

Authentication and Authorisation in the GGF

David Chadwick
University of Kent

Contents

- Past work of GGF WGs and RG
- Authentication
 - using Digital Signatures and Proxy Certificates
- Authorisation
 - Requirements and architecture
- Current work of GGF WGs
 - Incorporating external Authorisation services
- Future work in the GGF

Past GGF WGs and RGs

- Site Authentication, Authorization, and Accounting Requirements RG
 - A set of Authn and Authz (& A/c) requirements
- Grid Security Infrastructure WG
 - RFC 3820: Internet X.509 Public Key Infrastructure (PKI) Proxy Certificate Profile
 - GSSAPI Extensions as a GGF Experimental doc
- Authorisation Frameworks and Mechanisms WG
 - Conceptual Grid Authorization Framework and Classification
 - Authorization Glossary
- OGSA Security WG
 - The Security Architecture for Open Grid Services
 - OGSA Security Roadmap

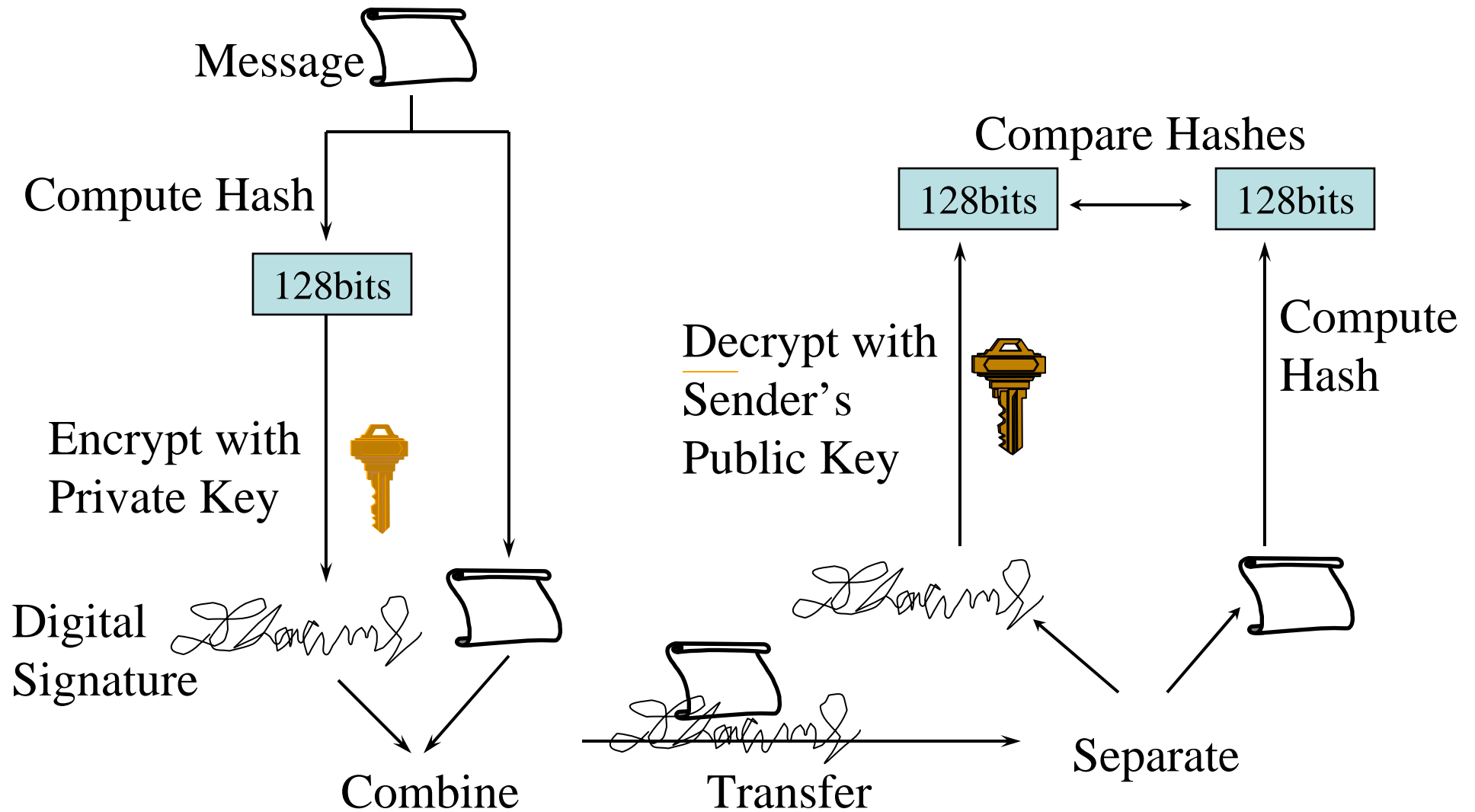
Grid Authentication Requirements (1)

