

# 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 operation). 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.

<u>Item</u>	<u>Encoding</u>
<u>Certify Counter</u>	<u>Long Integer</u>

Table 74: Certify Counter Attribute

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

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.

<u>Item</u>	<u>Encoding</u>
<u>Decrypt Counter</u>	<u>Long Integer</u>

Table 76: Decrypt Counter Attribute

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

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.

<u>Item</u>	<u>Encoding</u>
<u>Encrypt Counter</u>	<u>Long Integer</u>

Table 78: Encrypt Counter Attribute

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

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.

<u>Item</u>	<u>Encoding</u>
<u>Encrypt Counter</u>	<u>Long Integer</u>

Table 80: Sign Counter Attribute

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

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.

<u>Item</u>	<u>Encoding</u>
<u>Encrypt Counter</u>	<u>Long Integer</u>

Table 82: Signature Verify Counter Attribute

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

Table 83: Signature Verify Counter Attribute Rules



# Summary

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