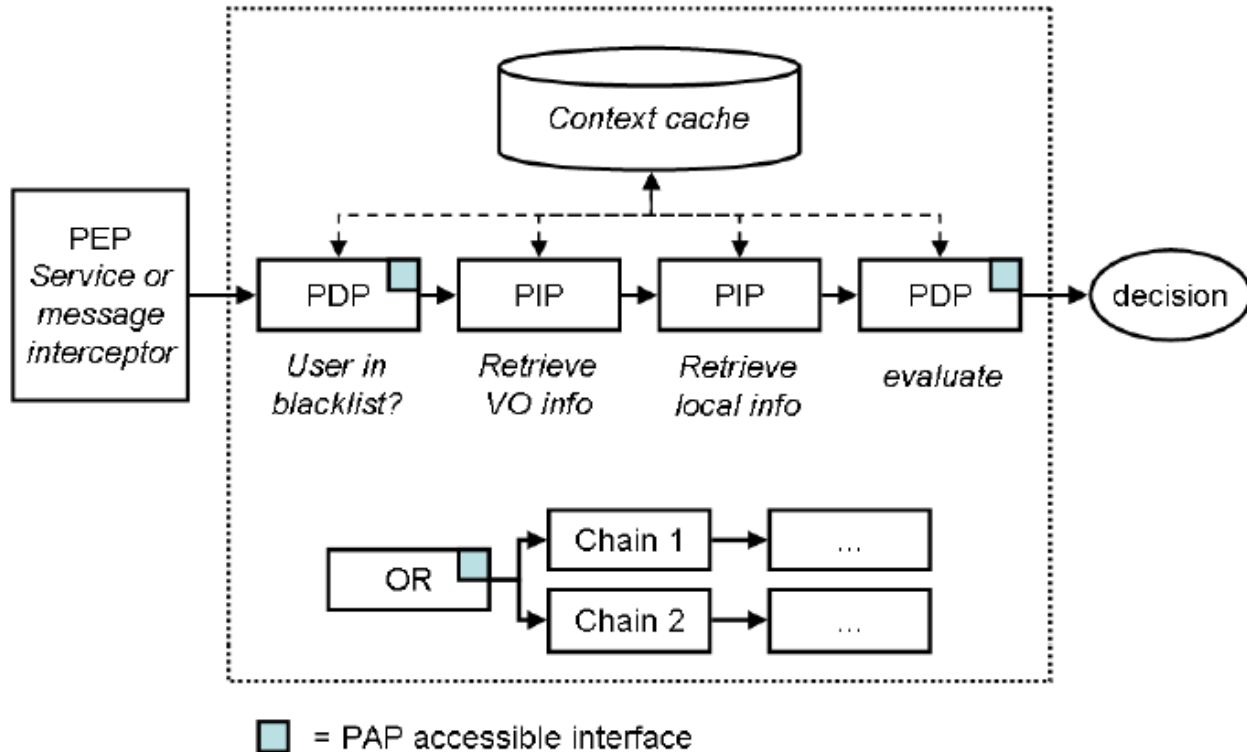


Figure 5: Conceptual model of the authorization framework, invoked from a evaluation point (PEP) in the application or service container. The authorization request and associated metadata is subsequently routed through a chain of information collectors (PIP), policy-driven decisions (PDP), or modules that perform logical operations on results from an underlying collection of chains (in the picture depicted by an OR).

Generic Service Request Sequence

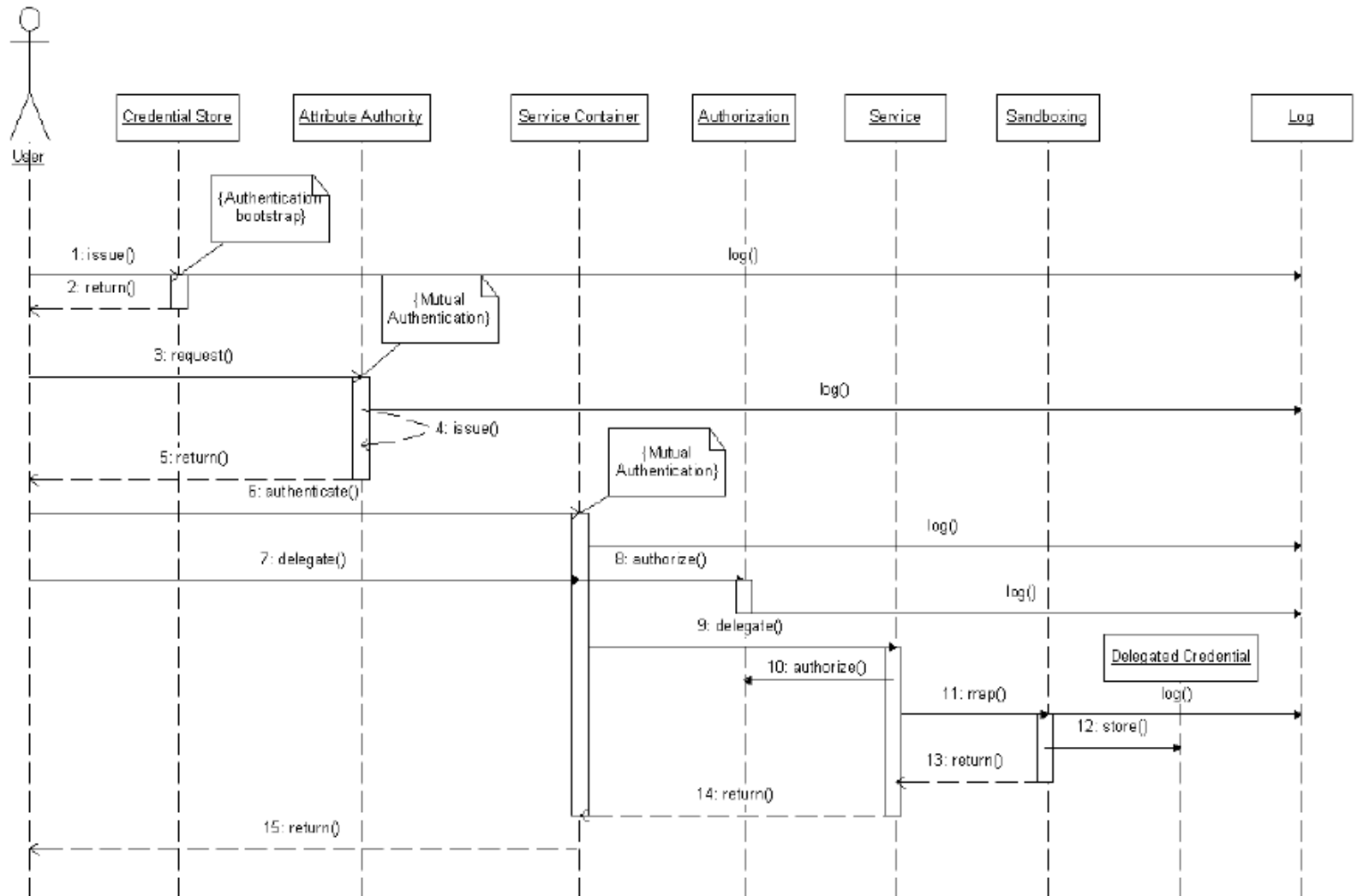


Figure 6: Sequence diagram over security architecture components and their interactions (1 of 2).