- Defines 3 strengths of authentication
 - Strong - long-lived reusable secrets are not transmitted over the network
 - Encrypted - long-lived reusable secrets are transmitted on the network in encrypted form
 - Cleartext - reusable secrets?? are transmitted in the clear
- Authentication strength must be mechanically deducible from credentials. Method used to perform authentication should be deducible from credentials
- Recognises 3 ways of storing secrets
 - Mental - secrets (PIN or pw) are held in users' own memory
 - Stored - secrets are stored in electronic devices in a manner that relies on users' willing diligence in protecting them against disclosure
 - Secured - secrets are stored in electronic devices with credible protection against disclosure to unauthorized parties, even in the event of user carelessness

Grid Authentication Requirements (3)

- Every set of authentication credentials should be tied to the identity of an individual. May forfeit this in order to provide temporary and generic identities
- Authentication methods based on stored secrets should indicate the machine from which they were used
- User authentication credentials must not be valid for more than 1Ms if no method for revocation checking
- Authorities issuing revocable credentials must publish the procedures for initiating revocation. For X.509 certificates, each revocable certificate should include a pointer to such procedures which must include the location and publication frequency of revocation information and an upper bound on the time required to act on a revocation request

Digital Signatures



TRUST in the Signature

- However.....
- We can only trust that the message came from the sender, if.....
- Only the sender can access the private key
 - If someone else can use my private key then they can masquerade as me
- The receiver has the correct public key for the sender
 - How do you know that it is actually my public key that you have

Storage of User Private Keys

- In an encrypted file, protected by a password
- In a smart card, protected by a password or PIN

PCMCIA
reader

Smartcard



Serial Port
reader

Public Key Distribution

- How do we know that this public key REALLY belongs to that remote user?
- Potential for masquerade (key substitution)
- Have to secure them prior to network distribution
 - Digitally sign the key and owner's identity into a public key certificate
- Three ways to distribute public keys (certificates)
 - Personally exchange public keys (as in PGP)
 - Get a public key from someone you trust (e.g. a PGP trusted introducer)
 - Get a certified key (certificate) from a public repository (as in PGP and X.509)
- The key certifier is called a Certification Authority (CA)

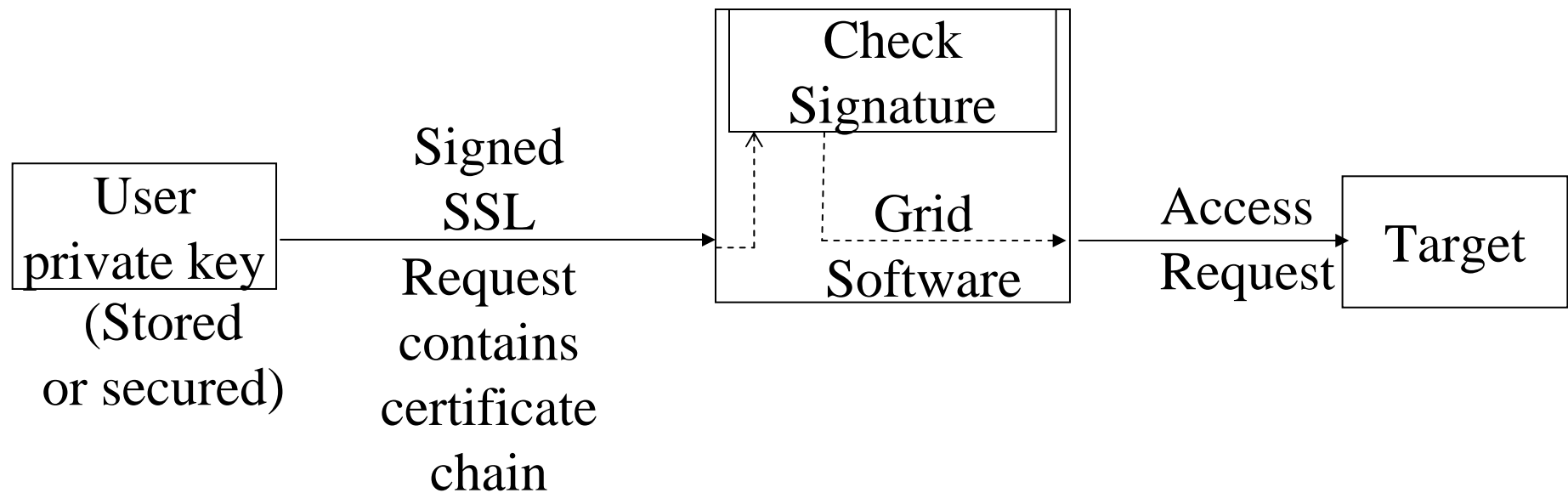
Storage of CA Root Private Keys

- These are the root of trust so
 - must be strongly protected
 - if compromised the whole PKI is lost
- For ultimate security, store in FIPS 140-1 level 3 or 4 hardware to be really safe



tamperproof, climate proof
key is destroyed if box attacked e.g.
Safekeyper from GTE
Luna CA³ from Chrysalis-ITS

