Enhancing Credential Selection in IETF Protocols

Stefan Santesson
stefans@microsoft.com

Problem

- The client user has a set of credentials
- The service request the user to authenticate using a credential
- The user has several credential matching the criteria from the service

Case study TLS and X.509

- Criteria restricted to CA names and public key algorithms
- We have encountered many situations where this is not sufficient
  - Multipple roles
  - Different services under common roots

Proposal

- http://www.ietf.org/internet-drafts/draft-santesson-credsel-01.txt
- A comon data construct for credential selection that can be sent in multipple protocols
- Currently generic, but may be restricted to X.509.

Structure

```
SelectionCriteria ::= SEQUENCE OF Criteria

        Criteria ::=  {
          credentialType     OBJECT IDENTIFIER  --identifier for
                                                 --credential type
          selectData          SelectData }

        SelectData ::= SEQUENCE {
          basicSelectData    [0]  BasicSelectData OPTIONAL
          advancedSelectData [1]  AdvancedSelectData OPTIONAL}


        AdvancedSelectData ::= {
          selectSyntaxID       OBJECT IDENTIFIER
          selectData           ANY DEFINED BY selectSyntaxID ]

        BasicSelectData ::= SEQUENCE {
          includeStrings   [0]   SelectStrings OPTIONAL
          excludeStrings   [1]   SelectStrings OPTIONAL }

        SelectStrings ::= SEQUENCE OF AltValues

        AltValues ::= SEQUENCE OF OCTET STRING
```

Example

BasicSelectData (SEQUENCE)

Include strings (SEQUENCE)

- Altvalues (SEQUENCE)
  - Certificate policy 1 OID
  - Certificate policy 2 OID
- Altvalues (SEQUENCE)
  - Key usage extension (with only digital signature bit set)

Exclude strings (SEQUENCE)

- Altvalues (SEQUENCE)
  - EKU A OID
  - EKU B OID

Certificate match if all of the following is true:

- includes certificate policy 1 or certificate policy 2 (or both)
- includes a key usage extension with only the digital signature bit set
- does not contain EKU OID A
- does not contain EKU OID B