Enabling Grids for E-sciencE

Policy Obligations - Bridging two fundamental security concepts

JRA1 All-Hands, NIKHEF, 20-22 February 2008

Yuri Demchenko
SNE Group, University of Amsterdam

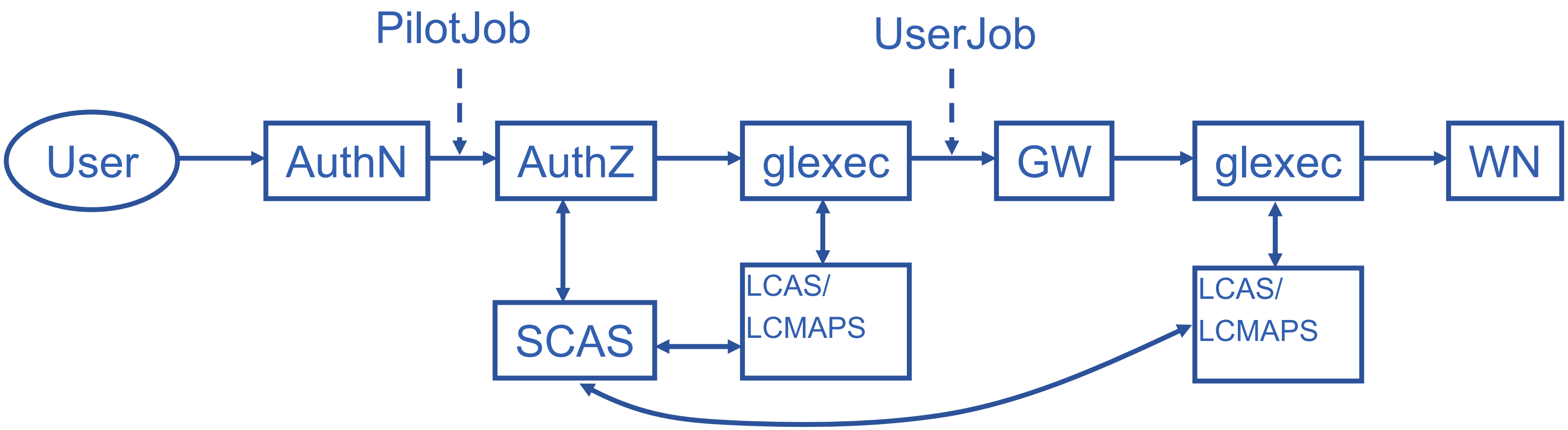
www.eu-egee.org
www.glite.org

Information Society and Media

Obligations for Interoperability in Grid

- **Part of the site centric SCAS based AuthZ infrastructure**
- **One of the main focuses of the AUTHZ-INTEROP initiative between OSG-EGEE-GT**
  - List of Obligations and their semantics
  - SAML-XACML Extension Library for OpenSAML2.0
- **Other components**
  - Obligations Handling Reference Model (OHRM)
  - Obligation Handler API and SAML-XACML design document
    - *to be finalised*
  - XACML Conformance test for typical and registered Obligations – *still to be done*
- **Another outcome**
  - IMHO, indicated a need for Grid security architecture and model re-thinking

Obligations and Pilot job use cases



- Introducing SCAS as external AuthZ service called from protected environment changes simple security model
  - AuthN-AuthZ-glexec flow needs analysis
  - Behind each (SCAS) policy should be clear operational model
- SCAS is verified to be compatible with the XACML policy and PDP
  - XACML uses pluggable security service model (i.e. called from major Service)
  - glexec is a kind of gateway/border device