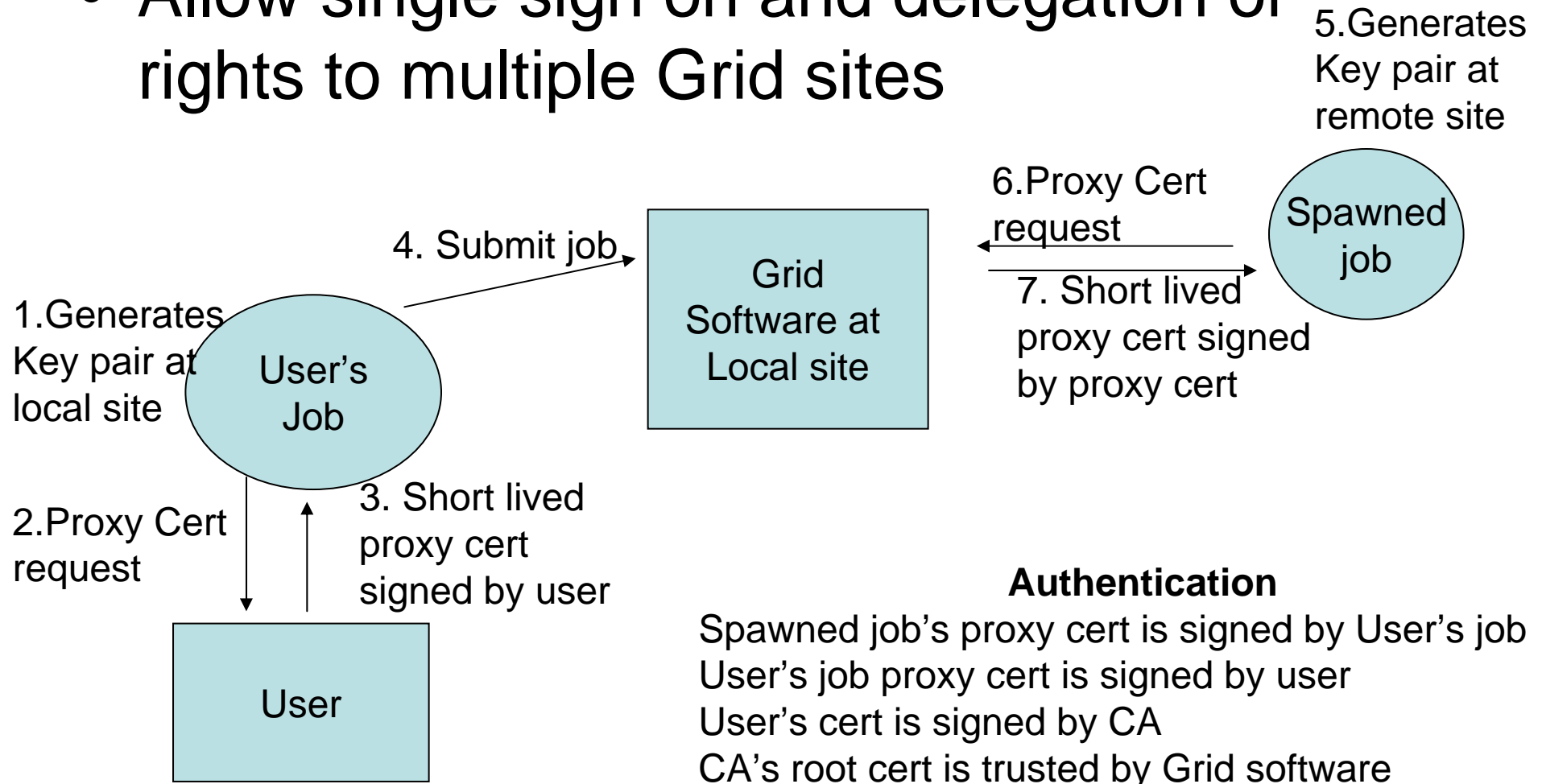
Digital Signatures in the Grid



*But what if the Grid job wants to run at multiple sites?
Or what if the user wants to initiate Grid jobs from
multiple locations?*

