

Certificate Policies Processing: Current Status & Practical Technical Considerations

William E. Burr

8 September 1999

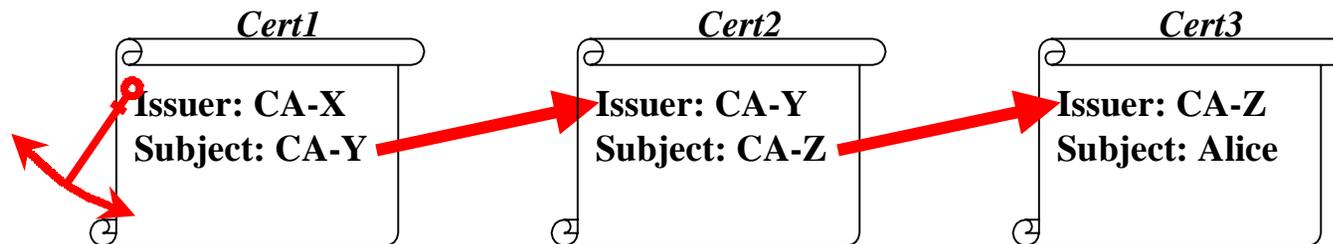
william.burr@nist.gov

301-975-2914



Certification path

- Starts with a “trust anchor”
 - public key of a trusted CA
- Chain of zero or more intermediate certificates (CA certificates)
- Leads to end-entity certificate



Path Processing

- Mechanical process:
 - a yes or no answer
 - additional information available to application
 - executed by relying party client
 - certificate policies, path length and name constraints
 - ignore path length and name constraints here

Path Processing

- Relying Party Inputs:
 - Initial Set of policies acceptable to RP
 - may have special value, *any-policy*
 - Initial require explicit policy indicator
 - Initial inhibit policy mapping indicator

Path Processing

(for certificate policies)

- Two Specifications:
 - X.509 1997
 - some problems with policy mapping
 - Draft Technical Corrigendum to fix most of them
 - RFC 2459
 - path processing is basically broken and needs to be fixed

Cert. Policy: “Technical Definition”

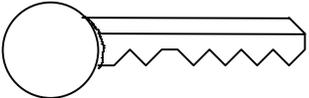
- ISO/ITU X.509 definition
 - “A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements”
- RFC 2459 definition
 - “...one or more policy information terms...these policy information terms indicate the policy under which the certificate has been issued and purposes for which the certificates may be used”

Certificate Policy Related Extensions

Certificate extensions that are used for policy processing:

- Certificate Policies
 - criticality
 - policy qualifiers
- Policy Mappings (CA certs.)
- Policy Constraints (CA certs.)
 - requireExplicitPolicy
 - inhibitPolicyMapping

Certificate Policies Extension in Certificates

Name		Policy OID: (2)(16)(840)...	Signature
------	---	-----------------------------	-----------

- **Policy Object Identifiers (a series of integers) asserted in certificates by Certification Authority (CA)**
- Related to Certificate Policy and Certification Practice Statement docs
- May be any number of policy OIDs in Certificate Policy field
- Roughly speaking - a “certificate policy” describes the “**level of assurance**” one can ascribe to a certificate asserting the policy, and the **community** and **applications** the certificates are intended to be used for.
- **Today, most applications ignore noncritical policies, & may not process policies at all.**

policyIdentifier

- Has different practical meaning in EE and CA certificates
 - **EE:** this certificate. was issued in accordance with the policies and procedures and is suitable for use in...
 - **CA:** a certification path with this policy supports EE certificate with this policy asserted