Obligations in Access Control and Management

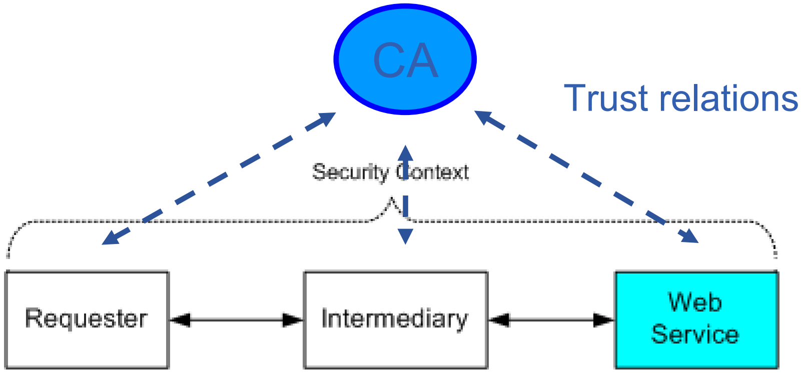
- **Access control in Grid and Policy Obligations**
  - Account mapping
  - Quota assignment
  - Environment setup/configuration
- **General Complex Resource provisioning**
  - Fixed, Time-flexible, Malleable/"Elastic" Scheduling
  - Usable Resource
- **Other/general**
  - Accounting, Logging, Delegation

- **Obligations in access control and policy based management**
  - Obligated policy decision
  - Provisional policy decision

OSI-Security vs TCB Security

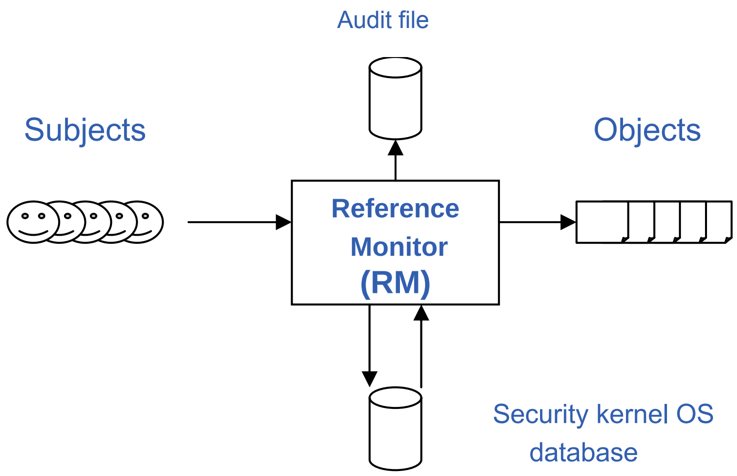
Open Systems and Internet

- Open Systems Interconnection (OSI) Security Architecture
  - ISO7498-2/X.800
- Independently managed interconnected system
- Trust established mutually or via 3rd party
- PKI and PKI based AuthN and key exchange
- Concept of the Security Context



Trusted Computing Base (TCB)

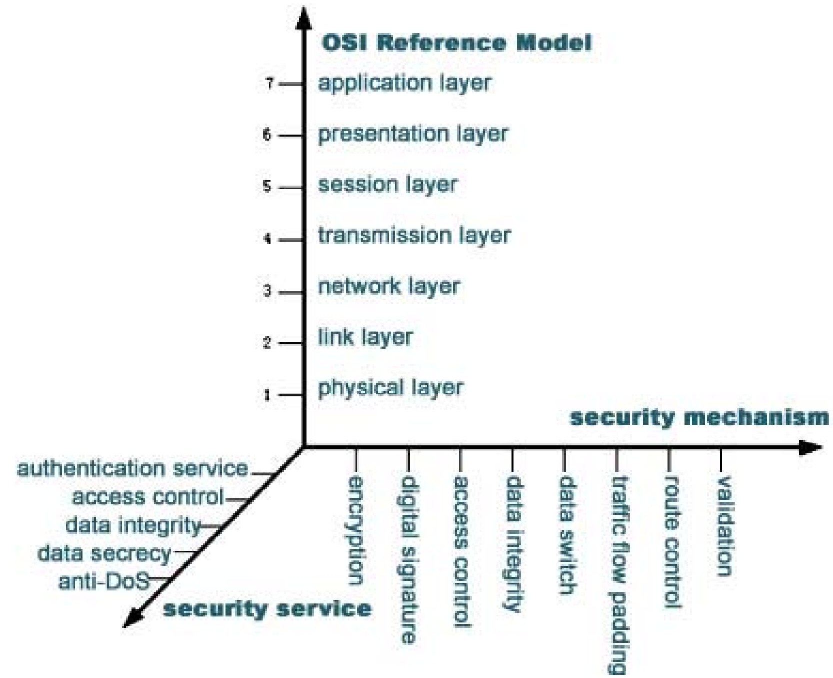
- Reference Monitor (RM) by J.P.Anderson “Computer Security Planning Study” (1972)
- Models Bell-LaPadula and Biba
- Certification criteria TCSEC/Common Criteria (1984)
  - A1, B1, B2, B3, C1, C2, D



