Proposal for Basic Asymmetric Key Profiles

Created by: Sean Turner, IECA Inc.

Contributors:

Kelley Burgin, National Security Agency

Chris Dunn, SafeNet, Inc.

Indra Fitzgerld, HP

Judith Furlong, EMC Corporation

Jay Jacobs, Target Corporation

Version: 1.6

Date: 20 May 2010

Reference: Key Management Interoperability Protocol Specification Version 1.0 Committee Draft 10, 18 March 2010

1.1 Basic Asymmetric Key Store Conformance Clauses

This proposal intends to meet this OASIS requirement by building on the KMIP Server Conformance Clauses defined in the KMIP Specification to allow asymmetric key pairs generated external to the key server to be vaulted by a key server. The intent is to simply support key registration for a very limited number of key types.

1.1.1 Implementation Conformance

An implementation is a conforming KMIP Basic Asymmetric Key Store if the implementation meets the conditions as outlined in the following section.

1.1.2 Conformance as a Basic Asymmetric Key Store

An implementation conforms to this specification as a KMIP Asymmetric Key Store if it meets the following conditions:

1. Supports the conditions required by the KMIP Server conformance clauses ([KMIP-Spec] 12.1)
2. Supports the following additional objects:
    a. Public Key ([KMIP-Spec] 2.2.3)
    b. Private Key ([KMIP-Spec] 2.2.4)
3. Supports the following client-to-server operations:
    a. Register ([KMIP-Spec] 4.3)
4. Supports the following subset of enumerated attributes:
    a. Object Type ([KMIP-Spec] 3.3 and 9.1.3.2.11)
        i. Public Key
        ii. Private Key
    b. Cryptographic Algorithm ([KMIP-Spec] 3.4 and 9.1.3.2.12)
        i. RSA

c. Link ([KMIP-Spec] 3.29 and 9.1.3.2.19)
    i. Public Key Link
    ii. Private Key Link
5. Supports the following subset of enumerated objects:
    a. Key Format Type ([KMIP-Spec] 2.1.3 and 9.1.3.2.3)
        i. Raw
        ii. PKCS#1
6. Optionally supports any clause within [KMIP-Spec] that is not listed above
7. Optionally supports extensions outside the scope of this standard (e.g., vendor extensions, Conformance Clauses) that do not contradict any requirements within this standard

1.2 Basic Asymmetric Key and Certificate Store Conformance Clauses

This proposal intends to meet this OASIS requirement by building on the KMIP Server Conformance Clauses defined in the KMIP Specification to allow asymmetric key pairs and certificates generated external to the key server to be vaulted by a key server. The intent is to simply support key and certificate registration for a very limited number of key types.

1.2.1 Implementation Conformance

An implementation is a conforming KMIP Basic Asymmetric Key and Certificate Store if the implementation meets the conditions as outlined in the following section.

1.2.2 Conformance as a Basic Asymmetric Key and Certificate Store

An implementation conforms to this specification as a KMIP Asymmetric Key and Certificate Store if it meets the following conditions:

1. Supports the conditions required by the KMIP Server conformance clauses ([KMIP-Spec] 12.1)
2. Supports the following subsets of additional objects:
    a. Certificate ([KMIP-Spec] 2.2.1)
    b. Public Key ([KMIP-Spec] 2.2.3)
    c. Private Key ([KMIP-Spec] 2.2.4)
3. Supports the following client-to-server operations:
    a. Register ([KMIP-Spec] 4.3)
4. Supports the following subset of enumerated attributes:
    a. Object Type ([KMIP-Spec] 3.3 and 9.1.3.2.11)
        i. Certificate
        ii. Public Key
        iii. Private Key
    b. Cryptographic Algorithm ([KMIP-Spec] 3.4 and 9.1.3.2.12)
        i. RSA
    c. Certificate Type ([KMIP-Spec] 3.8 and 9.1.3.2.6)
        i. X.509

d. Certificate Identifier ([KMIP-Spec] 3.9)
e. Certificate Subject ([KMIP-Spec] 3.10)
f. Certificate Issuer ([KMIP-Spec] 3.11)
g. Link ([KMIP-Spec] 3.29 and 9.1.3.2.19)
    a. Certificate Link
    b. Public Key Link
    c. Private Key Link

