

DRAFT

# SKS (Secure Key Store)

## API and Architecture



*Disclaimer:* This is a system in development. That is, the specification may change without notice.

# Table of Contents

1	Introduction.....	4
2	Core Functionality.....	4
2.1	Architecture.....	4
2.2	Provisioning API.....	4
2.3	User API.....	5
2.4	Security Model.....	5
2.5	Transaction Based Operation.....	5
2.6	Privacy Enabled Provisioning.....	6
2.7	Device ID.....	6
2.8	Backward Compatibility.....	6
3	Objects.....	7
3.1	Key Entries.....	7
3.2	PIN and PUK Objects.....	8
3.3	Provisioning Objects.....	8
4	Algorithm Support.....	9
4.1	Mandatory Algorithms.....	9
4.2	Special Algorithms.....	10
4.3	Optional Algorithms.....	10
5	Protection Attributes.....	11
5.1	Export Protection.....	11
5.2	Delete Protection.....	11
5.3	Biometric Protection.....	11
5.4	PIN Input Methods.....	12
5.5	PIN Patterns.....	12
5.6	PIN and PUK Formats.....	12
5.7	PIN Grouping.....	13
5.8	Application Usage.....	13
6	Session Security Mechanisms.....	14
6.1	Encrypted Data.....	14
6.2	MAC Operations.....	14
6.3	Attestations.....	14
6.4	Target Key Reference.....	14
7	Detailed Operation.....	15
7.1	Data Types.....	15
7.2	Return Values.....	16
7.3	Error Codes.....	16
7.4	Method List.....	16
	getDeviceInfo [1].....	17
	createProvisioningSession [2].....	19
	closeProvisioningSession [3].....	25

enumerateProvisioningSessions [4].....	26
abortProvisioningSession [5].....	27
signProvisioningSessionData [6].....	28
updateKeyManagementKey [7].....	29
createPUKPolicy [8].....	30
createPINPolicy [9].....	31
createKeyEntry [10].....	32
getKeyHandle [11].....	36
setCertificatePath [12].....	37
importSymmetricKey [13].....	39
importPrivateKey [14].....	41
addExtension [15].....	42
postDeleteKey [50].....	45
postUnlockKey [51].....	47
postUpdateKey [52].....	48
postCloneKeyProtection [53].....	49
enumerateKeys [70].....	50
getKeyAttributes [71].....	51
getKeyProtectionInfo [72].....	52
getExtension [73].....	54
setProperty [74].....	55
deleteKey [80].....	56
exportKey [81].....	57
unlockKey [82].....	58
changePIN [83].....	59
setPIN [84].....	60
updateFirmware [90].....	61
signHashedData [100].....	62
asymmetricKeyDecrypt [101].....	63
keyAgreement [102].....	64
performHMAC [103].....	65
symmetricKeyEncrypt [104].....	66
Appendix A. KeyGen2 Proxy.....	67
Appendix B. Sample Session.....	68
Appendix C. Reference Implementation.....	68
Appendix D. Remote Key Lookup.....	69
Appendix E. Security Considerations.....	70
Appendix F. Intellectual Property Rights.....	70
Appendix G. References.....	71
Appendix H. Acknowledgments.....	73
Appendix I. Author.....	73

# 1 Introduction

This document describes the API (Application Programming Interface) and architecture of a system called SKS (Secure Key Store). SKS is essentially an enhanced smart card that is optimized for *secure, reliable, and user-friendly on-line provisioning and life-cycle management* of cryptographic keys and associated attributes.

In addition to PKI and symmetric keys (including OTP applications), SKS also supports recent additions to the credential family tree like [Information Cards](#).

The primary objective with SKS and the related specifications is *establishing two-factor authentication as a viable alternative for any provider* by making the scheme a standard feature in the “Universal Client”, the Internet browser.

An equally important means for reaching this undeniable bold goal, is that the API and protocols mandate full “on-the-wire” compliance in order to eliminate the current “Smart Card Middleware Hell”; *a single driver per platform should suffice*.