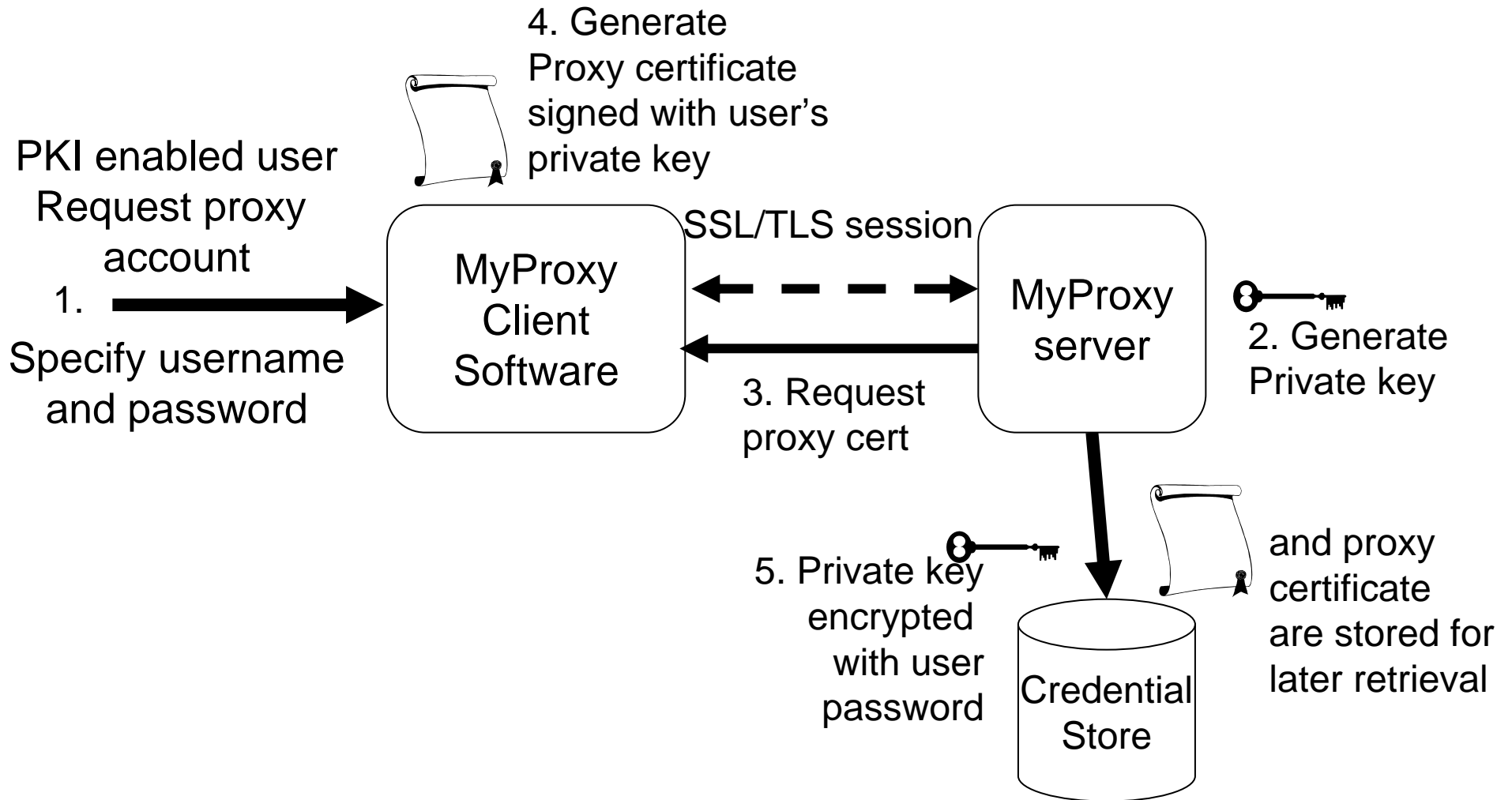
Proxy Certificates (RFC 3820)