5. Supports the following subset of enumerated objects:
    d. Key Format Type ([KMIP-Spec] 2.1.3 and 9.1.3.2.3)
        i. Raw
        ii. PKCS#1
        iii. X.509
6. Optionally supports any clause within [KMIP-Spec] that is not listed above
7. Optionally supports extensions outside the scope of this standard (e.g., vendor extensions, Conformance Clauses) that do not contradict any requirements within this standard

1.3 Basic Asymmetric Key Foundry and Server Conformance Clauses

This proposal intends to meet this OASIS requirement by building on the KMIP Server Conformance Clauses defined in the KMIP Specification to provide basic asymmetric key services for central key generation (by the key server). The intent is to simply allow key creation and serving with very limited key types.

1.3.1 Implementation Conformance

An implementation is a conforming KMIP Basic Asymmetric Key Foundry and Server if the implementation meets the conditions as outlined in the following section.

1.3.2 Conformance as a Basic Asymmetric Key Foundry and Server

An implementation conforms to this specification as a KMIP Asymmetric Key Foundry and Server if it meets the following conditions:

1. Supports the conditions required by the KMIP Server conformance clauses ([KMIP-Spec] 12.1)
2. Supports the following additional objects:
    a. Public Key ([KMIP-Spec] 2.2.3)
    b. Private Key ([KMIP-Spec] 2.2.4)
3. Supports the following client-to-server operations:
    a. Create Key Pair ([KMIP-Spec] 4.2)
    b. Re-key Key Pair ([KMIP-Spec] TBD)
4. Supports the following subset of enumerated attributes:
    a. Object Type ([KMIP-Spec] 3.3 and 9.1.3.2.11)
        i. Public Key
        ii. Private Key
    b. Cryptographic Algorithm ([KMIP-Spec] 3.4 and 9.1.3.2.12)

i. RSA

c. Link ([KMIP-Spec] 3.29 and 9.1.3.2.19)

i. Public Key Link

ii. Private Key Link

iii. Replacement Object Link

iv. Replaced Object Link

5. Supports the following subset of enumerated objects:

c. Key Format Type ([KMIP-Spec] 2.1.3 and 9.1.3.2.3)

i. Raw

ii. PKCS#1

iii. Transparent RSA private key ([KMIP-Spec] 2.1.7.4)

iv. Transparent RSA public key ([KMIP-Spec] 2.1.7.5)

6. Optionally supports any clause within [KMIP-Spec] that is not listed above
7. Optionally supports extensions outside the scope of this standard (e.g., vendor extensions, Conformance Clauses) that do not contradict any requirements within this standard

1.4 Basic Certificate Server Conformance Clauses

This proposal intends to meet this OASIS requirement by building on the KMIP Server Conformance Clauses defined in the KMIP Specification to provide basic asymmetric key services for local key generation (external to the key server) and certification via a key server.

1.4.1 Implementation Conformance

An implementation is a conforming KMIP Basic Certificate Server if the implementation meets the conditions as outlined in the following section.

1.4.2 Conformance as a Basic Certificate Server

An implementation conforms to this specification as a KMIP Certificate Server if it meets the following conditions:

1. Supports the conditions required by the KMIP Server conformance clauses ([KMIP-Spec] 12.1)
2. Supports the following additional objects:
   a. Certificate ([KMIP-Spec] 2.2.1)
   b. Public Key ([KMIP-Spec] 2.2.3)
   c. Private Key ([KMIP-Spec] 2.2.4)
3. Supports the following client-to-server operations:
   a. Certify ([KMIP-Spec] 4.6)
   b. Re-Certify ([KMIP-Spec] 4.7)
4. Supports the following subset of enumerated attributes:
   a. Object Type ([KMIP-Spec] 3.3 and 9.1.3.2.11)
      i. Certificate
      ii. Public Key
      iii. Private Key
   b. Cryptographic Algorithm ([KMIP-Spec] 3.4 and 9.1.3.2.12)