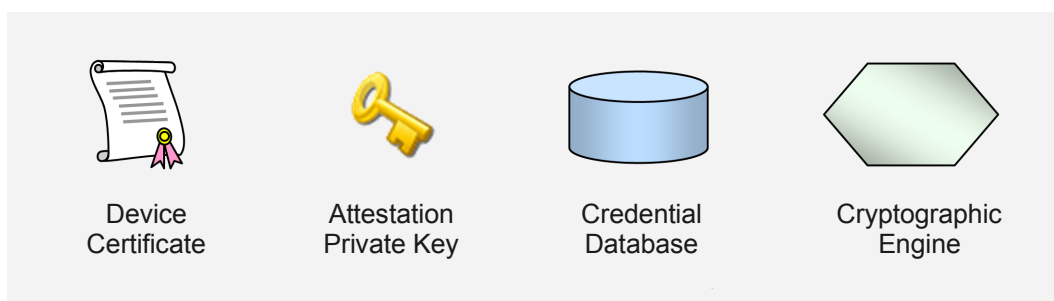
Could *existing* smart card users also benefit from an upgraded token technology? Yes, the new ways of working, like *virtual organizations*, doesn't make the current distribution scheme “Come and get your card” particularly useful.

For maintaining a link to the world of legacy authentication an SKS may also serve as a “Password Vault”.

## 2 Core Functionality

### 2.1 Architecture

Below is a picture showing the core components in the SKS architecture:



The *Device Certificate* forms together with a matching *Attestation Private Key* the foundation for the session mechanism that facilitates secure provisioning of keys, also when the provisioning middleware and network are non-secure.

The *Credential Database* holds keys and other data that is related to keys such as protection and extension objects. It also keeps the provisioning state.

The *Cryptographic Engine* performs in addition to standard cryptographic operations on private and secret keys, the core of the provisioning operations which from an API point-of-view are considerably more complex than the former.

A vital part of the *Cryptographic Engine* is a high quality random number generator since the integrity of the entire provisioning scheme is relying on this.

All operations inside of an SKS are supposed to be protected from tampering by malicious external entities but the degree of *internal* protection may vary depending on the environment that the SKS is running in. That is, an SKS housed in a smart card which may be inserted in an arbitrary computer must keep all data within its protected memory, while an SKS that is an integral part of a mobile phone processor *may* store credential data in the same external Flash memory where programs are stored, but sealed by a CPU-resident “Master Key”.

### 2.2 Provisioning API

Although SKS may be regarded as a “component”, it actually comprises of three associated pieces: The [KeyGen2](#) protocol, the SKS architecture, and the provisioning API described in this document. These items are *tightly matched* which is more or less a prerequisite for *large-scale, secure and interoperable* ecosystems of cryptographic keys. Also see [KeyGen2 Proxy](#).

One of the core features of the SKS Provisioning API is enabling independent issuers securely *sharing* a single “Key Ring”. The rationale for this is mainly to support mobile phones with embedded “Trusted Hardware”, but it appears that the already quite popular USB memory sticks augmented with SKS functionality would be a realistic product offering if they could deal with a potentially large chunk of a consumer's authentication hassles on the Internet.

## 2.3 User API

In this document “User API” refers to operations that are required by security applications like [TLS](#) client-certificate authentication, [S/MIME](#), and [Kerberos](#) (PKINIT).

The User API is not a core SKS facility but its implementation is anyway **recommended**, particularly for SKSes that are featured in “connected” containers such as smart cards since smart card middleware has proved to be a major stumbling block for wide-spread adoption of PKI cards for consumers.

The described User API is fully mappable to the subset of [CryptoAPI](#), [PKCS #11](#), and [JCE](#) that the majority of current PKI-using applications rely on.

The standard User API does not utilize authenticated sessions like featured in [TPM 1.2](#) because this is a *local security option*, which is independent of the *network centric* [Provisioning API](#).