- Allow single sign on and delegation of rights to multiple Grid sites

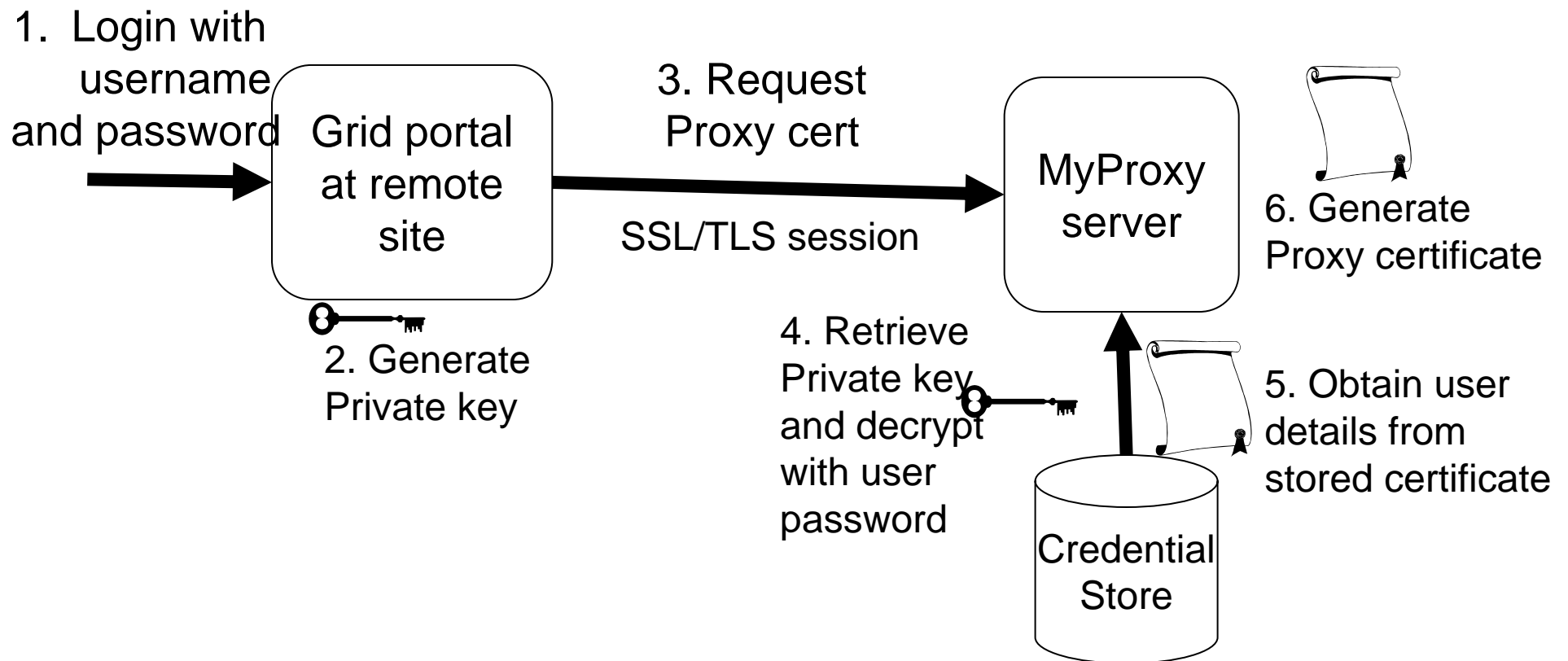


MyProxy (storage)

- Allows a user to run a grid job from anywhere



MyProxy (retrieval)



Grid Authn and Authz Requirement

- Current proxy certificate specifications ensure that proxy and delegation operations never require private keys to be sent across the network. It is important to state clearly to developers that all future protocols must continue this practice. If it is necessary to send a passphrase or password across the network, they need to be encrypted at a strength equivalent to the strength of the key

OGSA Security Roadmap

Authentication Requirements

- OGSA implementations must be authentication mechanism agnostic and work with Kerberos and different PKI variants e.g. X.509, PGP, AADS and SPKI

Authorisation

Grid Authorisation Requirements (1)

- The authorization process must be consistent within a VO. Users and VO managers must be able to rely on consistent interpretation of their policies
- The authorization method must be application independent
- The authorization mechanism must preserve the Subject Identity of the user who originated the request
- The level of authentication must be included with the credential information presented to all resource managers... access to a resource.. may depend on the strength of the authentication
- There must be the ability to quickly revoke a particular remote authorized service that may be operated under dubious procedures

Grid Authorisation Requirements (2)

- Assertions of membership in roles and groups within a VO must be able to be validated by relying parties. Validation of such assertions should not succeed more than 1Ms after an authority removes the subject's membership
- VO attributes describing the roles and groups must follow a published standard, agreed upon at least within the domain of the VO
- A user must be able to select and de-select VOs and roles for a specific access
- A user should be able to individually define the set of privileges to be used with a specific service request

Grid Authorisation Requirements (3)

- The owner of a resource or data must be able to allow or deny the authorization of an end entity to carry out an action using any of the following criteria
 - None
 - having some acceptable authentication without specifying identity
 - membership in a VO
 - role(s) within a VO
 - a combination of memberships of VOs and roles
 - individual identity certificates
 - the presence/absence of specific authorization attribute(s)
- The authorization method must allow any combination of the above authorization requirements
- Precedence rules for applying authorization decision criteria must be clearly stated.

