Grid Security

Current Status and Future Development

Christoph Witzig, SWITCH
(christoph.witzig@switch.ch)

www.eu-egee.org

Information Society and Media

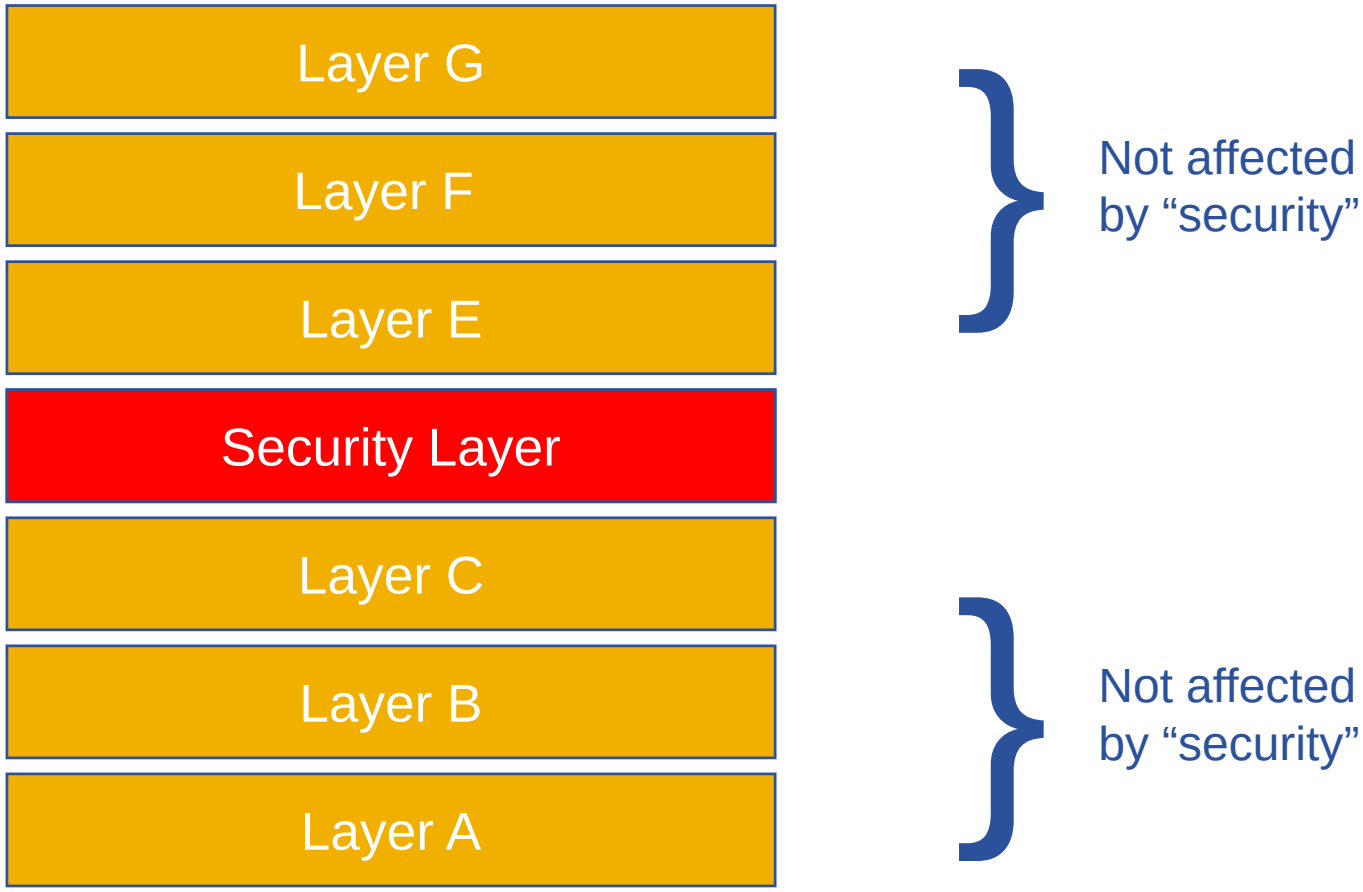
Outline

- Introduction
- Authentication and Authorization
- Delegation
- Outlook
- Summary