X.800/OSI Security – Layers vs Services vs Mechanisms

Service \ Mechanism ->	Encipherment	Digital signature	Access control	Data integrity	Authentication exchange	Traffic padding	Routing control	Notarization
Authentication, Peer entity	Y	Y			Y			
Authentication, Data origin	Y	Y						
Access control service	Y		Y					
Connection confidentiality	Y						Y	
Connectionless confidentiality	Y						Y	
Selective field confidentiality	Y							
Traffic flow confidentiality	Y					Y	Y	
Connection Integrity with recovery	Y			Y				
Connection integrity without recovery	Y			Y				
Selective field connection integrity	Y			Y				
Connectionless integrity	Y	Y		Y				
Selective field connectionless integrity	Y	Y		Y				
Non-repudiation. Origin		Y		Y				Y
Non-repudiation. Delivery		Y		Y				Y

Service	Layer 1	2	3	4	5	6	7*
Peer entity authentication			Y	Y			Y
Data origin authentication			Y	Y			Y
Access control service			Y	Y			Y
Connection confidentiality	Y	Y	Y	Y		Y	Y
Connectionless confidentiality		Y	Y	Y		Y	Y
Selective field confidentiality						Y	Y
Traffic flow confidentiality	Y		Y				Y
Connection Integrity with recovery				Y			Y
Connection integrity without recovery			Y	Y			Y
Selective field connection integrity							Y
Connectionless integrity			Y	Y			Y
Selective field connectionless integrity							Y
Non-repudiation Origin							Y
Non-repudiation. Delivery							Y



- Similar model should be probably proposed for WS SOAP based security services and mechanisms
- Layers model for above Application layer are uncertain

From OSI/Internet to SOA/WSA Security Model

- **X.800 Security Architecture for Open Systems Interconnection for CCITT applications. ITU-T (CCITT) Recommendation, 1991**
  - ISO 7498-2:1989 Information processing systems -- Open Systems Interconnection -- Basic Reference Model -- Part 2: Security Architecture
- **Web Services Security Roadmap (2002)**
  - http://www.ibm.com/developerworks/library/specification/ws-secmap/
- **OGSA Security Model Components (2002-2006)**
  - GFD.80 - OGSA version 1.5, Section 3.7 Security Services
  - Re-states Web Services Security roadmap
- WS-Security stds specify using SOAP header for security related issues
  - Considered as orthogonal to major service

