Attribute Certificate Profile for XMPP Domain Name Assertion
draft-hildebrand-dna-00.txt

Presented to XMPP/PKIX WG
By Sean Turner
IETF 76
What’s the Problem?

• As large hosting providers begin providing XMPP services for multiple domains, several issues with previous mechanisms for server-to-server federation have become apparent.

• Hosting providers can’t hold customer certs
  – Too much responsibility
  – Not allowed by customers

• Too many connections between servers
  – Two for each domain pair
  – E.g.: 10k domains each side = 200 million sockets
A Possible Solution

• Assert domain names
  – OUTSIDE start-TLS
  – At the application level

• Verify domains with extensible proof
  – One such proof: Attribute Certificates (RFC 3281)
  – Others (such as SAML) can be added later
  – Custom assertions possible
Attribute Certificate Profile

• Based on RFC 3281bis: An Internet Attribute Certificate Profile for Authorization.
• Unfortunately, it’s not just as easy as pointing there are:
  – Choices for pointers to issuer’s certificate
  – Choices to identify holder
  – Choices for attribute
  – Choices for extensions
  – Choices for revocation
  – Choices for signature algorithm
Attribute Certificate Issuer’s Public Key Certificate

• RFC 3281 requires that the issuer’s public key certificate:
  – Conforms to RFC 5280,
  – Has digitalSignature set in Key Usage,
  – Not include Basic Constraints’ cA boolean set to TRUE.

• RFC 5280 allows NULL subject name and critical subject alternative name.
  – Suggest that we require non-NULL subject names and include issuer alternative name if subject alternative name present.
Holder Options

• Supports pointing to public key certificate, a name, or an object.

• Recommend that we follow RFC 3281 “SHOULD” and use issuer/serial #.
Attribute Choices

• Attribute certificates need at least one attribute.
• Recommend Access Identity:

\[
\text{SvceAuthInfo ::= SEQUENCE \{} \begin{array}{ll}
\text{service} & \text{GeneralName}, \\
\text{ident} & \text{GeneralName}, \\
\text{authInfo} & \text{OCTET STRING OPTIONAL} \end{array} \}
\]

• Need to define an OTHER-NAME for service and ident (can we use one name for both?):
  – Define XMPP service OID: id-xmpp
  – Define XMPP ident OIDs: id-xmpp-client and id-xmpp-server
Extension Choices

• Issuers may have more than one public key certificate.
  – Recommend including Authority Key Identifier if issuer has more than one public key certificate.

• Issuer may also have subject alternative names.
  – Recommend including non-critical issuer alternative name if issuer’s certificate includes subject alternative name. (IAN not in RFC 3281)

• One other we’ll discuss in a minutes.

• Others are OPTIONAL.
Revocation Choices

- RFC 3281 supports two schemes:
  - No Revocation Available, and
  - Pointer in AC.

- Recommend the No Revocation Available scheme:
  - It’s the MUST scheme in RFC 3281,
  - The XMPP certificates are good for 1-year, and
  - There will be contracts involved.
Signature Algorithm Choices

• Propose that we move to PKCS #1 version 1.5 signature algorithm with SHA-256, as defined in RFC 4055.
  – Avoids transitioning from SHA-1.
Transfer Encoding

• Deciding whether to use “certs-only” CMS message or XML `<ac> </ac>` & `<pkc> </pkc>`