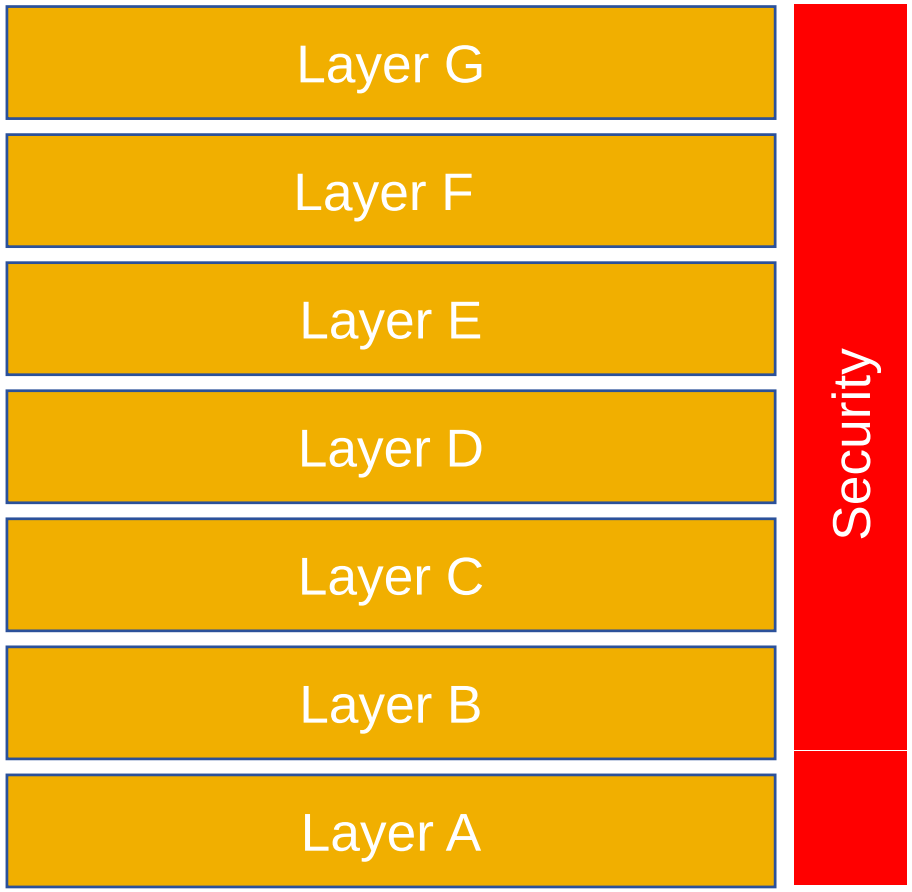
Properties of Security

- **The one and only nice property of security:**
  - Security creates assurance
  - ***> That's why we need it!***
- **A pretty useless property of security:**
  - Security doesn't add functionality
  - ***> That's why we are tempted to ignore it!***
- **The many stupid properties of security:**
  - Imposes limits, which often vary over time (often suddenly)
  - Creates dependencies on things beyond our control
  - Is utterly unimpressed by cool features, but forces us to think about very weird stuff happening in weird circumstances
  - In short: it's a pain!
  - ***> That's why we hate it!***

