Clarifications to KMIP v1.1 for Asymmetric Crypto and Certificates

J. Furlong

29 September 2010

Topic 1: Cryptographic Length of Asymmetric Keys

For PublicKey and PrivateKey objects:

1) How do we represent the CryptographicLengths of these objects? The actual lengths of the cryptographic material may vary, depending on input parameters, but users thinking they have a 1024-bit key pair will be quite dismayed if our length calculator reports anything other than what was input to the generation process. This becomes more problematic for keys that arrive via Register, rather than CreateKeyPair.

Would propose that the lengths should be what the keypair generator would require as input, rather than a mechanical evaluation of the key itself. This may require some "fuzzy logic"...it's 1024-bitish...the spec should clearly instruct the server implementers what to do and what the limits might be on their flexibility.

- Disposition
  - No change to KMIP Specification
  - Add text to the KMIP Usage Guide to address the ‘fuzziness’ of asymmetric key lengths

Topic 2: Signature Algorithms in Certificate Objects

For Certificate objects:

1) Do all Certificates have a CryptographicAlgorithm? If so, what is it? None of the current algorithms seem to relate to the actual signature on the certificate.

Would propose that the algorithm of the Certificate is the algorithm of the enclosed public key.

- Disposition
  - Need to add signature algorithm to KMIP Specification
    - Open question as to how to represent the signature algorithm as an enumerated attribute or as a composite attribute (like crypto parameters)

Topic 3: Certificate Length

2) Do all Certificates have a CryptographicLength? If so, what is it? I do not believe that the bitlength of the encoded certificate is very interesting...

Would propose that the length of the Certificate is the length of the enclosed public key (as interpreted above).

- Disposition
  - Need to add certificate length to the KMP Specification
    - Open question as to what value should be used as the certificate length either the encoded length of the certificate or the length of the public key included in the certificate

Topic 4: ASN.1 to String Conversion

3) The CertificateSubject is a structure with the distinguished name of the subject, along with alternate names. Both of these are simply listed as text strings, but no mechanism is suggested for producing these strings from the underlying ASN.1 in the certificate. We may luck out on producing the former, but the latter is the road less travelled, and may produce more mismatches. (Not to mention that one may loses some context in knowing what kind of alternate name this was, if I remember correctly. Simply rendering as a text string may lose the fact that this alternate name was the DNS Name, for example).

Would propose that a TC member might take this one as a work item, if we are addressing only in 1.1. (And I suspect a production rule is really needed even for the dn.)

4) Similar comments regarding CertificateIssuer.

- Disposition
  - Need to add guidance to KMIP Specification as how to translate different name formats form ASN.1 to the string format used in KMIP
    - Open question as to details of this guidance
  - May also require changes to KMIP Usage Guide and KMIP Use Cases