If another User API is used the only requirement is that the key objects created by the provisioning API, are compatible with the former.

## 2.4 Security Model

Since the primary target for SKS is authentication to arbitrary service providers on the Internet, the security model is quite different to traditional multi-application card schemes like [GlobalPlatform](#). In practical terms this means that it is the *user* who grants an issuer the right to create keys in the SKS. That is, there are no preconfigured “Security Domains”.

However, an issuer may during a provisioning session define a VSD (Virtual Security Domain) which enables *post provisioning (update) operations* by the issuer, while cryptographically shielding provisioned data from similar actions by *other* issuers.

When using [KeyGen2](#) the grant operation is performed through a GUI dialog triggered by an issuer request, which in turn is the result of the user browsing to an issuer-related web address.

The SKS itself only trusts inbound data that can securely be derived from a session key created in the initial phase of a provisioning session. See [createProvisioningSession](#).

The session key scheme is conceptually similar to [GlobalPlatform](#)'s SCP (Secure Channel Protocol) but details differ because [KeyGen2](#) uses an on-the-wire JSON format requiring encoding/decoding by the middleware, rather than raw APDUs.

Regarding who trusts an SKS, this is effectively up to each issuer to decide and may be established anytime during an enrollment procedure. Trust in an SKS can be highly granular like only accepting requests from preregistered units or be fully open ended where any SKS compliant device is accepted. A potentially useful issuer policy would be specifying a set of endorsed SKS brands, presumably meeting some generally recognized certification level like EAL5.

Many smart card schemes depend on roles like SO (Security Officer) which squarely matches scenarios where users are associated with a *multitude of independent service providers*. By building on an E2ES (End To End Security) model, the *technical* part of the SO role, exclusively becomes an affair between the SKS and the *remote* issuers, *where each issuer is confined to their own virtual cards and SO policies*.

Also see [Security Considerations](#) and [Privacy Enabled Provisioning](#).

## 2.5 Transaction Based Operation

An important characteristic for maintaining integrity and robustness is that provisioning and management operations either succeed or leave the system intact. This is accomplished by *deferring* the actual “commit” of container-modifying operations until the terminating [closeProvisioningSession](#) call.

Ideally an SKS container should be able dealing with power-failures regardless when they occur.

## 2.6 Privacy Enabled Provisioning

Note: Credential *provisioning* and credential *usage* (at least when the issuer is independent of the relying party), *represent two entirely different scenarios from a privacy point of view*.

Although a one-size-fits-all approach would be nice, it seems that the span of Internet-related services motivates a design that supports on-line identity schemes where issuers have (often quite substantial) knowledge about users, as well as close to fully anonymous relationships.

The “Standard” E2ES (End To End Security) mode which exploits the SKS [Device Certificate](#) and [Attestation Private Key](#) in the provisioning API, is intended to suit the needs of banks, employers, governments, and high-security third-party identity providers.

The PEP (Privacy Enabled Provisioning) mode is identical to the E2ES mode, with the exception that the identity of the SKS is excluded. A valid question is if the PEP mode is equally secure as the E2ES mode. The simple answer to that is a clear “No”, since the issuer neither learns the type (=quality, brand), nor the identity of the SKS.

However, from a *user's horizon* the PEP mode is as secure and trustworthy as the E2ES mode as long as the client platform is intact and the correct issuer enrollment URL is used. After provisioning there are no security differences whatsoever between the two modes.

From a purely technical perspective, [Blind Signatures](#) or elaborate schemes like TCG's [DAA](#) (Direct Anonymous Attestation) could also have been applied. Adoption considerations for a mode primarily intended replacing passwords were governing the decision keeping things simple.

The PEP mode is selected by the [PrivacyEnabled](#) parameter of [createProvisioningSession](#).

Due to the fact that the “Standard” mode potentially affects the user's privacy, it is **recommended** that such requests are equipped with an appropriate user alert notice in the GUI

## 2.7 Device ID

Since the exposed identity of the SKS container is dependent on the mode as described in the previous section, the affected provisioning methods refer to a “Device ID” which is the literal string “**Anonymous**” or the [X.509](#) DER format of the [Device Certificate](#) for the [Privacy Enabled Provisioning](#) and [E2ES](#) mode respectively.

