PKCS #9 v2.0

Magnus Nyström
RSA Laboratories
PKCS Workshop, 1999

RSA
LABORATORIES

Background

- Historically, PKCS #9 has specified *selected attributes*
- They have been used in PKCS #6, PKCS #7 and PKCS #10
- With increasing popularity for LDAP-accessible directories, more attributes (and a supporting object class) were needed

Overview of differences from v1:

- Two new (auxiliary) object classes:
  - pkcsEntity
  - naturalPerson
- New attributes for use with these classes (e.g. “pseudonym”)
- Some other new attributes:
  - Random nonce
  - Sequence number

Overview of differences, cont..

- Some older attributes have been updated (DirectoryString, internationalization)
- “Compilable” ASN.1 module included
- Collected undocumented OIDs and attributes defined elsewhere
- BNF Schema summary included for easier integration in LDAP services

The pkcsEntity object class

```
pkcsEntity OBJECT-CLASS ::= {
  SUBCLASS OF {top}
  KIND auxiliary
  MAY CONTAIN {PKCS9AttributeSet}
  ID pkcs-9-oc-pkcsEntity
  }
```

The PKCS9AttributeSet

-
  ```
  PKCS9AttributeSet ATTRIBUTE ::= {
  userPKCS12 | pKCS15Token |
  encryptedPrivateKeyInfo, …}
  ```

The userPKCS12Attribute

- Intended to store PKCS #12 PFX PDUs in directories
- Multi-valued

The pKCS15Token attribute

- Intended for storage of PKCS #15 soft-tokens in directories (once such tokens are defined in PKCS #15…)
- Multi-valued

The encryptedPrivateKeyInfo attribute

- Intended for storage of simple encrypted private keys in directories
- Note: No (explicit) integrity check!
- Multi-valued

The naturalPerson object class

```
• naturalPerson OBJECT-CLASS ::= {
    SUBCLASS OF {top}
    KIND auxiliary
    MAY CONTAIN {NaturalPersonAttributeSet}
    ID pkcs-9-oc-naturalPerson
    }
```

The NaturalPersonAttributeSet

-
  ```
  NaturalPersonAttributeSet ATTRIBUTE ::= {
  
  emailAddress | unstructuredName |
  unstructuredAddress | pseudonym | dateOfBirth |
  placeOfBirth | gender | countryOfCitizenship |
  countryOfResidence, …}
  ```

The pseudonym attribute

- Useful attribute in distinguished names for anonymous (at least in some sense) certificates
- Intended to be used in IETF’s *qualified certificates*
- Multi-valued (?)

The dateOfBirth attribute

- Specifies the date of birth
- Intended to be used in IETF’s *qualified certificates*
- Single-valued...

The placeOfBirth attribute

- DirectoryString
- Intended to be used in IETF's *qualified certificates*
- Single-valued...

The gender attribute

- Printable string (‘M’ or ‘F’)
- Intended to be used in IETF’s *qualified certificates*
- Single-valued

The countryOfCitizenship and countryOfResidence attributes

- Printable strings (ISO 3166)
- Intended to be used in IETF's *qualified certificates*
- Multi-valued

Other new attributes

- *randomNonce*: For use in conjunction with signatures to prevent replay attacks. Especially when no signingTime is available.
- *sequenceNumber*: For the same use. Similar to numbering your checks.

Modified (extended) old attributes

- *unstructuredName, unstructuredAddress, challengePassword, signingDescription*: Syntax now extended to allow internationalization (implementations SHOULD use old syntax if possible)
- *signingTime*: updated to be in accordance with S/MIME

Time schedule

- If you have any comments - please give them on or before October 25th.
- Expect third draft early in November, for a short (2 w) review period (unless major changes)
- v2.0 to be published in late November /early December 1999.

Comments & Suggestions

- Please send comments to
  - pkcs-tng@rsasecurity.com or
  - pkcs-editor@rsasecurity.com