Controlling digital multisignature with attribute certificate

Paul Axayacatl FRAUSTO BERNAL

Ecole des Mines d’Alès – LGI2P

2002 ACSAC
Outline

- Context
- Technology
- Proposition
  - Attribute certificate
  - Format for the Multisignature
  - ICARE Ver. 0.1 Tool
- Conclusion
Context
Motivation

Security on electronic transaction
Cryptography
Public Key Infrastructure (PKI)

digital Signature
Services about digital signature

Digital Certificate

PKI : Public Key Infrastructure
Asymmetric encryption = public key cryptography
Why new e-services?

- Digital signature is not valid
  - Who is enable to sign?
  - In which order must they sign?
E-services

The **attribute certificate** is an ideal way to add functionality to a conventional digital signature.

1) Habilitation/delegation

2) Certification of role

3) Controlling digital multisignature
Controlling digital multisignature

Characteristics:

- Adds constraints to digital signature to:
  - Indicate the entities authorized to sign the document,
  - Tressle the order in which they must sign the document, ...
- Protects the Timestamp
- Includes information additionally to validate the signature.
- Archives the signature.

BIND an attribute certificate to a document.
Application e-services

Signing an order form

They have right to sign !!!

Digital Multisignature is valid !!!
Current Technology and Proposition
Digital certificates

- **Identity certificate (X.509 v3)**
  - Bind key - entity (DN)
  - Authentication

- **Attribute certificate**
  - Bind permission - entity
  - Permission

X.509 v3: Digital certificate standard proposed for ITU-T, ISO
DN: Distinguished Name of X.500 standard

are complementary
Approaches of attribute certificates

- **SPKI**
  - Bind permission – key or name
  - Encoder in S-expressions
  - Allow anonymity and delegation
  - Decentralize Infrastructure Management
  - Supporter ACLs and names SDSI

- **X.509 version 2000**
  - Bind permission – entity
  - Allow access control
  - Centralize Infrastructure Management
  - Encoder in ASN.1
  - Supporter CRL and name X.500

---

SPKI: Simple public Key Infrastructure
X.509 v 2000: Digital certificate standard proposed for ITU-T, ISO
ASN. 1: Abstract Syntax Notation One
SDSI: Simple Distributed Security Infrastructure
New attribute certificate

- **Bind permissions to:**
  - Certificate (or reference)
  - Public key (or hash)
  - Role
  - Name valid for X.509 v. 2002
    - BaseCertificateId
    - EntityName
    - ObjectDigestInfo

- **Extensible infrastructure**

- **Attributes structure:**
  - AttributeName
  - AttributeValue
  - AttributeDescription

- **Encoder in XML**
New attributes

- **SignatureDelegation to:**
  - Empower the signature

- **SignaturePath to:**
  - Indicate the signatories
  - Indicate the sequence of signatures
  - Allow habilitation certificates
Format XMLDSIG

XMLDSIG (W3C - IETF)
- To ensure the integrity of the message and to confirm the identity of the sender.

Characteristics
- Several persons can sign different portions of the same message.
- Usages of different cryptographic algorithms
- Multipart encoding
- The signature is encoded in XML.
- Partial information to check the signature:
  - Inexistent timestamp protection
  - Does not consider: order of signatures, dates and policies associated to each signatories
New format to multisignature control

➢ To bind XMLDSIG recommendation + attribute certificate to:
  • Indicate the constraints (Who, When, How).
  • Give indications (signature polices).
➢ To ensure the Timestamp.
➢ To have the references to:
  • Signed Objects.
  • Certificates and CRL necessary to check the signature.
ICARE ver. 0.1 Tool
Infrastructure

Publication of attribute certificates and ACRLs

Management: Attribute Certificate

User

Verifier

PKI

RA

CA

CA Root

Management PKI

Stock of identity certificates and CRLs

Publication de certificate and CRLs

Generator

Stock of attribute certificates and ACRLs

Publication of Roles and certification policies
Application Generator

- Generate attributes certificates.
- Manage roles.
- Manage signature policies.
- Definite signatures path.
Application user to:

- Sign objects (simple and multiple)
- Empower the signature
- Check signatures
- Interact with the PKI
Application verifier to:

- Make the verification of:
  - The integrity of the documents
  - The validity of the signatures
  - The sequence of signatories
  - The dates of validity
  - The validity of attributes certificates
  - The validity of identity certificates
Architecture of ICARE Tool

- API Generator
- API User
- API verifier
- API Crypto (Cryptix and JDK 1.4)
- API XML (JDOM)
- API de base
- Servers Management
Conclusion
Conclusion

➢ Usage of attributes certificates to:
  • Control the signature/multisignature.
  • Empower, delegate the signature.
  • Permit anonymity.

➢ Usage of language XML to:
  • Make/interpret easy the format of the signature.
  • Adapter to transactions electronic.

➢ Trust infrastructure is:
  • Adapter a new services.
  • Extensible and configurable.

➢ Possibility of extension:
  • Access control
That’s all, thank you!

Paul Axayacatl FRAUSTO BERNAL
Paul.Frausto@ema.fr