## 2.8 Backward Compatibility

A question that arises is of course how compatible the SKS [Provisioning API](#) is with respect to existing protocols, APIs, and smart cards. The answer is simply: NOT AT ALL due to the fact that current schemes do *generally* not support secure on-line provisioning and key life-cycle management directly towards end-users.

In fact, *smart cards are almost exclusively personalized by more or less proprietary software under the supervision of card administrators or performed in automated production facilities*. It is evident that (at least) mobile phones need a scheme that is more consistent with the on-line paradigm since SIM-cards due to operator-bindings do not scale particularly well.

*“On the Internet anybody can be an operator of something”*

Note: unlike 7816-compatible smart cards, an SKS exposes no visible file system, only objects.

Although the lack of compatibility with the current state-of-the-art (“nothing”), may be regarded as a major short-coming, the good news is that SKS by separating key provisioning from actual usage, *does neither require applications nor cryptographic APIs to be rewritten*.

# 3 Objects

The SKS API (as well as its companion protocol [KeyGen2](#)), assumes that objects are arranged in a specific fashion in order to work. At the heart of the system there are the typical cryptographic keys intended for user authentication, signing etc., but also dedicated keys supporting life-cycle management and of user keys and attributes.

All provisioned user keys, including symmetric dittos (see [importSymmetricKey](#)), are identified by [X.509](#) certificates. The reason for this somewhat unusual arrangement is that this enables *universal key IDs* as well as *secure remote object management by independent issuers*. See [Remote Key Lookup](#).

## 3.1 Key Entries

The following picture shows the elements forming an SKS key entry:



Element	Description
Public Key	Public part of the asymmetric key-pair created by <a href="#">createKeyEntry</a>
Private Key	Private part of the asymmetric key-pair created by <a href="#">createKeyEntry</a>
End-Entity Certificate	<a href="#">X.509</a> certificate set by the <i>mandatory</i> call to <a href="#">setCertificatePath</a>
Symmetric Key	<i>Optional</i> symmetric key defined by calling <a href="#">importSymmetricKey</a>
CA Certificates	<i>Optional</i> <a href="#">X.509</a> CA certificates defined during the call to <a href="#">setCertificatePath</a>
Extension Objects	<i>Optional</i> extension objects defined by calling <a href="#">addExtension</a>
PIN Error Count	<i>Optional</i> counter for keys protected by a PIN policy object. See <a href="#">createPINPolicy</a>
Key Attributes	Attributes defined during the call to <a href="#">createKeyEntry</a>

Note that key management operations always involve an entire key entry; *individual elements cannot be managed*.

## 3.2 PIN and PUK Objects

Keys can *optionally* be protected by PIN-codes (“passphrases”). PIN-protected keys maintain separate PIN error counters, but a single PIN policy object may govern multiple keys. A PIN policy and its associated keys can in turn be supplemented by an optional PUK (PIN Unlock Key) policy object that can be used to reset error-counters that have passed the limit as defined by the PIN policy. Below is an illustration of the SKS protection object hierarchy:



For the creation of protection objects, see [createPUKPolicy](#), [createPINPolicy](#) and [createKeyEntry](#).

For an example how [KeyGen2](#) deals with this structure, see [KeyCreationRequest](#).

Note that the set of keys bound to a particular PIN policy object “owns” the PIN policy object which means that when the *last* key of such a set has been deleted, the PIN policy object itself **must** be *automatically* deleted (by [postDeleteKey](#) and [deleteKey](#)). The very same principle is also valid for PUK policy objects. Due to this there are no specific PIN or PUK delete methods.

