ITU Liaison requests

Stefan Santesson
stefans@microsoft.com

Two liaison requests received

- Liaison to IETF on the removal of upper bound in X.509
  - https://datatracker.ietf.org/liaison/376/
- Liaison to IETF on the resolution of DR320
  - https://datatracker.ietf.org/liaison/375/

Liaison to IETF on the removal of upper bound in X.509

- "In response to developer demand in the early days of the standard X.520 contained a list of maximum lengths for a variety of string types, e.g., organizationalName. The values specified were non-normative."
- "We plan to remove the upper bounds specified in the standard"
- "The proposal does not change the definition of DirectoryString, but attribute definitions will look slightly different"

Liaison to IETF on the removal of upper bound in X.509

- Example
  - Before

```
streetAddress  ATTRIBUTE  ::=  {
  WITH SYNTAX               DirectoryString {ub-street-address}
  EQUALITY MATCHING RULE    caseIgnoreMatch
  SUBSTRINGS MATCHING RULE  caseIgnoreSubstringsMatch
  ID                        id-at-streetAddress }
```

  - After

```
streetAddress{INTEGER:maxSize} ATTRIBUTE ::= {
   WITH SYNTAX              DirectoryString {maxSize}
   EQUALITY MATCHING RULE   caseIgnoreMatch
   SUBSTRINGS MATCHING RULE caseIgnoreSubstringsMatch
   ID                       id-at-streetAddress }
```

Liaison to IETF on the removal of upper bound in X.509

- Discussion on the list
  - Removing ub harmonizes with LDAP
  - May cause interoperability issues
  - PKIX can still specify bounds and be compatible with X.509
- Required changes to rfc 3280bis?

Liaison to IETF on the resolution of DR320

- ITU rejected DR 320, calimin that DNs may not be unique.
- “The directory group believes that Distinguished Name values must be unique and unambiguously identify a single entity, hence the use of the term Distinguished.”
- “X.509 takes its definition of DN from X.501. Clause 9.2 of X.501 specifies the definition of DistinguishedName”

Liaison to IETF on the resolution of DR320

- We believe that if two entities claim the same name as top level CAs, there is a political/procedural breakdown much like the domain ownership arguments we have seen.
- Two claims were made at the 2007 Geneva meeting:
  - Certification Authorities are being deployed with names not acquired from naming authorities but with names arbitrarily chosen assuming that no other CA is or will be operating under that name
  - The IETF provides no guidelines on ensuring that the names of CAs are unambiguous

Liaison to IETF on the resolution of DR320

- Liaison request:
  - The IETF PKIX group to comment on this statement.
  - If the statement is correct, we ask the IETF to consider putting a mechanism in place to prevent conflict, e.g. a list of existing CA names that deployers of new CAs could check for naming conflicts.

Liaison to IETF on the resolution of DR320

- Response (proposed)
  - Yes the statement is true (IETF does not have any such mechanism in place)
    - 3280 4.1.2.4 Issuer - “This specification does not restrict the set of attribute types that may appear in names.”
  - No, it is not reasonable for IETF to put any such mechanism in place.

Way forward

- Response requested by 2008-03-01
- Response?