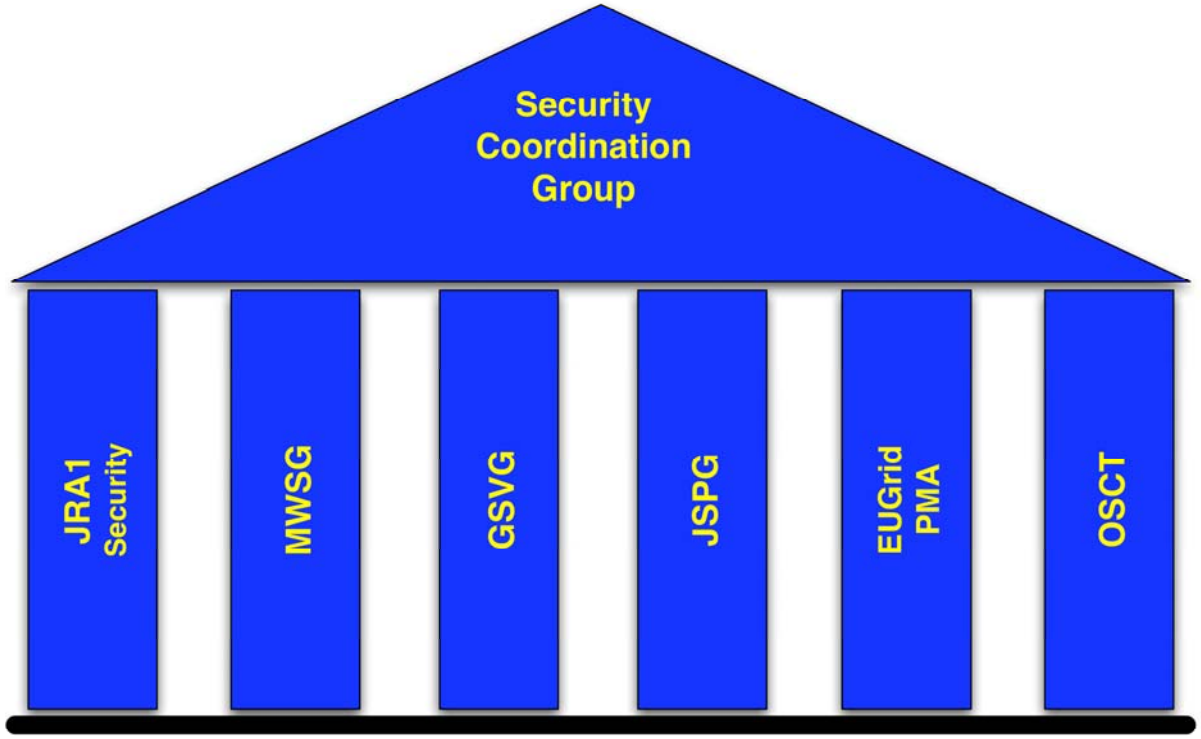
The ideal solution …



… and the Real World



EGEE Security Organization



JRA1 / Security

Middleware Security Group

Grid Security Vulnerability Group

Joint Security Policy Group

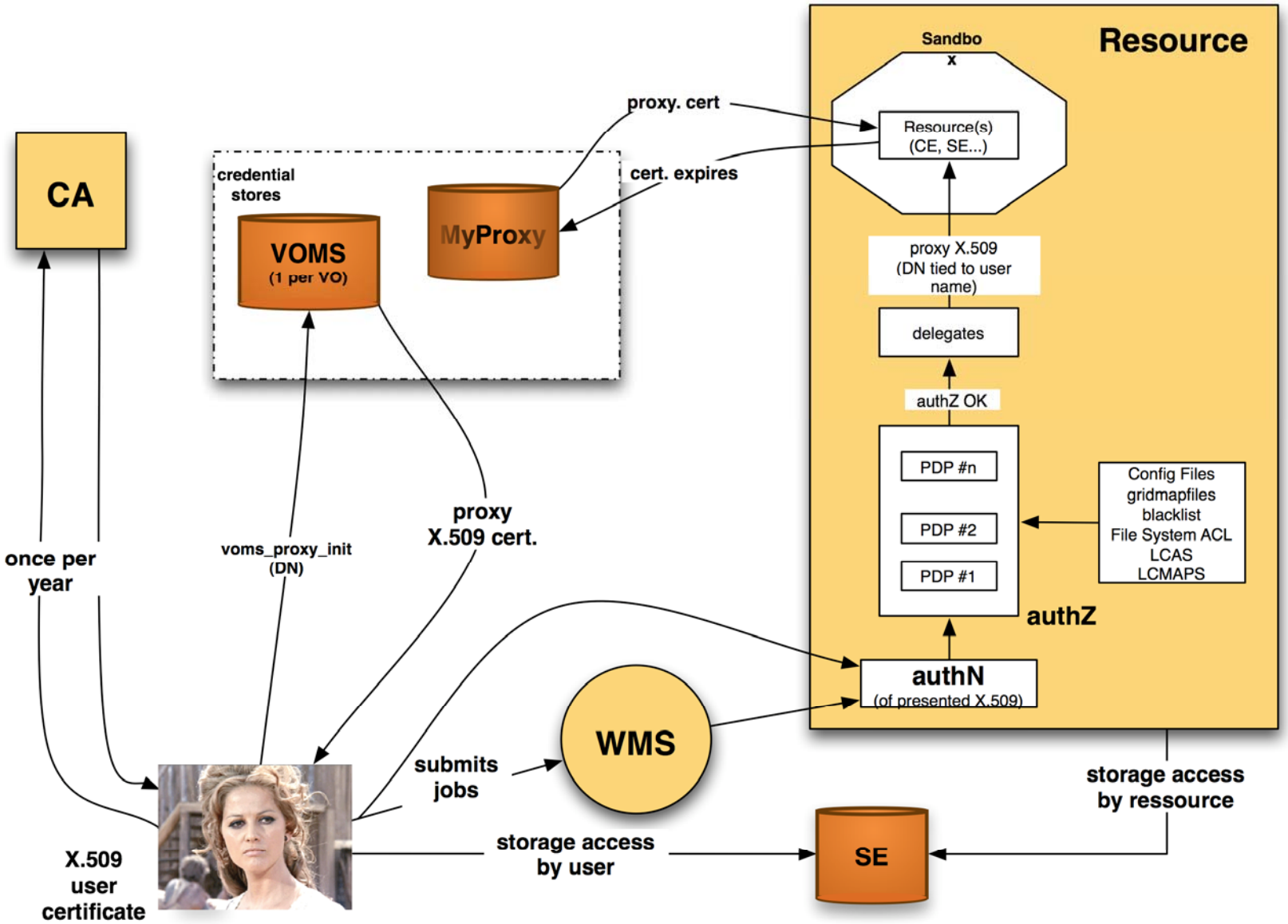
EUGridPMA

Operational Security Coordination Team

http://www.eu-egee.org/security/

Security in EGEE-III: 440 PM

Security and the Grid



Outline

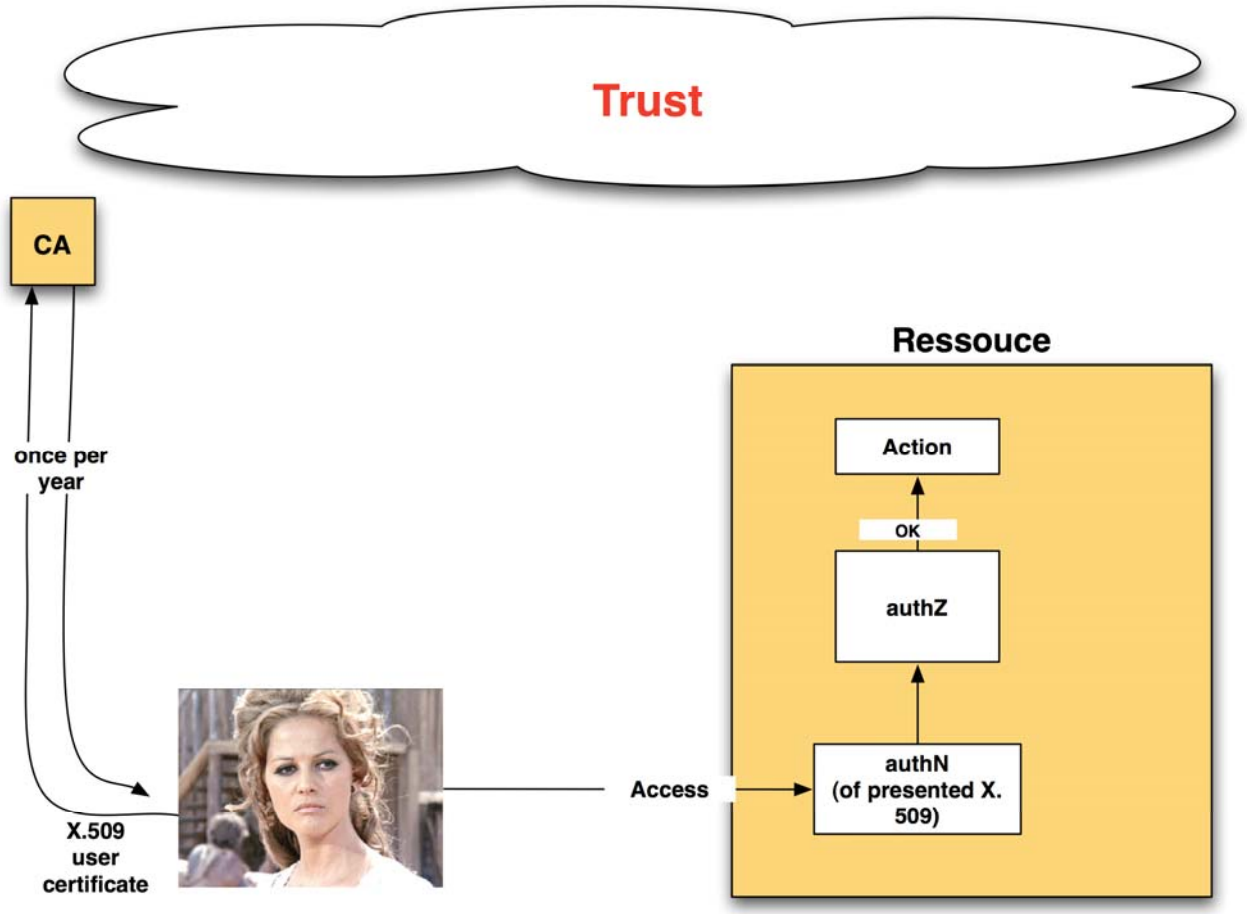
- Introduction
- **Authentication and Authorization**
- Delegation
- Outlook
- Summary

AA: Terminology

- **Authentication (authN):**
  - Process of ensuring a credential is valid and belongs to the individual that presents it.
- **Authorization (authZ):**
  - Process of checking that "someone" has the rights to perform an operation.
- **Note:**
  - authN and authZ are two different things