An *embedded* SKS **may** also support a device (system-wide) PIN and PUK. See [getDeviceInfo](#). *Usage and management of device PINs and PUKs is out of scope for the SKS API.*

## 3.3 Provisioning Objects

The following picture shows how provisioning objects “own” the keys they have provisioned:



For detailed information concerning the contents of a provisioning object see [createProvisioningSession](#).

Note that when the *last* key owned by a provisioning object has been deleted, the provisioning object itself **must** be *automatically* deleted (by [closeProvisioningSession](#) and [deleteKey](#)).

If a [KeyManagementKey](#) is deployed during provisioning object creation (establishing a [VSD](#)), *post-provisioning operations* can also be performed. See [postDeleteKey](#), [postUnlockKey](#), [postUpdateKey](#), and [postCloneKeyProtection](#). Also see [updateKeyManagementKey](#).



## 4 Algorithm Support

### 4.1 Mandatory Algorithms

Algorithm support in SKS **must** as a *minimum* include the following items:

URI	Description		
Symmetric Key Encryption			
http://www.w3.org/2001/04/xmlenc#aes128-cbc	See <a href="#">XML Encryption</a> . Note that IV <b>must</b> be <i>internally generated</i> as well as <i>prepended</i> to encrypted data		
http://www.w3.org/2001/04/xmlenc#aes192-cbc			
http://www.w3.org/2001/04/xmlenc#aes256-cbc			
http://xmlns.webpki.org/sks/algorithm#aes.cbc.pkcs5	See <a href="#">FIPS 197</a> . Support for 128, 192, and 256-bit keys		
http://xmlns.webpki.org/sks/algorithm#aes.ecb.nopad			
HMAC Operations			
http://www.w3.org/2000/09/xmlsig#hmac-sha1	See <a href="#">HMAC-SHA1</a>		
http://www.w3.org/2001/04/xmlsig-more#hmac-sha256	See <a href="#">HMAC-SHA256</a>		
Asymmetric Key Encryption			
http://xmlns.webpki.org/sks/algorithm#rsa.pkcs1_5	See <a href="#">RFC 3447</a>	<i>Decryption mode only</i>	
http://xmlns.webpki.org/sks/algorithm#rsa.oaep.sha1.mgf1p	MGF1: hash function = mgf1 function. No explicit argument		
http://xmlns.webpki.org/sks/algorithm#rsa.oaep.sha256.mgf1p			
http://xmlns.webpki.org/sks/algorithm#rsa.raw	Non-padded RSA operation		
Diffie-Hellman Key Agreement			
http://xmlns.webpki.org/sks/algorithm#ecdh.raw	See <a href="#">SP800-56A</a> ECC CDH primitive (Section 5.7.1.2)		
Asymmetric Key Signatures			
http://www.w3.org/2000/09/xmlsig#rsa-sha1	See <a href="#">XML Signature</a>	<i>Signing mode only</i>	
http://www.w3.org/2001/04/xmlsig-more#rsa-sha256			
http://www.w3.org/2001/04/xmlsig-more#ecdsa-sha256			
http://xmlns.webpki.org/sks/algorithm#rsa.pkcs1.none	See <a href="#">signHashedData</a>		
http://xmlns.webpki.org/sks/algorithm#ecdsa.none			
Asymmetric Key Generation			
http://xmlns.webpki.org/sks/algorithm#rsa1024	RSA 1024-bit key	<i>Implicit exponent: 65537</i>	
http://xmlns.webpki.org/sks/algorithm#rsa2048	RSA 2048-bit key		
http://xmlns.webpki.org/sks/algorithm#ec.nist.p256	EC NIST “P-256”	See <a href="#">FIPS 186-3</a>	
http://xmlns.webpki.org/sks/algorithm#ec.brainpool.p256r1	EC Brainpool “P256r1”	See <a href="#">RFC 5639</a>	

Supported algorithms can be acquired by calling [getDeviceInfo](#).

Note: RSA “multi-prime” keys are *not* supported by this specification.