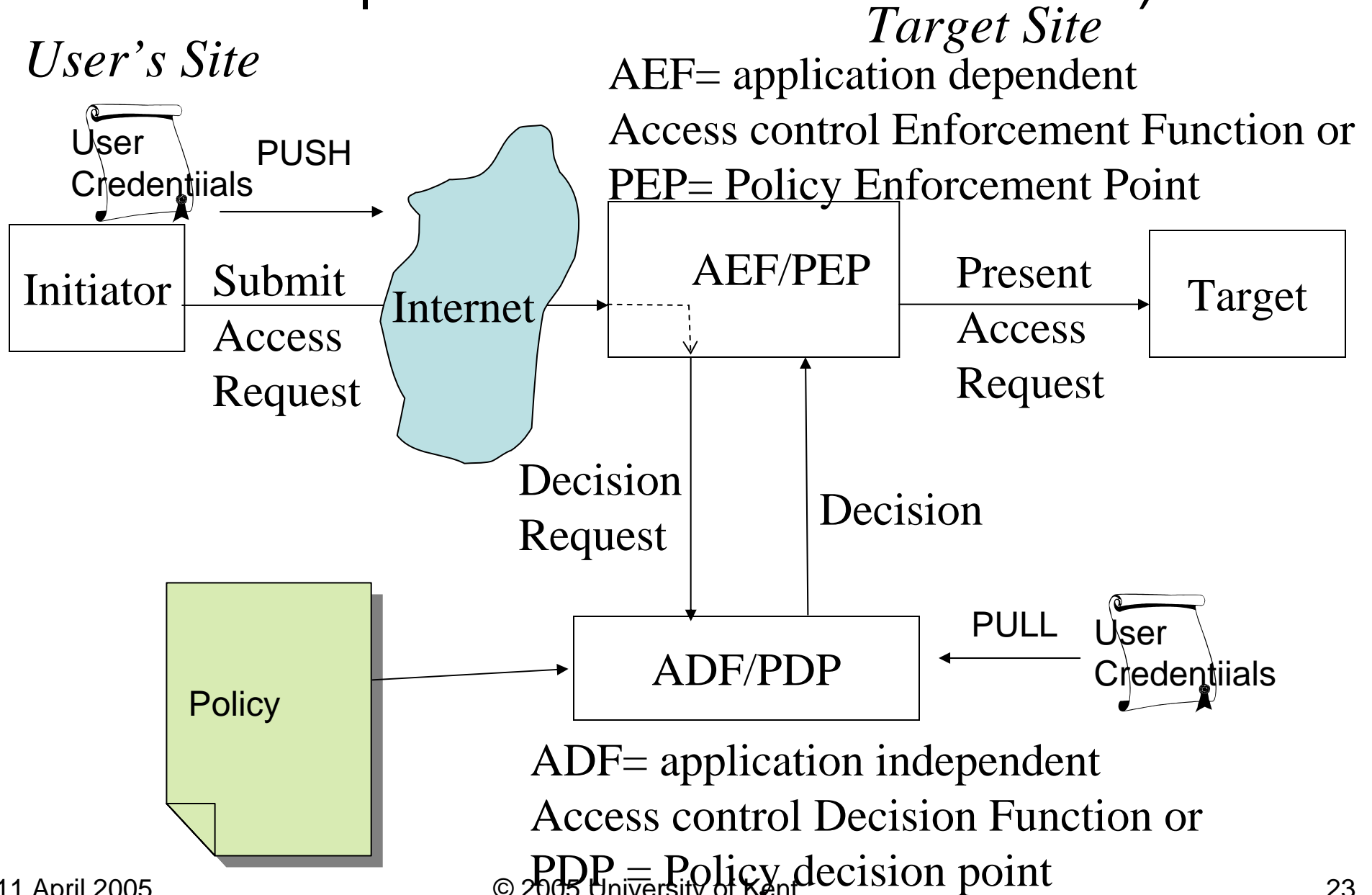
Grid Authorisation Requirements (4)

- The granularity requirement varies from fine grain (e.g. based on individual subject..) to coarser-grained authorization on the basis of groups or even sites.
- Support for role based access control mechanisms is specifically requested for future collaborative environments but may also be desirable for other grid systems
- It must be possible to determine the list of resources to which an end entity has access and what actions that entity is allowed to carry out in the VO(s) and role(s) set for the current session
- It must be possible to determine if a role or group has access to a resource...this information must be accessible... to the administrator..and security personnel for security audit and forensic purposes

Grid Authorisation Requirements (5)

- Control points must exist to allow for enforcement of authorization decisions and the inclusion of local policy decision functions
- It must not be possible for unauthorized users to produce a list of members of a VO, or the list of VOs to which a user belongs.
- It must be possible for the administrators to revoke all of a user's authorizations based on VO membership by removing the user from the VO
- It must be possible for an administrator to revoke a user's authorization by removing the user's ability to claim a given role or other attributes issued by an authority

Authorisation Framework (from X.812|ISO 10181-3 and RFC 2753)



