Result Status	Result Reason
Operation Failed	Object Not Found, Attestation Failed, Attestation Required, Feature Not Supported, Invalid Field, Invalid Message, Operation Not Supported, Permission Denied, Response Too Large

Table 213: Get Attribute List Errors

6.1.22 Get Constraints

This operation instructs the server to return the constraints that are being applied to Managed Objects during operations.

Request Payload		
Item	**REQUIRED**	**Description**

Table 214: Get Constraints Request Payload

Response Payload		
Item	**REQUIRED**	**Description**
Constraints	Yes	The set of Constraints that are being applied during operations.

Table 215: Get Constraints Response Payload

6.1.22.1 Error Handling – Get Constraints

This section details the specific Result Reasons that SHALL be returned for errors detected in a Get Constraints Operation.

Result Status	Result Reason
Operation Failed	Invalid Field, Invalid Object Type, Attestation Failed, Attestation Required, Feature Not Supported, Invalid Field, Invalid Message, Operation Not Supported, Permission Denied, Response Too Large

Table 216: Get Constraints Errors

~~6.1.22~~6.1.23 Get Usage Allocation

This operation requests the server to obtain an allocation from the current Usage Limits value to allow the client to use the Managed Cryptographic Object for applying cryptographic protection. The allocation only applies to Managed Objects that are able to be used for applying protection (e.g., symmetric keys for encryption, private keys for signing, etc.) and is only valid if the Managed Object has a Usage Limits attribute. Usage for processing cryptographically protected information (e.g., decryption, verification, etc.) is not limited and is not able to be allocated. A Managed Object that has a Usage Limits attribute SHALL NOT be used by a client for applying cryptographic protection unless an allocation has been obtained using this operation. The operation SHALL only be requested during the time that protection is enabled for these objects (i.e., after the Activation Date and before the Protect Stop Date). If the operation is requested for an object that has no Usage Limits attribute, or is not an object that MAY be used for applying cryptographic protection, then the server SHALL return an error.

Response Payload		
Item	**REQUIRED**	**Description**
Unique Identifier	Yes	The Unique Identifier of the Object.

Table 300~~297~~: Set Attribute Response Payload

~~6.1.47.16~~.1.48.1 Error Handling - Set Attribute

This section details the specific Result Reasons that SHALL be returned for errors detected in a Add Attribute Operation.

Result Status	Result Reason
Operation Failed	Invalid Attribute Value, Invalid Attribute Value, Multi Valued Attribute, Non Unique Name Attribute, Object Not Found, Read Only Attribute, Attestation Failed, Attestation Required, Feature Not Supported, Invalid Field, Invalid Message, Operation Not Supported, Permission Denied, Response Too Large

Table 301~~298~~: Set Attribute Errors

6.1.49 Set Constraints

This operation instructs the server to set the constraints that will be applied to Managed Objects during operations.

Request Payload		
Item	**REQUIRED**	**Description**
Constraints	Yes	The set of Constraints to apply during operations.

Table 302: Set Constraints Request Payload

Response Payload		
Item	**REQUIRED**	**Description**

Table 303: Set Constraints Response Payload

6.1.49.1 Error Handling – Set Constraints

This section details the specific Result Reasons that SHALL be returned for errors detected in a Set Constraints Operation.

Result Status	Result Reason
Operation Failed	Invalid Field, Invalid Object Type, Attestation Failed, Attestation Required, Feature Not Supported, Invalid Field, Invalid Message, Operation Not Supported, Permission Denied, Response Too Large

Table 304: Set Constraints Errors

7.4 Constraint

The *Constraint* is a structure that contains details of a constraint that is applied to operations that create Managed Objects.

Object	Encoding	REQUIRED
Constraint	Structure	Yes
Object Types	Structure	No
Object Groups	Structure	No
Attributes	Structure	No

Table 329: Constraint Structure

7.5 Constraints

A set of Constaint structures.

Object	Encoding	REQUIRED
Constraints	Structure	Yes
Constraint	Structure	No, May be repeated.

Table 330: Constraints Structure

~~7.4~~7.6 Correlation Value

The *Correlation Value* is used in requests and responses in cryptographic operations that support multi-part (streaming) operations. This is generated by the server and returned in the first response to an operation that is being performed across multiple requests. Note: the server decides which operations are supported for multi-part usage. A server-generated correlation value SHALL be specified in any subsequent cryptographic operations that pertain to the original operation.