## 4.2 Special Algorithms

Special algorithms are unique to SKS:

Special Algorithms	
<a href="http://xmlns.webpki.org/sks/algorithm#session.1">http://xmlns.webpki.org/sks/algorithm#session.1</a>	See <a href="#">createProvisioningSession</a>
<a href="http://xmlns.webpki.org/sks/algorithm#key.1">http://xmlns.webpki.org/sks/algorithm#key.1</a>	See <a href="#">createKeyEntry</a>
<a href="http://xmlns.webpki.org/sks/algorithm#none">http://xmlns.webpki.org/sks/algorithm#none</a>	See <a href="#">createKeyEntry</a> and <a href="#">importSymmetricKey</a>

## 4.3 Optional Algorithms

The following algorithms are defined but are *optional*:

Symmetric Key Encryption	
TBD	TBD

HMAC Operations	
<a href="http://www.w3.org/2001/04/xmldsig-more#hmac-sha384">http://www.w3.org/2001/04/xmldsig-more#hmac-sha384</a>	See <a href="#">XML Signature</a>
<a href="http://www.w3.org/2001/04/xmldsig-more#hmac-sha512">http://www.w3.org/2001/04/xmldsig-more#hmac-sha512</a>	

Asymmetric Key Encryption		
TBD	TBD	<i>Decryption mode only</i>

Diffie-Hellman Key Agreement	
TBD	TBD

Asymmetric Key Signatures		
<a href="http://www.w3.org/2001/04/xmldsig-more#rsa-sha384">http://www.w3.org/2001/04/xmldsig-more#rsa-sha384</a>	See <a href="#">XML Signature</a>	<i>Signing mode only</i>
<a href="http://www.w3.org/2001/04/xmldsig-more#rsa-sha512">http://www.w3.org/2001/04/xmldsig-more#rsa-sha512</a>		
<a href="http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha1">http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha1</a>		
<a href="http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha384">http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha384</a>		
<a href="http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha512">http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha512</a>		

Asymmetric Key Generation		
<a href="http://xmlns.webpki.org/sks/algorithm#rsa3072">http://xmlns.webpki.org/sks/algorithm#rsa3072</a>	RSA 3072-bit key	<i>Implicit exponent: 65537</i>
<a href="http://xmlns.webpki.org/sks/algorithm#rsa4096">http://xmlns.webpki.org/sks/algorithm#rsa4096</a>	RSA 4096-bit key	
<a href="http://xmlns.webpki.org/sks/algorithm#rsa1024.exp">http://xmlns.webpki.org/sks/algorithm#rsa1024.exp</a>	RSA 1024-bit key	<i>Variable exponent</i>  See <a href="#">KeyParameters</a>
<a href="http://xmlns.webpki.org/sks/algorithm#rsa2048.exp">http://xmlns.webpki.org/sks/algorithm#rsa2048.exp</a>	RSA 2048-bit key	
<a href="http://xmlns.webpki.org/sks/algorithm#rsa3072.exp">http://xmlns.webpki.org/sks/algorithm#rsa3072.exp</a>	RSA 3072-bit key	
<a href="http://xmlns.webpki.org/sks/algorithm#rsa4096.exp">http://xmlns.webpki.org/sks/algorithm#rsa4096.exp</a>	RSA 4096-bit key	See <a href="#">FIPS 186-3</a>
<a href="http://xmlns.webpki.org/sks/algorithm#ec.nist.p192">http://xmlns.webpki.org/sks/algorithm#ec.nist.p192</a>	EC NIST “P-192”	
<a href="http://xmlns.webpki.org/sks/algorithm#ec.nist.p384">http://xmlns.webpki.org/sks/algorithm#ec.nist.p384</a>	EC NIST “P-384”	
<a href="http://xmlns.webpki.org/sks/algorithm#ec.nist.p521">http://xmlns.webpki.org/sks/algorithm#ec.nist.p521</a>	EC NIST “P-521”	

## 5 Protection Attributes

The following section describes the attributes issuers need to set for defining suitable key protection policies. Also see [getKeyProtectionInfo](#), [KeyManagementKey](#), [DevicePINProtection](#), and [EnablePINCaching](#).

