Using the Same Asymmetric Key Pair in Multiple Algorithms

Judy Furlong, EMC

Version 0.3

11 February 2010

References:

KMIP Specification Version 1.0, Committee Draft 06, 09 November 2009

KMIP Usage Guide Version 1.0, Committee Draft 05, 09 November 2009

Background

There have been some questions raised as to why the v1 KMIP Specification provides separate key structures for DSA and DH keys and ECDSA and ECDH keys where a single key pair may be used in both algorithms. This proposal provides text for inclusion in the KMIP Usage Guide to explain why separate key structures were provided.

New Section for Inclusion in the KMIP Usage Guide

Using the Same Asymmetric Key Pair in Multiple Algorithms

There are mathematical relationships between certain asymmetric cryptographic algorithms such as the Digital Signature Algorithm (DSA) and Diffie-Hellman (DH) and their elliptic curve equivalents ECDSA and ECDH that allow the same asymmetric key pair to be used in both algorithms. In addition, one will notice overlaps in the key format used to represent the asymmetric key pair for each algorithm type.

Even though a single key pair may be used in multiple algorithms, the KMIP Specification has chosen to specify separate key formats for representing the asymmetric key pair for use in each algorithm. This approach keeps KMIP in line with the reference standards (e.g., NIST FIPS 186-3, ANSI X9.42) from which the key formats for DSA, DH, ECDSA, etc. are obtained and the best practice documents (e.g. NIST SP800-57 part 1, NIST 800-56A) which recommend that a key pair only be used for one purpose.