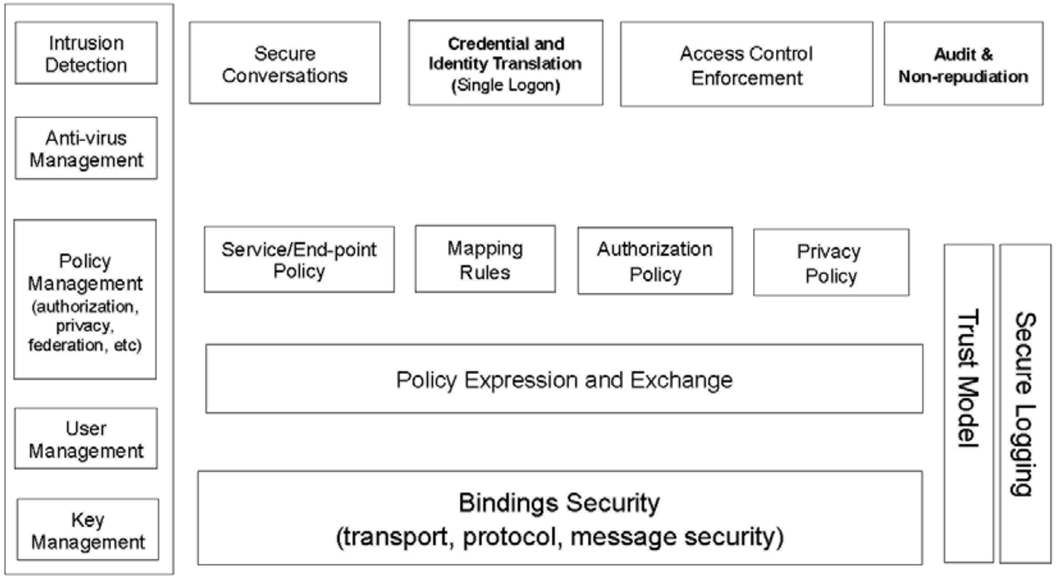
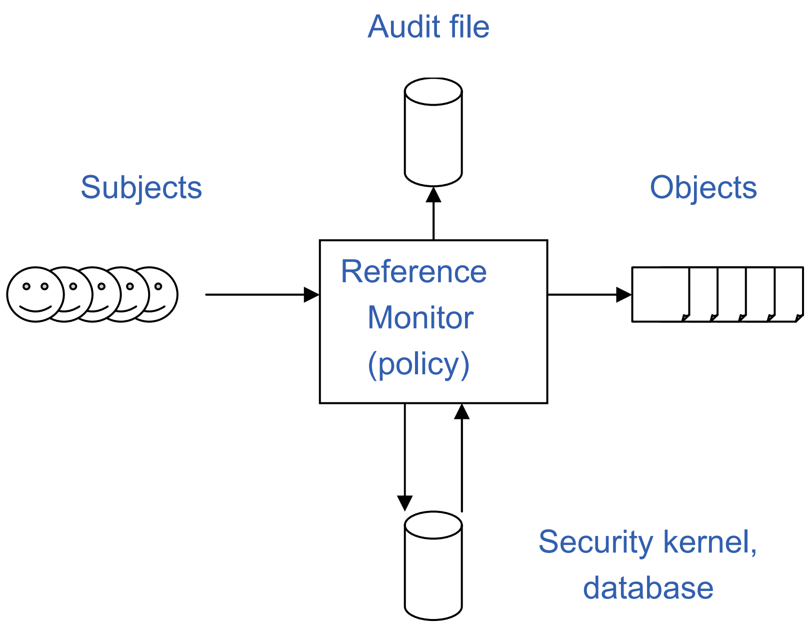


Figure 2: Components of Grid Security Model

Reference Monitor (RM) Concept



Proposed by J.P. Anderson in the report "Computer Security Planning Study" (1972)

RM property provides a basis for Multi-Level Security (MLS)

- **Complete mediation:** The security rules are enforced on every access, not just, for example, when a file is opened.
- **Isolation:** The reference monitor and databases must be protected from unauthorized modification.
- **Verifiability:** The reference monitor's correctness must be provable. That is, it must be possible to *demonstrate mathematically* that the reference monitor enforces the security rules and provides complete mediation and isolation.

- RM concept is a basis for TCB certification

Multi-Level Security Models

- **Bell–LaPadula (BLP) model**
  - No write down
  - No read up
- Focus – Confidentiality
  - Mandatory Access Control
- Applicability – Data
- Known flaw – not protected against insider “worm” virus

- **Biba model**
  - No write up
  - No read down
- Focus – Integrity
- Applicability – (Open) Data and Control/Mngnt

- **TCSEC Common Criteria**
  - A1 – B3 + formally/mathematically verified design
  - B1-B3 – Multilevel security, Formal security model, Mandatory AC
  - C1-C2 – Discretionary access control model, auditable user activity
  - D – minimal protection
  - Currently replaced by ISO 15408 Evaluation Assurance Level (EAL)