During provisioning of *user-defined PINs*, the provisioning middleware **should** maintain the PIN policy and optionally ask the user to create another PIN if there is a policy mismatch because [createKeyEntry](#) **must** return an error and abort the entire session if fed with incorrect data. Also see [KeyGen2 Proxy](#).

In addition to protection policies, a key **may** also be constrained with respect to algorithm usage. See [EndorsedAlgorithms](#).

### 5.1 Export Protection

The following table illustrates the use of the [ExportProtection](#) attribute:

KeyGen2 Name	Value	Description
<b>none</b>	0x00	No authorization needed for exporting the key
<b>pin</b>	0x01	Correct PIN is required
<b>puk</b>	0x02	Correct PUK is required
<b>non-exportable</b>	0x03	The key <b>must not</b> be exported

Also see [exportKey](#).

### 5.2 Delete Protection

The following table illustrates the use of the [DeleteProtection](#) attribute:

KeyGen2 Name	Value	Description
<b>none</b>	0x00	No delete restrictions apply
<b>pin</b>	0x01	Correct PIN is required
<b>puk</b>	0x02	Correct PUK is required
<b>non-deletable</b>	0x03	The key <b>must not</b> be deleted

Also see [deleteKey](#).

### 5.3 Biometric Protection

An SKS **may** also support using biometric data as an alternative or complement to PINs. See [getDeviceInfo](#). The following table shows the biometric protection options as defined by the [BiometricProtection](#) policy attribute:

KeyGen2 Name	Value	Description
<b>none</b>	0x00	No biometric protection
<b>alternative</b>	0x01	The key may be authorized with a PIN <i>or</i> by biometrics
<b>combined</b>	0x02	The key is protected by a PIN <i>and</i> by biometrics
<b>exclusive</b>	0x03	The key is <i>only</i> protected by biometrics

Note that there is no API support for biometric authentication, such information is typically provided through GPIO (General Purpose Input Output) ports between the biometric sensor and the SKS. The type of biometrics used is outside the scope of SKS and is usually established during enrollment.

The biometric protection option is only intended to be applied to [User API](#) methods like [signHashedData](#).

## 5.4 PIN Input Methods

The [InputMethod](#) policy attribute tells how PINs **should** be inputted to the SKS according to the following table:

KeyGen2 Name	Value	Description
<b>any</b>	0x00	No restrictions
<b>programmatic</b>	0x01	PINs <b>should</b> only be given through the SKS User API
<b>trusted-gui</b>	0x02	Keys <b>should</b> only be used through a trusted GUI that does the actual PIN request and API invocation

Note that this policy attribute requires that the middleware is “cooperative” to be enforced.

## 5.5 PIN Patterns

The [PatternRestrictions](#) policy attribute specifies how PINs **must** be designed according to the following table:

KeyGen2 Name	Value	Description
<b>two-in-a-row</b>	0x01	Flags 1124 as <i>invalid</i>
<b>three-in-a-row</b>	0x02	Flags 1114 as <i>invalid</i>
<b>sequence</b>	0x04	Flags 1234, 9876, etc as <i>invalid</i>
<b>repeated</b>	0x08	All PIN bytes <b>must</b> be <i>unique</i>
<b>missing-group</b>	0x10	The PIN format <b>must</b> be <b>alphanumeric</b> or <b>string</b> and contain a mix of <i>letters</i> and <i>digits</i> . The <b>string</b> format also requires <i>lowercase</i> letters and <i>non-alphanumeric</i> characters. See <a href="#">PIN and PUK Formats</a>

Note that the [PatternRestrictions](#) byte actually holds a *set of bits*. That is, 0x00 means that there are no pattern restrictions, while 0x06 imposes two constraints. Also note that pattern policy checking is supposed to be applied at the *binary* level which has implications for the binary PIN format (see [PIN and PUK Formats](#)).

