KMIP Counters

Tony Cox

Problem

- No way to determine usage of Cryptographic objects
  - Has this CSR been signed?
  - How many unsigned CSRs exist?
  - Has this key been used to encrypt or decrypt?
  - How many enc/dec has this key performed?
- Lack of data limits server automation scope

Solution

- Add “Counters” as an attribute for cryptographic objects
- Simple integer-based increment counter set and maintained by the server.
- Apply to common crypto operations- Certify, Decrypt, Encrypt, Sign, Signature Verify
- Document in the same style as Links

4.13 Counters

There are object attributes with name suffixes that identify themselves as "Counter" attributes. These attributes serve to record an instance of usage of an object as the subject of a KMIP operation. The prefix of the attribute name states the nature of the counter (which opaeration). Modification of this attribute is performed by the server via incrementing the counter value on each instance of "use".

"Counter" attributes SHALL be present for Certificates, Certificate Requests, Private keys, Public keys and Symmetric keys.

4.13.1 Certify Counter

The *Certify Counter* attribute is recorded against a given Certificate Request or Public Key and records each instance of a certify operation being performed on that Certificate Request or Public Key.

The Certify Counter SHALL be incremented upon completion of a Certify or Recertify operation.

Item	Encoding
Certify Counter	Long Integer

Table 74: Certify Counter Attribute

SHALL always have a value	Yes
Initially set by	Server
Modifiable by server	Yes – incremented on Certify & ReCertify
Modifiable by client	No
Deletable by client	No
Multiple instances permitted	No
When implicitly set	Create, Register, Import
Applies to Object Types	Certificate Request, Public Key

Table 75: Certify Counter Attribute Rules

4.13.2 Decrypt Counter

The *Decrypt Counter* attribute is recorded against a given object and records each incidence of a decrypt operation being performed using that object.

The Decrypt Counter SHALL be incremented upon completion of a Decrypt operation.

Item	Encoding
Decrypt Counter	Long Integer

Table 76: Decrypt Counter Attribute

SHALL always have a value	Yes
Initially set by	Server
Modifiable by server	Yes – incremented on Decrypt
Modifiable by client	No
Deletable by client	No
Multiple instances permitted	No
When implicitly set	Create, Register, Import
Applies to Object Types	Cryptographic Objects

Table 77: Decrypt Counter Attribute Rules

4.13.3 Encrypt Counter

The *Encrypt Counter* attribute is recorded against a given object and records each incidence of a encrypt operation being performed using that object.

The Encrypt Counter SHALL be incremented upon completion of an Encrypt operation.

Item	Encoding
Encrypt Counter	Long Integer

Table 78: Encrypt Counter Attribute

SHALL always have a value	Yes
Initially set by	Server
Modifiable by server	Yes – incremented on Encrypt
Modifiable by client	No
Deletable by client	No
Multiple instances permitted	No
When implicitly set	Create, Register, Import
Applies to Object Types	Cryptographic Objects

Table 79: Encrypt Counter Attribute Rules

4.13.4 Sign Counter

The *Sign Counter* attribute is recorded against a object and records each incidence of a sign operation being performed using that object.

The Sign Counter SHALL be incremented upon completion of a Sign operation.

Item	Encoding
Encrypt Counter	Long Integer

Table 80: Sign Counter Attribute

SHALL always have a value	Yes
Initially set by	Server
Modifiable by server	Yes – incremented on Sign
Modifiable by client	No
Deletable by client	No
Multiple instances permitted	No
When implicitly set	Create, Register, Import
Applies to Object Types	Cryptographic Objects

Table 81: Sign Counter Attribute Rules

4.13.5 Signature Verify Counter

The *Signature Verify Counter* attribute is recorded against an object and records each incidence of a sign operation being performed on that object.

The Signature Verify Counter SHALL be incremented upon completion of a Signature Verify operation.

Item	Encoding
Encrypt Counter	Long Integer

Table 82: Signature Verify Counter Attribute

SHALL always have a value	Yes
Initially set by	Server
Modifiable by server	Yes – incremented on Signature Verify
Modifiable by client	No
Deletable by client	No
Multiple instances permitted	No
When implicitly set	Create, Register, Import
Applies to Object Types	Cryptographic Objects

Table 83: Signature Verify Counter Attribute Rules

Summary

- Solves interoperability problem (various solutions in play)
- Provides useful data to aid in reporting and automation