  - They don't have to be done by the same service

- **authN:**
  - Ensuring the user has the private key to the certificate that he provides
    - Note: This does not mean that the holder of the private key is the intended recipient of the private key!
  - Performing a trust evaluation on a certificate

AuthN and PKI (1/2)



Trust = process of ensuring that the issuer of a credential, and the credential itself, is trustworthy

AuthN and PKI (2/2)

- **Trusted Third Parties (TTP):**
  1. "Quality" of the TTP:
     - Operational procedures, general conduct of TTP
  2. Quality of the initial identity vetting
  3. Security of the private data needed to prove the possession of the credential (private key)

  1 and 2 can be controlled through common TTP guidelines (IGTF)

  In PKI: only the user controls item 3

PKI Consequences for the User

- **He must get a certificate from a trusted CA to access the Grid**
  - These CAs exist outside the realm of his institution
  - Consequence 1: Tedious process to obtain a certificate

- **Most Grid users have the private key as a file**
  - Consequence 2: User is responsible for properly protecting the private key
    - Good passphrase
    - Proper file permissions
    - No “random” copying to any host

private key is something very precious

that has to be looked after

PKI Consequences for the Infrastructure

- **Co-ordination of TTP, distribution of trust**
  - EUGridPMA
  - IGTF
- **Mechanisms**
  - to provide certificate to the user
  - to renew certificate of the user
  - to revoke certificate of the user
  - to distribute revocation information
  - to check validity of the certificate
- **Future?**
  - Easier credential to manage and operate

AuthZ (1/2)

