Overview of existing and developing systems for Authentication and
Authorisation and Policy/Role based Privilege Management

Yuri Demchenko
April–May 2003

1. Reference documents related to PKI and PMI
2. Overview of existing and currently developing PKI based systems
   for Authorisation and Authentication

1. Reference documents related to PKI and PMI

There is a number of RFCs and current Internet drafts describing
different components of X.509 PKI: PKC, CP, AC, PMI, etc., - and some
implementation issues, in particular LDAP Schemas for PKC and AC and
matching rules (what is the main component of the widely used LDAP/PKI
based authentication mechanism).

Documents targeting some specific issues in deploying PKI for different
application areas and services include some documents of interest (in
the framework of IETF and GGF):
- Internet X.509 Public Key Infrastructure Proxy Certificate Profile,
- CA-based Trust Model for Grid Authentication and Identity Delegation
- Multiple Credentials scenarios
- others.

List of document with comments will be provided with the next update
of this document.

Good implementation set of documents on Electronic Signature (which
superset of PKI and digital signature) is developed by ETSI

One document is of obvious interest "ETSI TR 102 044 Requirements for
role and attribute certificates" (http://webapp.etsi.org/action\PU/20021203/tr_102044v010101p.pdf). It
describes a set of requirements for attributes used both with PKC and AC
and provides a good set of practical recommendations and particularly
Guidelines for the certification of roles in subscription certificates.

PKI-Lite set of document developed and implemented by Internet2 among US
Universities - http://www.cren.net/crenca/pkilite/, particularly two
major documents:
"X.509 Certification Authority Policy & Practices" -
http://www.cren.net/crenca/pkilitepages/pkilitecpcps.html
Relying Party Statement -
http://www.cren.net/crenca/pkilitepages/relyingparty.html

2. Overview of existing and currently developing PKI based systems
for Authorisation and Authentication

Proposed improved secure communication system for RIPE NCC users
actually require extensive range of functionality that needs to cover
both Authentication, Authorisation issues and Auditing and Accounting
issues.

There is no available general purpose system with such range of
functionality, however some components and solutions can be reused for
existing solutions.

2.1. PERMIS (PrivilEge and Role Management Infrastructure Standards
validation)
PERMIS is a project at Information Systems Security Research Group (ISSRG) in University of Salford, UK
http://sec.isi.salford.ac.uk/permis/

PERMIS is built on a basic concept of separating AuthN and AuthZ and provides policy based authorisation service (i.e., PMI) that uses X.509 AC to hold roles/attributes.

* It can work with any and every AuthN system (e.g., username/pswd, PKI, Kerberos, etc.) that provides AuthN decision and requests PERMIS for the decision.

* Given a username, a target and an action, it says whether the user is granted or denied access based on the policy for the target; PERMIS needs access to the policy repository, attributes/roles or AC can may be received in the request or retrieved from the AC storage.

* The policy is a role/attribute based, i.e. users are given roles/attributes. Roles/attributes are given permissions to access targets.

* The policy is written in XML similar to XACML.

* PERMIS can work in push or pull mode (i.e. attributes are send to PERMIS, e.g. by AuthN service or target's Source of Authority, or PERMIS can fetch them from AC storage).

Additional information:

* PERMIS is created by the Information Systems Security Research Group (ISSRG) in University of Salford chaired by David Chadwick
<d.w.chadwick@salford.ac.uk>

* PERMIS - is included into the Internet2 NMI-EDIT software release.

Note. Currently the further development of the PERMIS for role-based portal access solutions is considered with partial funding by European NRENs for total amount of 50-60 KEuro. RIPE NCC can participate with its share and define the policy and technical requirements for the project extension.

Conclusion:

PERMIS can work with planned RIPE NCC improved security system with either using extended PKC for attributes/roles assignment or using AC for AuthZ purposes.

2.2. SPOCP (Simple POlicy Control Protocol)

SPOCP is a cooperative project whose task is to create software for authentication and authorisation services. The project started informally May 10, 2002, and is planned to end on May 31, 2003.


User authentication is provided by authentication service through both user name/passwords and x509-certificates. The authentication service is normally deployed as a local authentication service.

SPOCP offers policy controlled authorisation advice to its clients, using information provided by

* the user/client: authentication strength and an assumed role; and
* directories or other information services (user and resource attributes such as roles and identity).
SPOCP uses LISP S-expression
(http://www.umu.se/it/projupp/spocp/software/s-expr.html) to compare level of permissions requested by user/service and described by resource access rules. Allowed access/AuthZ level is derived from ordered set of rules described by policy for which request belongs to particular rule: Request<=Rule(m)

Example: (role UmU admin finance) <= (role UmU admin)

Example SPOCP query from SMTP server:
(spocp (resource mailrelay)(action mail)(subject (smtpauth roland)))

SPOCP provides simplified data/request exchange procedure (optimised for policy based AuthZ) comparing to general purpose XACML and SAML in the context of standard PMI (http://xml.coverpages.org/xacml.html). SPOCP involves only communication between Application, Resource and SPOCP server/engine. SPOCP has also simplified message format and policy description format in a form of S-expressions.

SPOCP provides more flexible way of policy/role based access control/AuthZ comparing to simple attribute matching approach (see below), however requires more detailed policy description.

