Base Object Examples

Example 1

Current:

2.1.2 Credential

A credential is a protocol-only object, used for client identification purposes and not managed by the key management system, e.g., user id/password pairs, Kerberos tokens, etc. See Section 8.

Object	Encoding	Required
Credential	Structure	Yes
Credential Type	Enumeration	Yes
Credential Value	Octet String	Yes

Proposed:

2.1.2 Credential

A credential is a structure (see Table yy) used for client identification purposes and not managed by the key management system (e.g., user id/password pairs, Kerberos tokens, etc. See Section 8).

Table y - Credential Structure Format

Field	Encoding	Required
Credential Type	Enumeration	Yes
Credential Value	Octet String	Yes

Example 2

Current:
(text section not included)

Object	Encoding	Required Field
Key Wrapping Data	Structure	Yes
Wrapping Method	Enumeration	Yes
Encryption Key Information	Structure	No
MAC/Signature Key Information	Structure	No. Corresponds to the symmetric key used to MAC the Key Value or the private key used to sign the Key Value
MAC/Signature	Octet String	No
IV/Counter/Nonce	Octet String	No

Proposed:

Table x - Key Wrapping Data Structure Format

Field	Encoding	Required
Wrapping Method	Enumeration	Yes
Encryption Key Information	Structure	No
MAC/Signature Key Information	Structure	No. Corresponds to the symmetric key used to MAC the Key Value or the private key used to sign the Key Value
MAC/Signature	Octet String	No
IV/Counter/Nonce	Octet String	No

Managed Object Examples

Current:

2.2.2 Certificate

A Managed Cryptographic Object, which is a digital certificate, such as an encoded X.509 certificate.

Object	Encoding	Required Field
Certificate	Structure	Yes
Certificate Type	Enumeration	Yes
Certificate Value	Octet String	Yes

2.2.2 Symmetric Key

A Managed Cryptographic Object, which is a symmetric key.

Object	Encoding	Required Field
Symmetric Key	Structure	Yes
Key Block	Structure	Yes

Proposed:

2.2.1 Certificate

A certificate object (see Table yy) is a Managed Cryptographic Object, and contains a digital certificate (e.g., an encoded X.509 certificate).

Table yy - Certificate Object Format

Field	Encoding	Required
Certificate Type	Enumeration	Yes
Certificate Value	Octet String	Yes

2.2.2 Symmetric Key

A symmetric key object (see Table xx) is a Managed Cryptographic Object, and contains a symmetric key.

Table xx - Symmetric Key Object Format

Field	Encoding	Required
Key Block	Structure	Yes

Notes:

- The name/title of each object or structure is relocated to the title of the table. This simplifies the tables, and allows the column headers to consistently indicate the contents. It also removes any implied recursion (i.e., object that contains itself).
- Each table is titled and referenced from the text (this suggestion is applicable to the entire standard).
- Base objects seem to be consistently ‘structures’, which facilitates just calling them structures instead of objects (or perhaps “base structures” or “object structures”) and further distinguishes them from managed objects.