
Authorization Policy in a PKI Environment

Mary Thompson
Srilekha Mudumbai
Abdelilah Essiari
Willie Chin

Lawrence Berkeley National Laboratory

Distributed Environments

- **Widely distributed computing environments, collaborative research environments**
- **Resources, stakeholders and users are all distributed**
- **Spanning organizational as well as geographical boundaries, e.g., DOE Collaboratories, Grids, Portals**
- **Requires a flexible and secure way for stakeholders to remotely specify access control for their resources**
- **Requires a flexible but secure way to identify users and their attributes**

Public Key Infrastructure

- Provides a uniform way for different organizations to identify people or other entities through X.509 identity certificates containing public keys.
- These certificates and keys can be used through secured connections (SSL) to positively establish the identity of the entities on the connection.
- The keys can be used to provide digital signatures on documents. The authors and contents of signed documents can be verified at the time of use.
- Mature Certificate Authority software packages are available and widely deployed. Entrust, Verisign, iPlanet RSA Keon and OpenSSL.

Goals for an Authorization system

- **Use Public Key Infrastructure standards to identify users and create digitally signed certificates**
- **Use existing SSL protocol to authenticate users**
- **Access based on policy statements made by stakeholders**
- **Handle multiple independent stakeholders for a single resource**
- **Emphasize usability**

Authorization Models

- **Access Control**

- User is authenticated by some means
- The resource gatekeeper checks the user against a policy to determine access
- Application needs to pass only an identity token to resource

- **Capability**

- User goes to a policy manager and gets an unforgeable token (capability) that grants the holder rights to some resource
- The resource gatekeeper verifies the capability and allows the actions specified in the capability
- Application must get the capability token (short-lived)
- Application must pass identity token and capability token to the resource
- Facilitates delegation of rights

Akenti Authorization

- **Minimal local Policy certificates (self-signed)**
 - Who to trust, where to look for certificates.
- **Based on the following digitally signed certificates:**
 - X.509 certificates for user identity and authentication
 - UseCondition certificates containing stakeholder policy
 - Attribute certificates in which a trusted party attests that a user possesses some attribute, e.g. training, group membership
- **Can be called from any application that has an authenticated user's identity certificate and a unique resource name, to return that user's privileges with respect to the resource.**

Emphasis on usability

- **Usability is critical:**
 - **Policy and attributes must be easy for stakeholders to generate and read**
 - **Minimal change to applications seeking use of resources**
 - **Simple API for resource gateway to check access**
- **Akenti certificate generators provide a user friendly interface for stakeholders to specify the use constraints for their resources.**
- **User or stakeholder can see a static view of the policy that controls the use of a resource.**
- **Akenti Monitor applet provides a Web interface for a user to check his access to a resource to see why it succeeded or failed.**