TCSEC/ISO Common Criteria

- **TCSEC Certification Criteria**
  - A1 – B3 + formally/mathematically verified design
  - B3 – Clear security model and layered design, Security functions tamperproof, Auditing mandatory
  - B2 – Least-privilege access control model, Certifiable security design implementation, *Covert channels analysis*
  - B1 – Labelled security protection, MAC-BLP + DAC
  - C2 – Discretionary access control model, auditable user activity
  - D – minimal protection

- **Currently replaced by ISO 15408 Evaluation Assurance Level (EAL)**
  - EAL1: Functionally Tested
  - EAL2: Structurally Tested
  - EAL3: Methodically Tested and Checked
  - EAL4: Methodically Designed, Tested and Reviewed
  - EAL5: Semiformally Designed and Tested
  - EAL6: Semiformally Verified Design and Tested
  - EAL7: Formally Verified Design and Tested

- **EAL1-4 – commercial systems, EAL5-7 - special systems (EAL4 circa C2)**
  - Windows NT (EAL4+) and many routing and Unix systems certified for EAL4

Clark – Wilson Integrity Policy

Criteria for achieving data integrity (primary target for reliable business operation)

- Authentication of all user accessing system
- Audit – all modifications should be logged
- Well-formed transactions
- Separation of duties

Enforcement Rules

E1 (Enforcement of Validity) - Only certified TPs can operate on CDIs

E2 (Enforcement of Separation of Duty) - Users must only access CDIs through TPs for which they are authorized.

E3 (User Identity) - The system must authenticate the identity of each user attempting to execute a TP

E4 (Initiation) - Only administrator can specify TP authorizations

Certification Rules

C1 (IVP Certification) - The system will have an IVP for validating the integrity of any CDI.

C2 (Validity) - The application of a TP to any CDI must maintain the integrity of that CDI. CDIs must be certified to ensure that they result in a valid CDI

C3 - A CDI can only be changed by a TP. TPs must be certified to ensure they implement the principles of separation of duties & least privilege

C4 (Journal Certification) - TPs must be certified to ensure that their actions are logged

C5 - TPs which act on UDIs must be certified to ensure that they result in a valid CDI

TP – transformational procedure; IVP – integrity verification procedure;
CDI – constrained data Item; UDI - unconstrained data Item

Grid Security Model(s) – Still to be created?

- **Strong&consistent AthN is a good principle, BUT**
  - Can be considered as sufficient only if a subject logs in the trusted environment (like server/UNIX)
  - There other security aspects
- **Use TCB (Secure OS) design principles**
  - Layered design
    - Hardware, kernel, OS, user
    - Most sensitive operations in the (resource) innermost circle
- **Introduce security zones model**
  - AuthN, (Delegation,) AuthZ, (AuthZ Session,) glexec/Unix
  - Keep security context
  - Use AuthZ session management concept and security mechanisms