- **Authorization (authZ):**
  - Process of checking that “someone” has the rights to perform an operation.
- **Examples:**
  - Ensuring the DN is present in a configuration file that lists all authorized users
  - Insuring that an attribute listed in the extension of the certificate has a certain value in order to perform an operation
- **Authorization criteria:**
  - Identity: resources must know identity, no privacy
  - Attributes: flexible scheme, independent of identity, allows for privacy, requires common understanding of attributes
  - Tokens: requires token service

AuthZ (2/2)

- **Initial Grid middleware: identity based**
- **Current Grid middleware: “attribute-based”**
  - Groups and Roles in VOMS AC
  - Presence of attributes is required
- **Future Grid Middleware?**
  - Arbitrary key-value pair attributes
  - Common understanding of attributes through metadata
  - Attributes exist outside the credential (proxy)

Outline

- Introduction
- Authentication and Authorization
- **Delegation**
- Outlook
- Summary

Delegation and Proxies (1/2)

- **Delegation = process of empowering another entity to act on behalf of the user**
  - Delegation of the minimal subset of privileges necessary to perform the task
  - Limitation in time

- **In gLite: achieved through creation and propagation of proxy certificates**
  - Initial creation: by the user
  - Propagation: Grid services create key pair and let the requester create the proxy using the private key of the requestor
    - Consequence: private key never leaves the host
  - Access to the Grid “for a fist full of proxies”

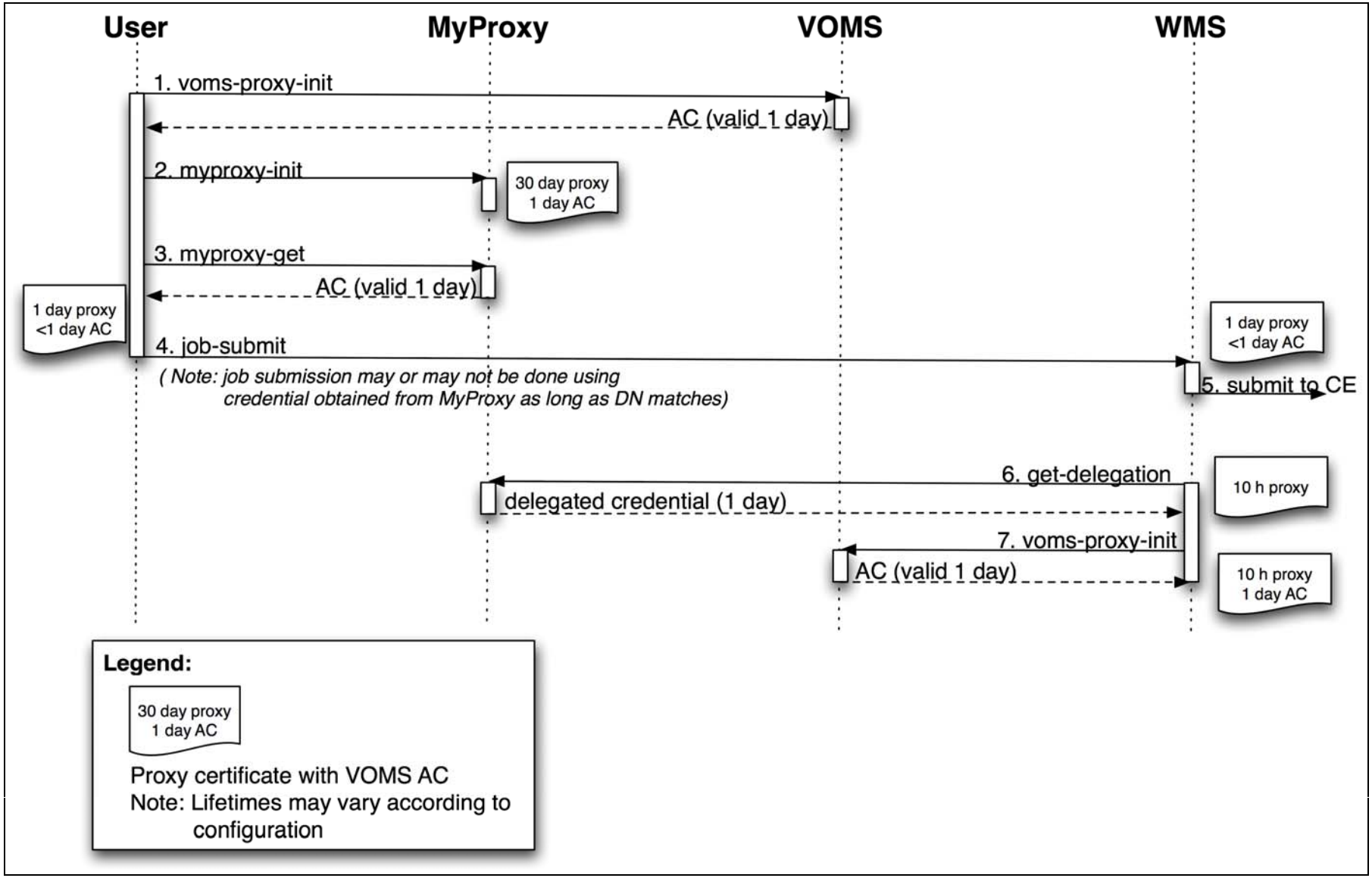
Delegation and Proxies (2/2)