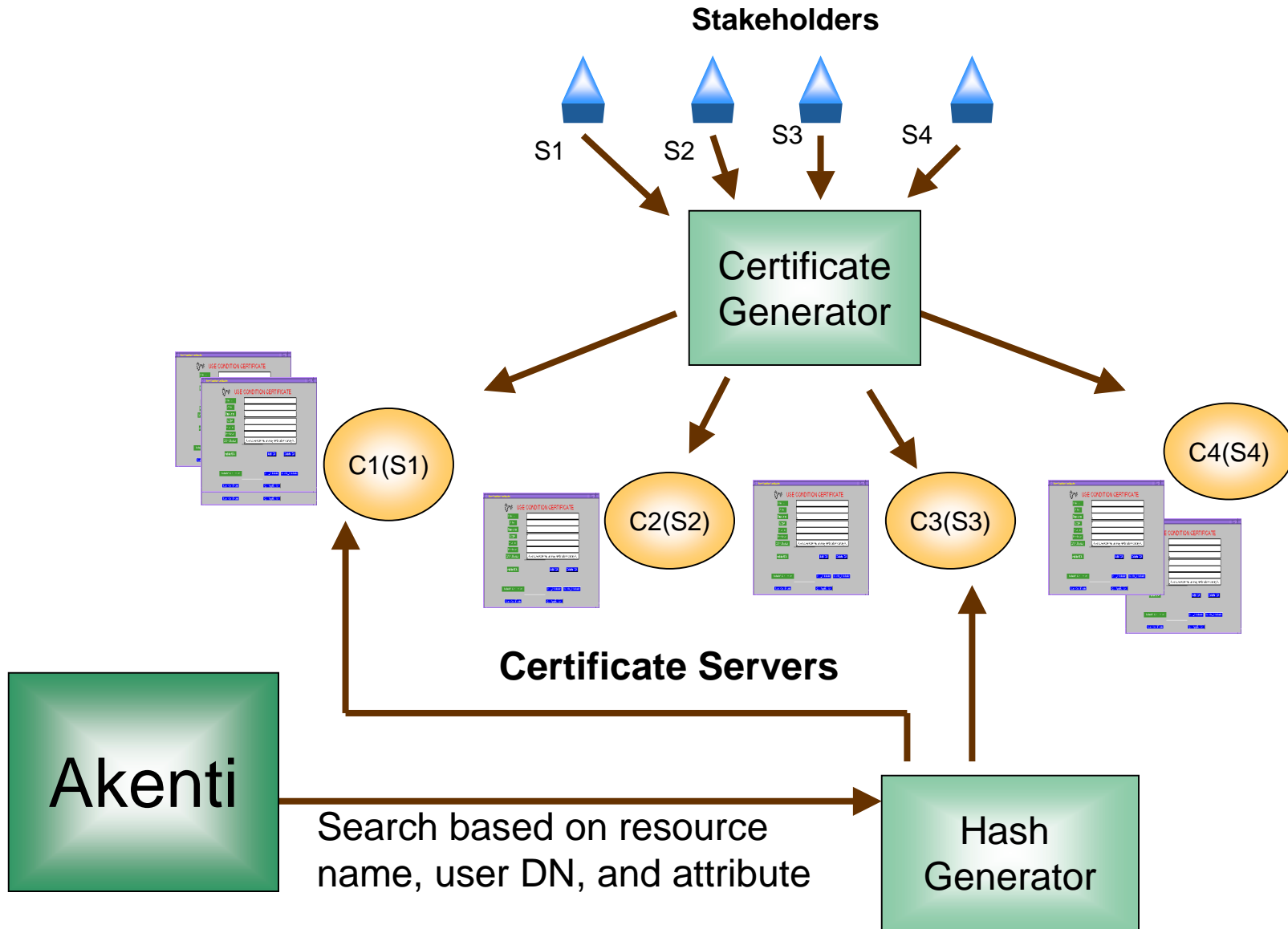
Certificate Management

- **Users need to generate signed certificates and store them in Web accessible places or be able to upload them securely to the resource gateway.**
- **Akenti needs to know where to search for certificates**
- **Once a certificate is found, Akenti will cache it for a a time not to exceed that specified by the stakeholder.**
- **When an access decision is made, a capability certificate containing the rights is cached and returned to the requester.**

Akenti Server Architecture



Akenti Certificate Management



Required Infrastructure

- **Certificate Authority to issue identity certificates (required)**
 - OpenSSL provides simple CA for testing
 - iPlanet CA - moderate cost and effort
 - Enterprise solutions - Entrust, Verisign, ...
- **Method to check for revocation of identity certificates (required)**
 - LDAP server - free from Univ. of Mich.. Or comes with iPlanet CA
 - Certificate Revocation lists - supported by most CA's
 - OCSP - not yet widely implemented
- **Network accessible ways for stakeholders to store their certificates (optional)**
 - Web servers
 - LDAP servers

Using Akenti for Authorization

- **C++ library that resource gatekeeper can link with**
- **Insecure server using TCP and returning rights as strings**
 - Use with thin client interface on the same machine
- **Secure server using SSL and returning signed capability certificates containing the rights**
- **As an authorization module with the SSL-enabled Apache Web server**