i. RSA

c. Certificate Type ([KMIP-Spec] 3.8 and 9.1.3.2.6)
   i. X.509
d. Certificate Identifier ([KMIP-Spec] 3.9)
e. Certificate Subject ([KMIP-Spec] 3.10)
f. Certificate Issuer ([KMIP-Spec] 3.11)
g. Link ([KMIP-Spec] 3.29 and 9.1.3.2.19)
   i. Certificate Link
   ii. Public Key Link
   iii. Private Key Link
   iv. Replacement Object Link
   v. Replaced Object Link
h. Certificate Request Type ([KMIP-Spec] 4.6, 4.7 and 9.1.3.2.21)
   i. PKCS#10
   ii. PEM

5. Supports the following subsets of enumerated objects:
   d. Key Format Type ([KMIP-Spec] 2.1.3 and 9.1.3.2.3)
      i. Raw
      ii. PKCS#1
      iii. X.509
6. Optionally supports any clause within [KMIP-Spec] that is not listed above
7. Optionally supports extensions outside the scope of this standard (e.g., vendor extensions, Conformance Clauses) that do not contradict any requirements within this standard

1.5 Basic Asymmetric Key Foundry and Certificate Server Conformance Clauses

This proposal intends to meet this OASIS requirement by building on the KMIP Server Conformance Clauses defined in the KMIP Specification to provide basic asymmetric key services for central key generation (by the key server). The intent is to simply allow key and certificate creation and serving with very limited key types.

1.5.1 Implementation Conformance

An implementation is a conforming KMIP Basic Asymmetric Key Foundry and Server if the implementation meets the conditions as outlined in the following section.

1.5.2 Conformance as a Basic Asymmetric Key Foundry and Certificate Server

An implementation conforms to this specification as a KMIP Asymmetric Key Foundry and Certificate Server (Central Generation) if it meets the following conditions:

1. Supports the conditions required by the KMIP Server conformance clauses ([KMIP-Spec] 12.1)
2. Supports the following additional objects:
   a. Certificate ([KMIP-Spec] 2.2.1)

b. Public Key ([KMIP-Spec] 2.2.3)
c. Private Key ([KMIP-Spec] 2.2.4)

3. Supports the following client-to-server operations:
   a. Create Key Pair ([KMIP-Spec] 4.2)
   b. Re-key Key Pair ([KMIP-Spec] TBD)
   c. Certify ([KMIP-Spec] 4.6)
   d. Re-Certify ([KMIP-Spec] 4.7)
4. Supports the following subset of enumerated attributes:
   a. Object Type ([KMIP-Spec] 3.3 and 9.1.3.2.11)
      i. Certificate
      ii. Public Key
      iii. Private Key
   b. Cryptographic Algorithm ([KMIP-Spec] 3.4 and 9.1.3.2.12)
      i. RSA
   c. Certificate Type ([KMIP-Spec] 3.8 and 9.1.3.2.6)
      i. X.509
   d. Certificate Identifier ([KMIP-Spec] 3.9)
   e. Certificate Subject ([KMIP-Spec] 3.10)
   f. Certificate Issuer ([KMIP-Spec] 3.11)
   g. Link ([KMIP-Spec] 3.29 and 9.1.3.2.19)
      i. Certificate Link
      ii. Public Key Link
      iii. Private Key Link
      iv. Replacement Object Link
      v. Replaced Object Link
   h. Certificate Request Type ([KMIP-Spec] 4.6, 4.7 and 9.1.3.2.21)
      i. PKCS#10
      ii. PEM
5. Supports the following subset of enumerated objects:
   d. Key Format Type ([KMIP-Spec] 2.1.3 and 9.1.3.2.3)
      i. Raw
      ii. PKCS#1
      iii. X.509
      iv. Transparent RSA private key ([KMIP-Spec] 2.1.7.4)
      v. Transparent RSA public key ([KMIP-Spec] 2.1.7.4)
6. Optionally supports any clause within [KMIP-Spec] that is not listed above
7. Optionally supports extensions outside the scope of this standard (e.g., vendor extensions, Conformance Clauses) that do not contradict any requirements within this standard