GSI Online Credential Retrieval Requirements

Jim Basney
jbasney@ncsa.uiuc.edu
http://www.ncsa.uiuc.edu/~jbasney/
Online Credential Retrieval Defined

Client

Authenticate

Request Credential

Server

Verify Authorization

Retrieve Credential
Motivation for OCR

• **Credential management**
  – Securely manage credential files on user’s behalf
  – Ease use of multiple credentials

• **Credential translation**
  – Single sign-on to multiple authentication mechanisms and domains

• **Credential renewal by trusted services**
  – Alternative to delegating long-lived proxies

• **Indirect credential delegation**
  – Example: web portals
# OCR Examples

<table>
<thead>
<tr>
<th>Service</th>
<th>Auth Method</th>
<th>Credential</th>
</tr>
</thead>
<tbody>
<tr>
<td>MyProxy</td>
<td>Password</td>
<td>X509 user proxy</td>
</tr>
<tr>
<td>K5Cert</td>
<td>Kerberos</td>
<td>K5 CA issued X509 cert</td>
</tr>
<tr>
<td>CAS</td>
<td>GSI</td>
<td>X509 community proxy</td>
</tr>
<tr>
<td>GSIklog</td>
<td>GSI</td>
<td>AFS token</td>
</tr>
<tr>
<td>SSLK5</td>
<td>SSL</td>
<td>Kerberos ticket</td>
</tr>
<tr>
<td>Kerberos KDC</td>
<td>AS_REQ+preauth</td>
<td>Kerberos ticket</td>
</tr>
<tr>
<td>CA</td>
<td>OOB or IAK</td>
<td>CA issued X509 certificate</td>
</tr>
</tbody>
</table>
OCR Implementations

• **Online Credential Authority**
  – Examples: Online CA, Kerberos KDC
  – Creates credentials on demand
  – Vulnerability of authority’s private key a concern

• **Encrypted credential repository**
  – Credentials stored encrypted in the repository
  – Credentials may be opaque to protocol and repository
  – Requires client to decrypt credentials on receipt

• **Delegating credential repository**
  – Unencrypted credential stored in repository
  – Server delegates credential to client
Proposed GGF Activity

• **OCR Requirements document**
  – What OCR services are needed for Grids?

• **OCR Framework document**
  – Address policy issues of credential repositories, credential translation, credential renewal
  – Recommendations for interoperability

• **OCR Protocol document**
  – Define an OCR protocol framework that enables interoperability between different types of OCR services
  – Share mechanisms between OCR implementations (auditing, delegation tracing, event notification, etc.)
Standards Activity

• IETF SACRED WG
  – Credential format MUST be opaque to the protocol
  – Protocol MUST NOT force credentials to be present in clear text on the server

• IETF PKIX WG
  – Online Certificate Authorities
    – Certificate request may include Initial Authentication Key
Protocol Requirements

• **Mutual authentication**
  – Client-side configuration required to authenticate server

• **Multiple authentication mechanisms**
  – Password, GSI, Kerberos

• **Delegate different credential types**
  – X509 cert, X509 proxy, Kerberos ticket

• **Client can choose among available credentials**
  – Query available credentials and choose
  – Request credential that meets specification

• **Administrative protocols**
  – Credential upload and remove
  – Authorization control (user, administrator, and community)

• **OGSA-compliant**
OCR Issues

- Authorization
- Restricted delegation
- Delegation tracing across multiple mechanisms
- Audit trail
- Notification services
- Compatibility with site security policies
- Availability/Replication
Discussion

- Is there a need for OCR services in the Grid?
  - If so, what types of OCR services are needed?

- Will production Grid policies allow OCR services?
  - Centralized key storage
  - Transitive trust

- Is there interest in GGF OCR activity?

- Any comments on requirements draft?

- Other comments or discussion topics?