Mod-Akenti

- **The SSL-enabled Apache Web server can be configured to require Client-side X.509 certificates.**
- **Replaces mod-authorization**
- **Calls out to Akenti with the user's identity**
- **Uses Akenti policy certificates to make the access decision – allows policy to be set remotely**
- **Allows the same access policy to be used for Web accessed resources as other resources**

Vulnerabilities

- **Primarily denial of service.**
- **Distributed certificates might not be available when needed.**
- **Independent stakeholders may create a policy that is inconsistent with what they intend. Easy to deny all access.**

Attribute Certificates

- **IETF PKIX Attribute Certificates**

- ASN.1 certificate – holder, attributes, issuer
- Attribute – type-value pair
 - Some standard types: group, access identity, role, clearance, audit identity, charging identity
- X.509 identities identified by CA and serial number
- Optional targeting information

- **SAML (Security Assertion Markup Language)
OASIS**

- XML signed certificate asserting that a principal has certain attributes
- One of a set of XML certificates containing assertions, authentication, authorization decision
- <Audience Restriction Condition>

KeyNote Trust Management

- **Common language for policies and credentials (ASCII Keyword-value)**
- **Uses opaque strings or cryptographic identities – separates secure naming from authorization.**
- **Policy assertions are defined for a resource. Can be signed and thus set remotely**
- **Requestor provides an identity and credential(s)**
- **Compliance checker checks the access**
- **M Blaze, J. Feigenbaum, J. Ioannidis, A. Keromytis**

Shibboleth

- **Internet2 Project**
- **Users have a credential that is a handle back to their home institutions**
- **Resource providers ask the home institution for the user's attributes. E.g. student, faculty**
- **Need inter-domain trust and common vocabulary**
- **Users can get access to resources while remaining anonymous to the resource provider.**

CAS Community Authorization Server

- **Globus Project**
- **Resources grant bulk access rights to communities of users**
- **A CAS controls fine-grained access for community members**
- **CAS issues a short-lived delegated credential containing the users rights (X.509 certificate)**
- **Users connect to the resource with the CAS delegated credential via GSI/SSL.**
- **More scalable than current Globus grid-map-file**

Experience

- **Akenti enabled Apache Web Server has been used at LBNL and Sandia for the Diesel Combustion Collaboratory.**
 - **Controlling Akenti code distribution, secure data/image repository, ORNL electronic notebooks, PRE accessed remote job executions**
- **Used with CORBA applications**
- **Used by the National Fusion Collaboratory**
 - **Access to remote code execution started by the Globus job-manager**
- **Easy to for applications to use if connections are made over SSL**
- **Runs on Solaris and RedHat Linux**

Trust Models

- **Resource domain establishes one on one trust with all its users**
 - Difficult for users, doesn't scale
- **Different domains establish mutual trust to allow users of one domain to access resources in another**
 - Cross-realm Kerberos trust
 - Shibboleth
- **Delegated trust – Resource trusts a few entities but allows them to delegate their rights to others**
 - CAS model
- **Resource domain would like to limit degree of trust**
 - Limit actions
 - Audit actions
 - Revoke trust in a timely fashion

Future Directions

- **Further development of Use Conditions that use dynamic variables such as time-of-day, originating IP address, state variables.**
- **Recognize restricted delegation credentials**
 - **Possibly use delegation credentials restricted by the delegator to a specified role**
- **Use the XML signature implementation to sign Akenti certificates – XMLSec Library, Aleksey Sanin**
- **Implement Akenti as a Web service acting as a trusted third party.**
 - **Use signed SOAP messages or SOAP over SSL?**
- **Consider using new SAML, WS-security standards**

Conclusions

- **Leverages off the increasing use of X.509 identity certificates.**
- **Akenti/SSL overhead acceptable for medium grained access checking. E.g , starting an operation, making a authenticated connection.**
- **Ease of use for stakeholders must be emphasized.**
- **Transparency for users and applications is important**