Other Grid Security specifics - Open list

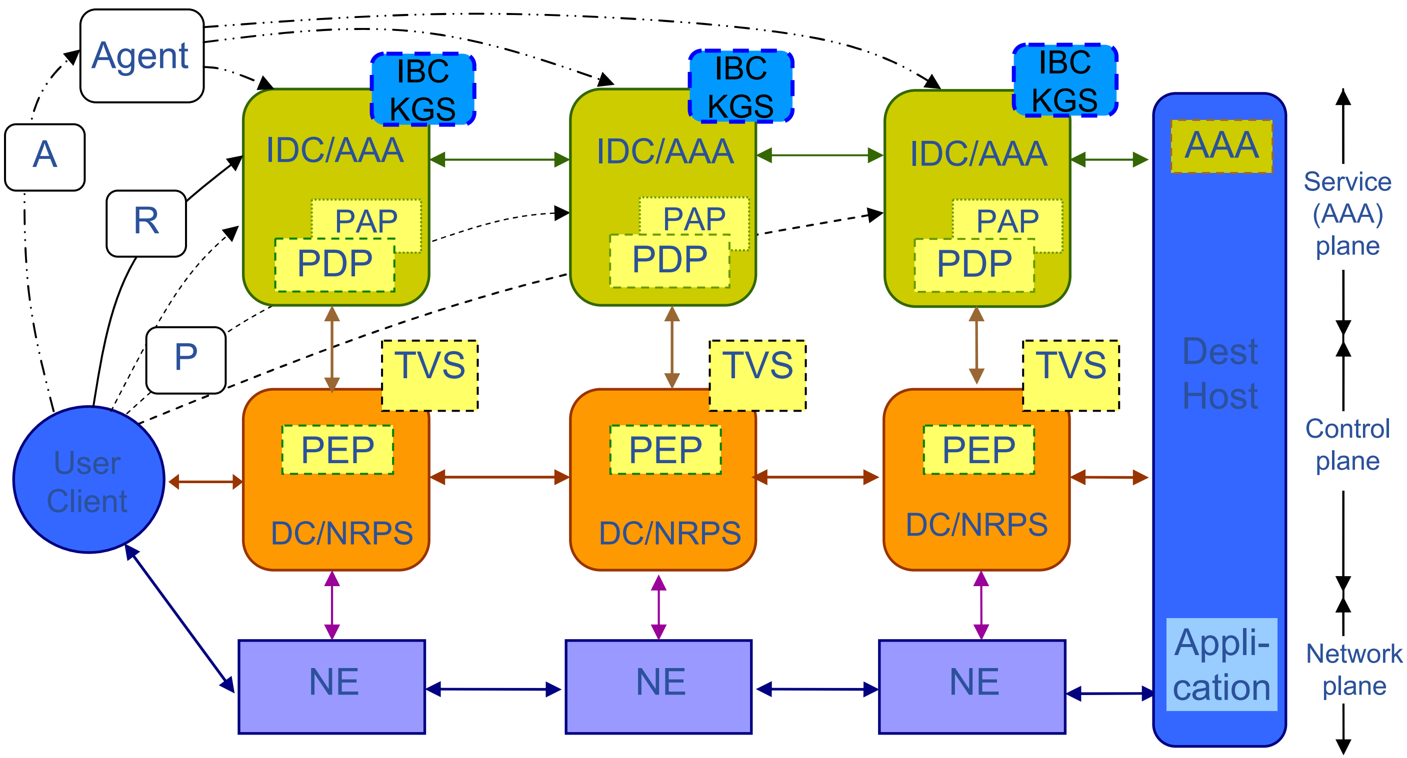
- **Re-factoring policy-based access control to policy-based object management**
  - Many use cases in Grid job processing workflow fit better into generic policy based object management than to access control
    - Policy (and access conditions) are attached to the object (i.e. job) at its invocation and checked locally by glexec or RM
- **Virtualisation**
  - Provides specific operational and security environment for security services
- **Trusted Computing Platform Architecture (TCPA)**
  - Provides a basis for inter-connecting trusted computing hosts/environments
  - Defines Trusted Network Connect framework (TNC)
  - Allows combination with the Virtualisation platform to extend user-trusted environment to remote hosts

PKI vs IBC

Identity Based Cryptography (IBC)

- **Uses publicly known remote entity's identity as a public key to send encrypted message or initiate security session**
  - Initially proposed by Shamir in 1984 as an alternative to PKI
    - Shamir is one of the RSA inventors in 1977 (Rivest, Shamir, Adleman)
  - Identity can be email, domain name, IP address
  - Allows conditional private key generation
- **Requires infrastructure different from PKI but domain based (doesn't require trusted 3rd party outside of domain)**
  - Private key generation service (KGS)
    - Generates private key to registered/authenticated users/entities
  - Exchange inter-domain trust management problem to intra-domain trust

Using IBC for key distribution in multidomain NRP



Provisioning sequences

- Agent (A)
- Polling (P)
- Relay (R)

