claimSigning EKU

Agenda

- Purpose
- Use Cases
- Discussion of Approach
- Next Steps

Purpose of the claimSigning EKU

- Indicates that the certificate holder is authorized to sign security tokens to assert claims, or attributes, about a subject
- Provides a method for a service to assert that a statement about a subject is true
- Indicates that the certificate is to be used for the purpose of signing claims
  - Just as a certificate that asserts certSigning key usage indicates that the certificate is intended to be used for signing Identity Certificates

Why?

- Most CAs populate EKU with ServerAuth (and sometimes clientAuth)
  - Strict interpretation of RFC5280 means that using this cert to “sign” anything other than handshake material should lead to a failure to validate.
  - SO:
    - Either change various protocols and product to not require serverAuth OR
    - Have a new EKU for claimSigning OR
    - Overload CP OIDs yet again
      - May cause OID explosion if doing Federated Identity at multiple assurance levels
      - MUCH harder to process.
      - Moves Federation Designation into the CA realm, and makes a mess of the CP.

Use Case #1: Secure Token Service

- An IdP secure token service (STS) could use an X.509 certificate containing the claimSigning EKU to sign SAML assertions containing an identifier and attributes about a user
- This indicates to the relying party that they can relying on the assertions made in the claim
  - Realm designation is out of scope.

Use Case #1: Federated Single Sign On (STS by another name)

1. A Relying Party (RP) relies on SAML Assertions from an Identity Provider (IdP) to grant access to a protected resource.
2. The IdP authenticates the user and generates a SAML Assertion containing claims (email address, first-name, etc.) about the end user.
3. The IdP digitally signs the SAML Assertion using an X.509 certificate that contains the claimSigning EKU and sends the Assertion to the RP.
4. As part of the signature validation process the RP checks that the certificate used to sign the assertion contains the claim signing EKU.

Use Case #2: Attribute Authority

1. An Attribute Authority (AA) is issued a certificate containing the claimSigning EKU.
2. The AA then issues attribute certificates, which contain claims (clearance level, professional certifications, etc.) about a security principle
3. An attribute certificate is then presented to an RP to convey this claim information
4. As part of the signature validation process the RP verifies that the AA's certificate contains the claimSigning EKU.
5. If the EKU is present and the signature validates, the RP then knows the AA is authorized to sign Attribute Certificates.

- NOTE: This is similar to the certSigning key usage bit, which is used to identify the certificate issued to a CA that is to be used for signing Identity Certificates.

Approach

- Submitted draft to PKIX
  - Some suggest a claimSigning EKU is better suited in the Application WG
    - How is claimSigning different from emailProtection?
- What is the best approach that benefits the widest community?
- Other options?
  - What about making it more generic "tokenSigning"

Next Steps

- Concrete actions for obtaining a claimSigning EKU

Contact

Patrick Patterson
President and Chief PKI Architect
Carillon Information Security Inc.
http://www.carillon.ca

tel: +1 514 485 0789
mobile: +1 514 994 8699
fax: +1 450 424 9559

Matt King
Protiviti, Inc.
Government Services
Matthew.King@pgs.protiviti.com
410-271-5624 (Mobile)