- **Proxies:**
  - **Should** be limited for only a short amount of time
  - Cert file contains private key
  - Don't really implement principle of least privilege

- **Consequences:**
  - Must be renewed in order to support long-running jobs
  - Only protected by file access restriction
  - More than a "fist full of proxies" lay around all over the Grid
  - Proxy certificate cannot be revoked

- **Renewal process:** ("for a few proxies more")
  - Involves storing long-lived proxies (certificates) in a certificate store, from where a new (short-lived) proxy can be obtained
    - Security of storing long-lived proxies centrally
    - Need to renew not only proxy but also VOMS AC

Proxy Renewal



Consequences

- **Dependencies between services in order to keep proxies valid**
- **No concept of anonymity and privacy**
- **Pseudonymity**
  - Service has been implemented in EGEE-II
  - Not widely used

Outline

- Introduction
- Authentication and Authorization
- Delegation
- **Outlook**
- Summary

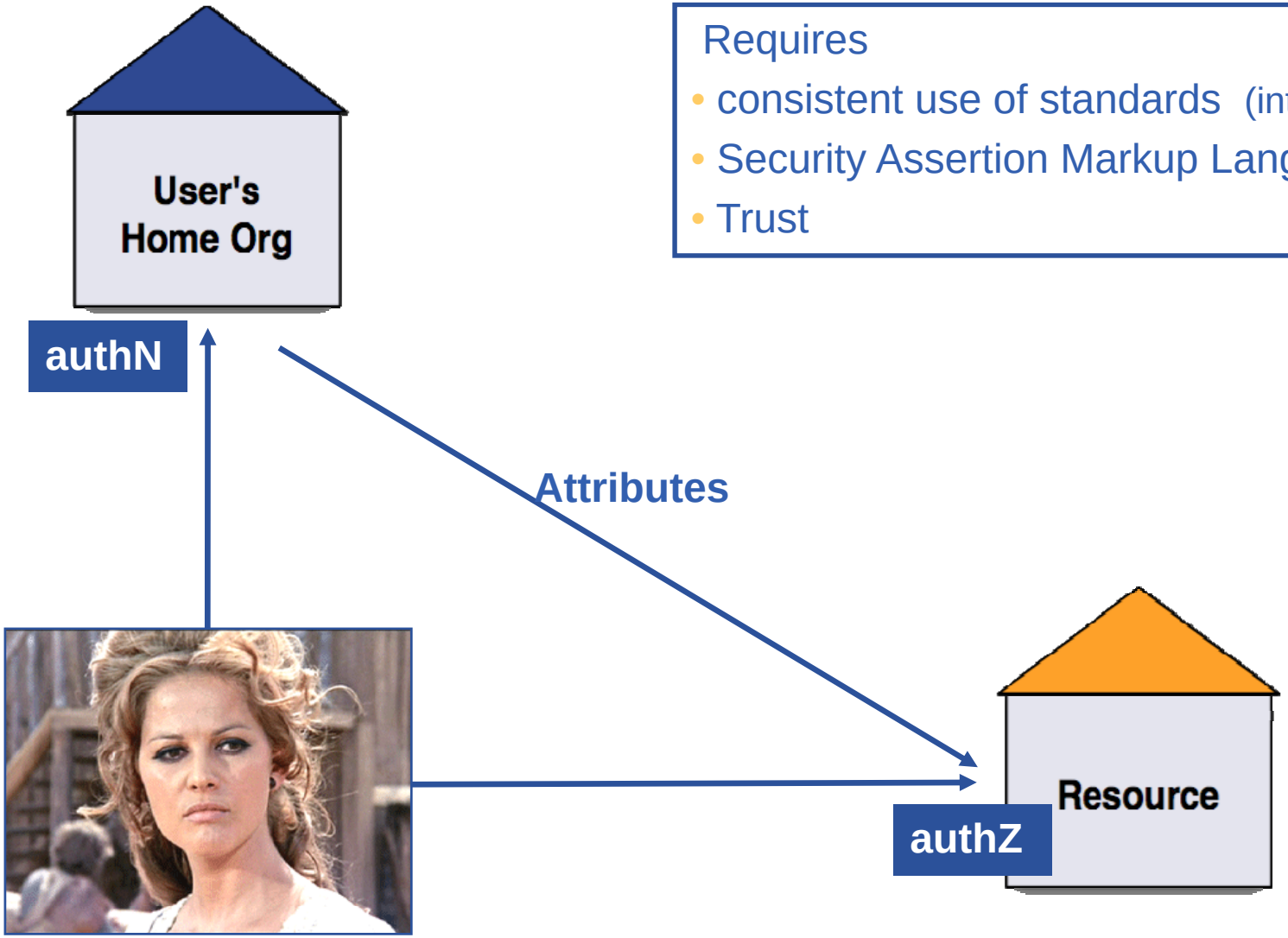
Federated Identity (1/2)

- **Federated Identity:**
  - Secure exchange of identity information across administrative boundaries
  - “The virtual reunion, or assembled identity, of a person's user information (or principal), stored across multiple distinct identity management systems”

- **Authentication and Authorization Infrastructures: AAI**
  - Are emerging in Europe
  - Mostly driven by National Research and Education Networks (NREN)
  - Example: SWITCHaai
    - ~250’000 users (95% of academic community in Switzerland)
    - Based on Shibboleth