Conclusion:

SPOCP can be used for policy based AuthZ service using X.509 Certificates with permissions described in a form of S-expressions, and LDAP as a policy and user attributes storage.

2.3. PAPI (Point of Access to Providers of Information)

PAPI is a system for providing access control to restricted information resources across the Internet. PAPI relies on authentication provided by local to user authentication service, while leaving the information providers full control over the resources they offer.

The authentication mechanisms are designed to be as flexible as possible, allowing each organization to use its own authentication scheme and apply local privacy rules.

AuthN service issues user attributes/permissions (in form of cookies) which are presented to the Point of Access (PoA) or Global PoA managing access policy to the resource (or group of resources). (G)PoA can apply filters to user attributes to make an AuthZ decision and issues AuthZ token in form of cookie that grants specific level of access to particular resource or group of resources managed by PoA's.

Summary:

PAPI uses simple and straightforward solution in issuing user attributes token by AuthN server (but still not declared as any form of standard format like X.509 AC). AuthZ granularity and flexibility is achieved by AuthZ/attribute filters at (G)PoA. PAPI has an intention to implement AC and SAML for AuthN/AuthZ assertions.

2.4. A-Select

http://a-select.surfnet.nl/

A-Select offers a uniform user authentication service to web applications in an organisation. A-Select can also be used for cross-organisational authentication where users of federated organisations can be authenticated according to the existing policy. A-Select is completely web based and doesn't require any additional
software for users to install.

The A-Select systems consists of several components that communicate with each other to provide user authentication to requested application/service:

* A-Select Aware Applications:
Applications may communicate directly with the A-Select Server or use the A-Select Agent.

A-Select Agent:
The A-Select Agent is a software (a lightweight server or daemon) that runs on the application server and communicate with the application via API. A-Select Agent provides session management and generation of application tickets.

A-Select Server:
The A-Select Server authenticates users in a transparent manner. The A-Select Server has a database storing information about users and how they can be authenticated. Applications that need to authenticate a user will redirect him/her to the A-Select Server. When the user is authenticated, the A-Select Server will issue the user credentials and redirect him/her back to application. The A-Select Server does not authenticate users himself but rather redirects him/her to an A-Select Authentication Service Provider (ASP). The A-Select Server maintains a registry of all ASP servers and also knows which ASP can authenticate which users.

A-Select Authentication Service Provider:
The A-Select Authentication Service Provider (ASP) is a server that knows how to authenticate a user in some manner. Typically, an ASP offers a web front-end for traditional authentication systems like RADIUS, LDAP authentication etc. ASPs may be local or remote.

A-Select uses a tickets which hold user credentials. There are two types of tickets: "ticket granting ticket" issued after successful user AuthN by ASP and "application ticket" issued by A-Select aware application. Single-Sign-on functionality is provided by assigning longer lifetime for ticket granting tickets. The A-Select tickets are implemented as non-persistent cookies which are stored in the browser memory and are visible only for target server/service.

Applications may define different level of authentication. A-Select has well developed trust model that relies on the following trust relations between involved parties:

- users trust application servers
- users trust A-Select server
- users trust ASP server
- applications trust A-Select server
- A-Select server trusts ASP server
- ASP trusts A-Select server
- A-Select server trusts A-Select servers

Summary:
A-Select uses rather complicated authentication scheme because of separating ASP function. This approach may be beneficial for future migration to Identity management technology like Liberty.

2.5. Shibboleth and WebISO/Pubcookie

http://shibboleth.internet2.edu/
http://middleware.internet2.edu/webiso/
Shibboleth and WebISO/Pubcookie (Web Initial Sign-On) are technologies developed by Internet2 project for US Universities respectfully for inter-institutional AuthZ and AuthN and SSO.

Shibboleth provides attribute-based AuthZ model. A particular feature of Shibboleth is its concern with the privacy of the individual, its protocol requires attributes to be maintained and stored by the institutions, and released selectively to resource providers with only those attributes which are required for the authorisation decision requested by resource provider. Shibboleth protocol/architecture intents to keep user anonymity when accessing the resource. The individual user is given power to control which attributes may or may not be released to specified remote services.

Shibboleth is attracting definite interest from commercial providers, it's developed with contribution from IBM. It generically uses SAML for security assertions exchange.

WebISO system is designed to allow users, with standard browsers, to authenticate to web-based services across many webservers, using a standard (typically username/password) central AuthN system. WebISO components:
- Weblogin service
- Verification Service
- Web Application Agent
- Web Application
- Web browser

Pubcookie security model uses a shared symmetric key to encrypt certain messages sent between each application server and the login server, to prevent certain types "man-in-the-middle" attacks. New keys are generated by the Pubcookie "keyserver" application running on a site's login server. They are negotiated and distributed using the Pubcookie "keyclient" utility during the setup phase of each application server. Keys are then maintained by the Pubcookie "keyserver" application running on a site's login server. Key can be revoked at the login server, but automatic expiration and renewal processes are not yet provided.


This section will provide basic reference information about XML based technologies for providing security assertions and secure AA/Identity tokens exchange for AA(A) and PMI solutions.

Particular topics will include: XML Signature, XML Encryption, SAML, XACML, Liberty Identity management, and others related to Web Services security.