Internationalized Email Addresses in X.509 certificates

IETF96

Alexey Melnikov
Weihaw Chuang (presenting)
local-part@domain
   local-part: UTF-8
   domain: U-label or NR-LDH

GeneralName ::= CHOICE {
   otherName [0]     OtherName,
   rfc822Name [1]     IA5String,
   ....}

OtherName ::= SEQUENCE {
   id-on-smtputf8Name (type-id) OBJECT IDENTIFIER,
   smtputf8Name (value) [0] EXPLICIT ANY}
Design Choices- Potential Open Issues

● OtherName vs GeneralName
  ○ OtherName less likely to break existing code
  ○ OID overhead

● smtputf8Name name constraint intentionally excludes similar types
  ○ prevent interaction
  ○ "duplicate" rfc822Name name constraint
Version 01 - Closed Issues

- Pick one representation (ACE and U-label)
- Minimize ACE / U-label conversions
- Specify name constraints and comparisons

Version 02/03 - Closed Issues

- Internationalization, ABNF, Unicode terminology, general language clean up
  - ACE -> A-label
- Restrict smtputf8Name to non-ASCII local-part
- Comparison language clean up
Version 04 - Closed Issues

- Language clean up
- Diagram added

Planned work

- Diagram clean up
Deployment Considerations

- **Openssl**
  - Update probably about a year- patch helps

- **CA**
  - Not started
  - Chrome security team can facilitate