Internationalized Email Addresses in X.509 certificates

IETF98

Alexey Melnikov
Wei 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}
Status

- Last call feedback on drafts 06-08
  - Name constraint repair (rest of slides)
  - Domain must conform to IDNA2008 (including those in rfc822Name)
  - RFC5322 vs RFC5321 email address
  - Prohibiting look-alike A-label ('cc--' prefix)
  - Case-folding (ASCII domain lower case otherwise none allowed)
Name Constraints

- smtpUTF8Name name constraint independent from rfc822name
Legacy ICA Bypass  (SmtpUTF8Name aware path verifier)

- smtpUTF8Name unconstrained

```
<p>| |</p>
<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Legacy Intermediate CA</td>
</tr>
<tr>
<td>Permitted</td>
</tr>
<tr>
<td>rfc822Name: example.com</td>
</tr>
</tbody>
</table>

<p>| |</p>
<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Entity</td>
</tr>
<tr>
<td>subjectAltName</td>
</tr>
<tr>
<td>rfc822Name: <a href="mailto:student@example.com">student@example.com</a></td>
</tr>
<tr>
<td>SmtpUTF8Name: 学生@example.com</td>
</tr>
</tbody>
</table>
```
Path verifier checks name constraints validity

- smtpUTF8Name subject requires both smtpUTF8Name + rfc822Name name constraint, else fail
- legacy rfc822Name name constraint on rfc822Name subject allowed

Intermediate CA

Permitted
rfc822Name: example.com

Entity

subjectAltName
rfc822Name: student@example.com

SmtpUTF8Name: 学生@example.com

not allowed
Path verifier checks name constraints validity (cont)

- smtpUTF8Name subject requires both smtpUTF8Name + rfc822Name name constraint, else fail
- legacy rfc822Name name constraint on rfc822Name subject allowed
Legacy path verifier *(SmtpUTF8Name aware ICA)*

- smtpUTF8Name unconstrained but...
- (09: extensions critical $\implies$ verification fails)

```
Intermediate CA

Permitted
rfc822Name: example.com

Excluded
SmtpUTF8Name: example.com

Entity

subjectAltName
rfc822Name: student@example.com

SmtpUTF8Name: 学生@example.com
```