Authorisation using Proxy Certs

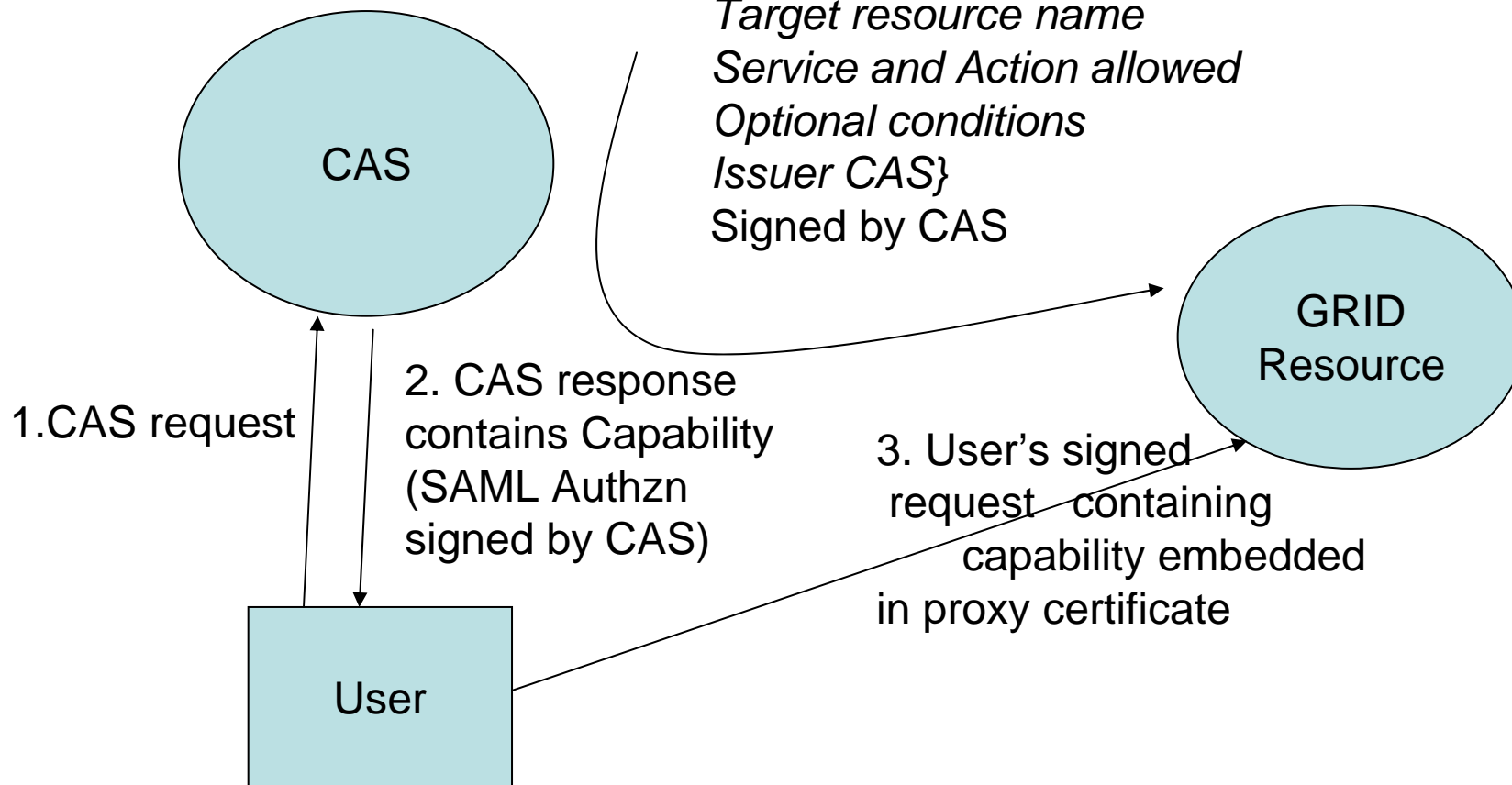
- Proxy certs are specified in RFC 3820
- Proxy certs have an extension to hold delegation of access rights
- This can be all or none, or a subset, but the way the subset is specified is not standardised. It is simply identified by an OID and an opaque field containing the policy rules defining the subset
- CAS makes use of this field to insert a community policy, as a capability

The Community Authorisation Server (CAS)

- Allows resource owners to grant access to blocks of resources to a community as a whole
 - CAS's DN is mapped into a local username in the Gridmap file
- The community itself manages fine-grained access control within the allocation
 - CAS's policy says who is allowed to do what on which resource
- CAS issues a signed SAML Authzn assertion to the user authorising it a subset of the CAS's privileges
- User inserts this in a proxy cert and submits job to Grid
 - Grid software validates job's signature using proxy cert, checks that user DN in cert is same as in SAML assertion, checks that SAML assertion allows user request, then maps the CAS name into a local username according to Gridmap file to ensure that local policy allows the job

The Community Authorisation Server (CAS)