Token based policy enforcement

- GRI – Global Reservation ID
- AuthZ tickets for multidomain context mngnt

NRPS – Network Resource Provisioning System

DC – Domain Controller

IDC – Interdomain Controller

AAA – AuthN, AuthZ, Accounting Server

PDP – Policy Decision Point

PEP – Policy Enforcement Point

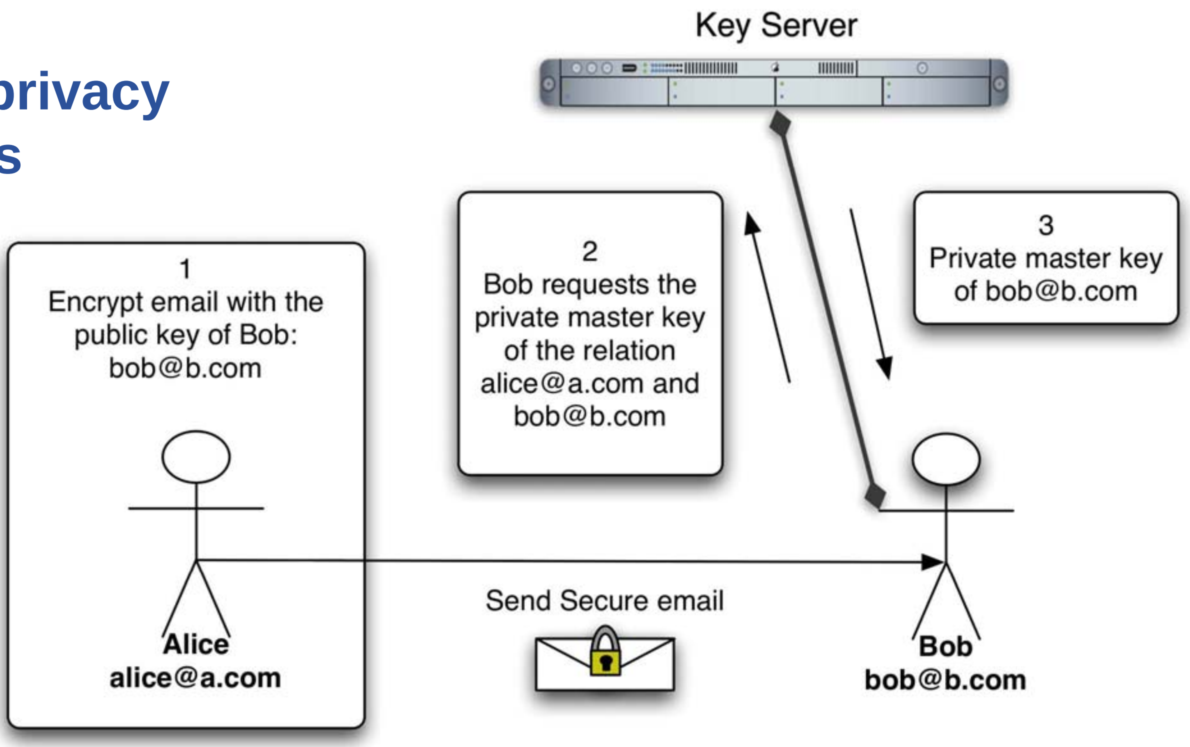
TVS – Token Validation Service

KGS – Key Generation Service

Identity Based Cryptography (IBC)

Available implementations

- **Voltage Identity-Based Encryption (C based)**
  - Used in Microsoft Exchange Server
- **Eyebee by Univ Ireland (Java)**
  - Tested by us and will be implemented in IDC
- **Strong motivation for privacy concerned applications**
  - E.g. patient-doctor communication



Discussion and Future

- **It was fun working for EGEE**
- **New security area with lot of unsolved problems**
  - Some of them are becoming visible
  - Not resolving them or ignoring will result in non-consistent design or excessive work to address emerging problems
- **Hope to meet you in other projects and at different meetings**
  - Will be interested in future offers for partnership in research and projects
- **Our research at SNEG/UvA will continue in the area of multidomain Complex Resource Provisioning (Grid enabled)**
  - AuthZ and Security
  - Research on the Grid security model(s)