Policy Qualifier

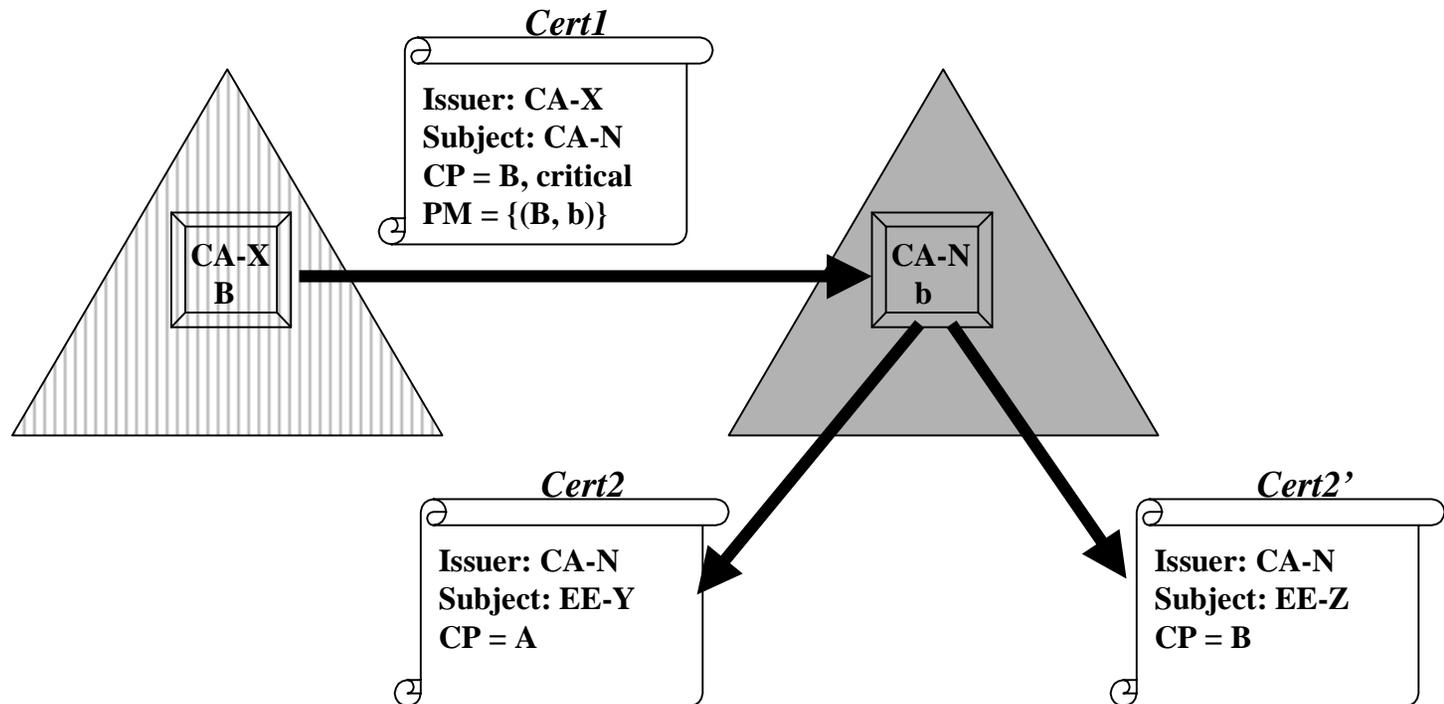
- Supposed to pass application specific policy information
- As construed by the IETF, there are two uses:
 - user notice
 - a URI to the CPS

Policy Mapping

- US Government wants to use
- Problems in current (1997) X.509 standard
 - Addressed in Draft Technical Corrigendum 7
- Effect of policy mapping
 - Currently: adds new policies to *authorities-constrained-policy-set*
 - Proposed DTC7: new policy to be substituted for old in *authorities-constrained-policy-set*

Example of problem

It appears to be difficult for a CA issuing a cross-certificate to a subject CA to restrict the policies that may be asserted by the subject CA.



If *initial-policy-set* is $\{A, B\}$, then the above chains will be valid. It is difficult for **CA-X** to restrict **CA-N** to only asserting policy **b** in **Cert2** and **Cert2'**

A 2nd Example of the Problem

User init. policy set = USHigh

Issuer:	USA CA
Subject:	Friendly CA
Cert Policy:	USHigh
Policy Map:	FrnHigh = USHigh
IPM skipcerts:	0
REP skipcerts:	0

Note that policy mapping is inhibited and explicit policy required

Issuer:	Friendly CA
Subject:	Lybia CA
Cert Policy:	FrnHigh
Policy Map:	LybHigh = FrnHigh
IPM skipcerts:	0
REP skipcerts:	0

The LybHigh = FrnHigh mapping has no effect on USA CA Relying Parties

Issuer:	Lybia CA
Subject:	Bad Guy
Cert Policy:	USHigh

But Lybia CA cheats and asserts USHigh Policy OID

Other Certificate Policy Changes

- 1997 X.509 specified somewhat different processing for certificate policies with the critical bit set, than for other extensions
 - Corrigendum ends special processing
- special value *any-policy* can now be included in intermediate certs.
 - Agreed at 8/23 mtg. that should be a way to turn off *any-policy*

Path Processing (per DTC7)

- Starts with a prospective certification path from trust anchor to EE certificate
- CA acceptable policy set
 - starts with *any-policy*
 - reduced at each step in path to intersection of policies stated in certificate and old CA acceptable policy set
 - certificates may contain *any-policy*

Proposed Change to DTC7

- Propose to add `inhibitAnyPolicy` extension
 - inhibit use of *any-policy* after skipcount certs in path - also may be set by RP client
 - if *any-policy* is inhibited, then it is ignored in certificates, but other policy OIDs processed
 - if *any-policy* is present in certificates and not inhibited, then other policy OIDs can be ignored

Policy Mapping (under DTC7)

- *Substitutes* new policy for old
 - old policy no longer valid in path
 - if mapping disabled (by `inhibitPolicyMapping` skipcount in certificates, or by RP client), mapped policies are deleted from CA acceptable policy set.

Explicit Policy

- CA may assert `requireExplicitPolicy`
 - skipcount
 - client may also initialize
 - if Explicit Policy becomes effective, the path processing terminates if the CA acceptable policy set becomes null
 - the only condition related to certificate policies that causes processing to automatically fail

Returned to RP Client

- Path Processing failure returns error indication
- If Path Processing completes it returns:
 - final CA acceptable policy set
 - a list of zero or more policies present (as mapped) in every certificate in the path
 - a list of accumulated policy qualifiers
 - use is application specific

Conclusion

- Certificate policies extension means something to a path processing machine
- CP & CPS documents used when a CA decides to cross-certify & issue certificates
- CP OIDs are processed by rules yielding a yes/no answer and (possibly) additional information
- May be confusion between legal & technical
- Policy path processing changed (DTC7) to be a refinement rather than an expansion process