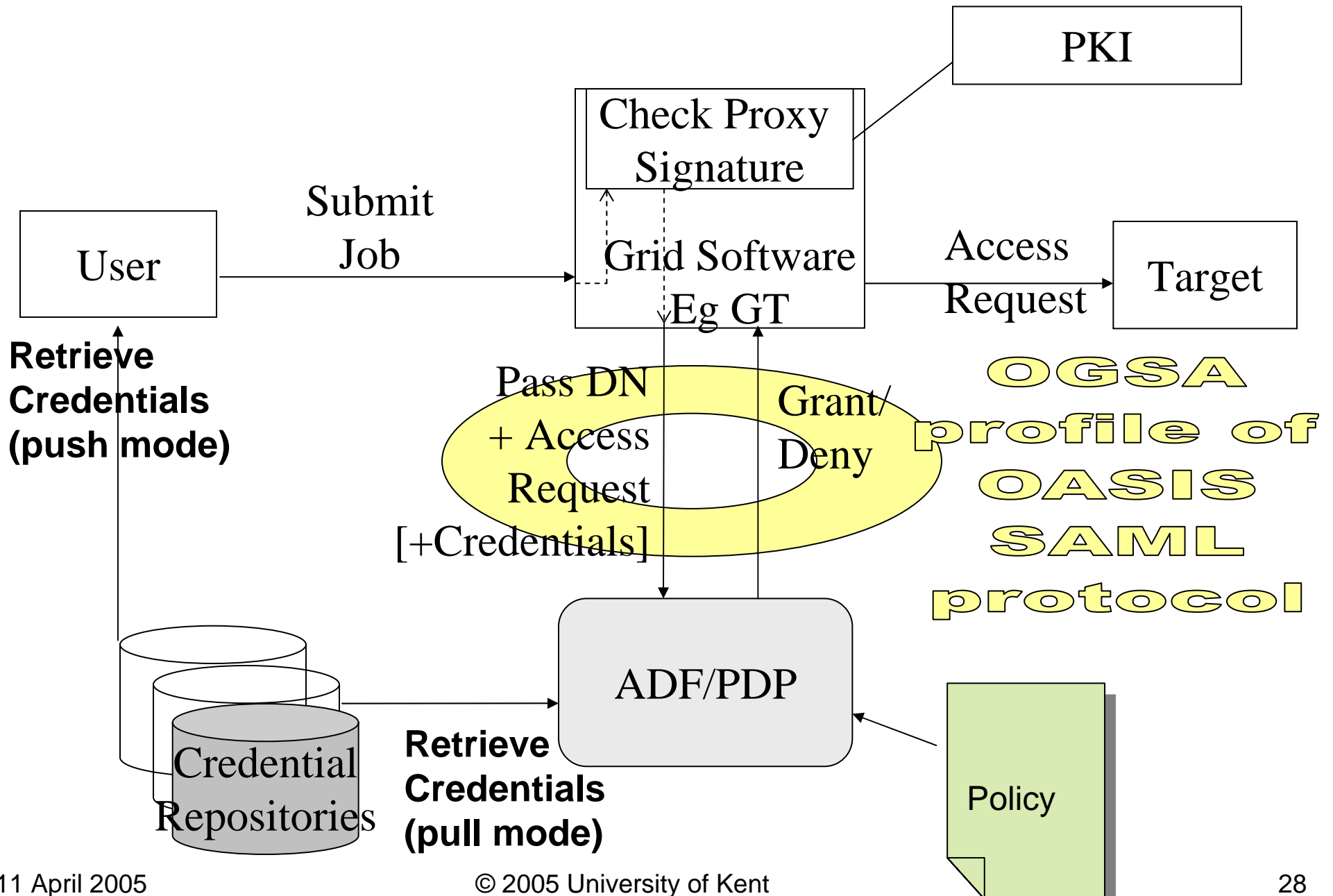
Capability (SAML Authzn assertion)
{*user's DN*
Target resource name
Service and Action allowed
Optional conditions
Issuer CAS}
Signed by CAS



Current GGF Working Groups

- OGSA Authorisation WG
 - leverage authorization work that is ongoing in the Web services world (e.g. SAML, XACML, the WS Security suite) and define specification for how these should be used for Grid services
 - **Attributes used in OGSA Authorization**
 - **Use of SAML for OGSA Authorization**
- CA Operations
 - develop operational procedures and guidelines that facilitate the use of X.509 and other technologies for cross grid Authentication
 - **Global Grid Forum Certificate Policy Model**
 - **CA-based Trust Issues for Grid Authentication and Identity Delegation**

OGSA SAML Specification



OGSA Security Roadmap

Authorization Requirements

- Any interaction between two parties requires that authorization decisions be made on both ends
 - Requester verifies that its policy allows it to invoke the request on the service provider, while the server checks whether its policy allows the request to be serviced.
- Names must be unique across different realms

Where To Next?

- Piloting the OGSA SAML specification has identified additional features that are needed in a V2 spec
 - Ability to pass Action Parameters so that decision can be made on them e.g. Write file if size LT 3 GB
 - Ability to pass back Obligations e.g. Grant access if UID set to Gz12
- OGSA Security Roadmap has identified a number of new standards that are needed e.g.
 - Naming users, services, groups, attributes, and actions (methods)
 - Mapping services for: names, policies, credentials
 - GSS API specification for WS Secure Conversation
 - Policy Management specifications
- New GGF Groups are on the horizon
 - Firewall Issues
 - WS Delegation
 - Trusted Computing
 - Grid VPN Research Group