Interoperability Issues for multi PKI domain

Masaki SHIMAOKA <shimaoka@secom.ne.jp>

As representative of
NPO Japan Network Security Association
Sponsored by IT Promotion Agency, Japan
Objectives

- To achieve interoperability on multi PKI domain
- To separate the interoperability issues
  - for multi PKI domain interoperability
  - for single PKI domain interoperability
- To establish the reference implementation
Our Background

- Reference Documents
  - ‘CA-CA Interoperability’ by PKI Forum
    - trust model (CA topology)
  - ‘Review of PKI Interoperability Issues’ by pki Challenge
    - interface for inter-domain

- Results of some multi PKI domain experiments
  - IPA/J NSA: Challenge PKI 2001
  - PKI-J: International experiment
  - Japanese GPKI: Corroborative experiment
    - All experiments have common objectives and similar environment
    - achieving PKI interoperability and multi PKI domain
PKI domain

- Multi PKI domain
  - To define before discussion about multi PKI domain
  - “Integrated heterogeneous PKI.”

- Single PKI domain
  - So what is an individual PKI?
  - PKI Forum defines some trust-models in ‘CA-CA Interoperability’
    - Strict-Hierarchy, Cross-Certification, Cross-Recognition, Bridge CA, Accreditation Certificate, Certificate Trust Lists
  - Is that all?
  - Are these an appropriate definition?
Issues for multi PKI domain

- CA-CA issues
  - Trust model (internal PKI domain)
  - Certificate Policy & Policy Mappings
  - Constraints

- Client issues
  - Path validation
  - Local validation

- VA issues
  - What kind of role
Topics

- Path Validation
  - Most of specifications is fixed in RFC3280
  - But, too complex for current implementations

- How to Policy Mapping
  - Integrating heterogeneous PKI
  - What is mapped?

- Processing certification path
  - What does critical-flag indicate?

- Directory Interoperability
  - DN encoding, multi-RDN, etc.
  - Name rollover in the end of 2003
Path Validation

- Necessity for single PKI domain
  - MAY be enough only subset
- Necessity for multi PKI domain
  - SHOULD implement full set
- How do we evaluate the implementations?
  - To clarify ‘Conformance Testing Guideline’
  - Each needs for single/multi PKI domain
How to Policy Mappings

- What is certificatePolicy?
  - Policy depends on each PKI domain and trust-model.
    - assurance-level, security-level, amount of transaction, restriction-level, strength-level, etc.
  - Policy is different between each PKI domain.
  - When should we change it?

- Necessity about Policy Mappings guideline
  - To integrate heterogeneous PKI
  - Especially for Cross-Certification and Bridge CA
What is criticality?
- issuingDistributionPoints
  - No necessary to process this field though marked critical.
- policyMappings
  - Necessary to process this field though marked non-critical.

Necessity for self-signed certificate profile
- Do we need the profile for multi PKI domain?
  - RFC3280 mentioned that self-signed certificate is used for distributing its public key.
- Effect of extensions in self-signed certificate is dependent on trust-model.
  - e.g., Cross-Recognition, Certificate Trust Lists.
Processing certification Path#2

- How to use keyIdentifier
  - Using certIssuer & certSerial cannot track certificate chains to other domains.
  - All cross-certificates SHOULD follow certain method about keyIdentifier!

- More clarification
  - serialNumber, alternativeNames, etc.

- Dependency between some extensions
  - cRLDP and issuingDP
  - some constraints and cA flag
  - etc.
Directory Interoperability?

- DN encoding
  - Comparing method between UTF8String and other encoding-type
  - Necessity about name rollover certificate
- DirectoryString order
  - To begin from country or cn?
- How to interconnect another directory
  - referral on LDAPv3
  - chaining on X.500
  - etc.
What will we do?

- To define various ‘PKI domain’ in some views
  - CA topology, Validation model, etc.
- To collect and categorize many interoperability issues
  - for multi PKI domain and single PKI domain
  - based on above definition of ‘PKI domain’
- To implement reference code
  - to provide implementation guideline
  - to implement comfortably
    - for application developer
    - for certificate profile designer
Thank you and let’s discuss!

multi-domain-pki@jnsa.org