Federated Identity (2/2)

Requires
- consistent use of standards (interoperability)
- Security Assertion Markup Language
- Trust



Interoperability Grid - AAI (1/2)

- **Use AAI to issue user X.509 certificate**
  - Short credential service (SLCS)
  - Lifetime less than 1 mio sec (~11.5 days)
  - Requires high quality AAI

- **First SLCS CAs in use, others being planned**

- **Main benefits:**
  - For the user:
    - Obtains X.509 in a simple way
    - In principle needs only one main credential
  - For the infrastructure:
    - Leverages AAI and CA

Interoperability Grid - AAI (2/2)

- **Portals allow making security invisible**
  - Typically specific for a given user community
- **Attribute aggregation between institution and VO**
  - Interoperability at VOMS level
- **But making all Grid service interoperable with security domains other than PKI will be hard**
- **Security Token Services:**
  - Allow transformation of different security tokens
    - e.g. SAML into X.509

Outline

- Introduction
- Authentication and Authorization
- Delegation
- Outlook
- **Summary**

Summary (1/2)

- **Grid security based on X.509**
  - For the user: Difficult to understand and handle
  - For the infrastructure: labor-intensive
- **Key building blocks:**
  - authN and authZ
    - Should be viewed as two different steps
  - Delegation
    - Leads to proxy certificates, hard to replace
- **Interoperability AAIs and Grids**

Summary (2/2)

Security is only as good as its weakest link, and people are the weakest link in the chain

Bruce Schneier, Secrets and Lies in a Digital Networked World

Keep your private key safe !