Object	Encoding
Correlation Value	Byte String

Table 331~~323~~: Correlation Value Structure

~~7.5~~7.7 Data

The *Data* object is used in requests and responses in cryptographic operations that pass data between the client and the server.

Encoding	Description
Byte String	The Data
Enumeration	Data Enumeration
Integer	Zero based nth Data in the response. If negative the count is backwards from the beginning of the current operation's batch item.

Table 332~~324~~: Data encoding descriptions

Import	0000002A
Export	0000002B
Log	0000002C
Login	0000002D
Logout	0000002E
Delegated Login	0000002F
Adjust Attribute	00000030
Set Attribute	00000031
Set Endpoint Role	00000032
PKCS#11	00000033
Interop	00000034
Re-Provision	00000035
Set Constraints	00000037
Get Constraints	00000038
Extensions	8XXXXXXX

Table 440~~432~~: Operation Enumeration

11.37 Padding Method Enumeration

Padding Method	
Name	**Value**
None	00000001
OAEP	00000002
PKCS5	00000003
SSL3	00000004
Zeros	00000005
ANSI X9.23	00000006
ISO 10126	00000007
PKCS1 v1.5	00000008
X9.31	00000009
PSS	0000000A
Extensions	8XXXXXXX

Table 441~~433~~: Padding Method Enumeration

11.38 PKCS#11 Function Enumeration

The PKCS#11 Function enumerations are the 1-based offset count of the function in the CK_FUNCTION_LIST_3_0 structure as specified in [PKCS#11]

Unsupported Protocol Version	The operation cannot be performed with the provided protocol version
Usage Limit Exceeded	The usage limits or request count has been exceeded
Wrapping Object Archived	Wrapping Object is archived
Wrapping Object Destroyed	The object exists, but is destroyed
Wrapping Object Not Found	Wrapping object does not exist
Wrong Key Lifecycle State	The key lifecycle state is invalid for the operation, for example not Active for an Encrypt operation
General failure	The request failed for a reason other than any other reason enumeration value.
Constraint Violation	The request failed because one or more constraints were violated

Table 447~~439~~: Result Reason Encoding Descriptions

Result Reason	
Name	**Value**
Item Not Found	00000001
Response Too Large	00000002
Authentication Not Successful	00000003
Invalid Message	00000004
Operation Not Supported	00000005
Missing Data	00000006
Invalid Field	00000007
Feature Not Supported	00000008
Operation Canceled By Requester	00000009
Cryptographic Failure	0000000A
(Reserved)	0000000B
Permission Denied	0000000C
Object Archived	0000000D
(Reserved)	0000000E
Application Namespace Not Supported	0000000F
Key Format Type Not Supported	00000010
Key Compression Type Not Supported	00000011
Encoding Option Error	00000012
Key Value Not Present	00000013
Attestation Required	00000014
Attestation Failed	00000015

Tag	
Name	**Value**
Server Hashed Password	420155
One Time Password	420156
Hashed Password	420157
Adjustment Type	420158
PKCS#11 Interface	420159
PKCS#11 Function	42015A
PKCS#11 Input Parameters	42015B
PKCS#11 Output Parameters	42015C
PKCS#11 Return Code	42015D
Protection Storage Mask	42015E
Protection Storage Masks	42015F
Interop Function	420160
Interop Identifier	420161
Adjustment Value	420162
Common Protection Storage Masks	420163
Private Protection Storage Masks	420164
Public Protection Storage Masks	420165
Constraints	420168
Constraint	420169
(Reserved)	420XXX – 42FFFF
(Unused)	430000 – 53FFFF
Extensions	540000 – 54FFFF
(Unused)	550000 - FFFFFF

Table 454446: Tag Enumeration

11.55 Ticket Type Enumeration

State	
Name	**Value**
Login	00000001
Extensions	8XXXXXXX

Table 455447: Ticket Type Enumeration

11.56 Unique Identifier Enumeration

The following values may be specified in an operation request for a Unique Identifier: If multiple unique identifiers would be referenced then the operation is repeated for each of them. If an operation appears multiple times in a request, it is the most recent that is referred to.