An alternative for organizations having strict requirements on PIN patterns, it is letting users define PINs during enrollment in a web application and then deploy issuer-set PIN codes during provisioning. See [PINValue](#).

## 5.6 PIN and PUK Formats

PINs and PUKs **must** adhere to one of formats described in the following table:

KeyGen2 Name	Value	Description
<b>numeric</b>	0x00	0 - 9
<b>alphanumeric</b>	0x01	0 - 9, A - Z
<b>string</b>	0x02	Any valid <a href="#">UTF-8 encoded</a> string
<b>binary</b>	0x03	Binary value, typically expressed as hexadecimal data

Note that format specifiers only deal with how PINs and PUKs are treated in GUIs; internally and in the SKS API, key protection data **must** always be handled as *decoded* strings of bytes. A conforming SKS **must** perform syntax validation during [createKeyEntry](#) on **numeric** and **alphanumeric** PIN data. Length of the clear-text binary value **must not** exceed 128 bytes. See **Format** attribute in [createPINPolicy](#) and [createPUKPolicy](#).

## 5.7 PIN Grouping

A PIN policy object may govern multiple keys. The [Grouping](#) policy attribute (which is intimately linked to the [Application Usage](#) scheme), controls how PINs to the different keys relate to each other according to the following table:

KeyGen2 Name	Value	Description
<b>none</b>	0x00	No restrictions
<b>shared</b>	0x01	All keys share the <i>same</i> PIN ( <i>synchronized</i> )
<b>signature+standard</b>	0x02	Keys with <a href="#">AppUsage</a> = <b>signature</b> share a common PIN while all other keys share <i>another</i> PIN ( <i>synchronized</i> )
<b>unique</b>	0x03	All four <a href="#">AppUsage</a> types must have <i>different</i> PINs while keys with the same <a href="#">AppUsage</a> share a common PIN ( <i>synchronized</i> )

Note that keys having a **shared** PIN grouping attribute **must** be treated as having a single virtual PIN error counter, while **signature+standard** implies two separate error counters. “Synchronized” means that a PIN *value* or *status* change **must** propagate to all keys sharing the PIN.

## 5.8 Application Usage

The [AppUsage](#) attribute specifies what *applications* keys are intended for according to the following table:

KeyGen2 Name	Value	Description
<b>signature</b>	0x00	The key <b>should</b> only be used in signature applications like <a href="#">S/MIME</a>
<b>authentication</b>	0x01	The key <b>should</b> only be used in applications like <a href="#">TLS</a> client certificate authentication and login to AD (Active Directory)
<b>encryption</b>	0x02	The key <b>should</b> only be used in encryption applications
<b>universal</b>	0x03	There are no restrictions on key usage

Enforcement of [AppUsage](#) is up to each *application* to perform.

Note that [AppUsage](#) **must not** constrain a key's *internal* use of cryptographic algorithms in any way, because for that purpose there is the [EndorsedAlgorithm](#) mechanism.

Although [AppUsage](#) could be regarded as a duplication of the [X.509](#) key usage and extended key usage attributes the latter have proved hard to use as “filters” to certificate selection GUIs. [AppUsage](#) is also applicable for other credentials like OTPs (One Time Passwords) and [Information Cards](#).

However, an equally important target for [AppUsage](#) is that in conjunction with [PIN Grouping](#) provide the means for aiding users in PIN input GUIs in the case an issuer requires separate PINs for different keys and applications.

The following matrix shows the **recommended** interpretation of PIN GUI “hints”:

PIN Grouping	<b>signature</b>	<b>authentication</b>	<b>encryption</b>	<b>universal</b>
<b>none</b>	PIN	PIN	PIN	PIN
<b>shared</b>	PIN	PIN	PIN	PIN
<b>signature+standard</b>	Signature PIN	PIN	PIN	PIN
<b>unique</b>	Signature PIN	Authentication PIN	Encryption PIN	PIN

For this scheme to work a prerequisite is (of course) that the middleware is specifically adapted for SKS.

## 6 Session Security Mechanisms

After the [SessionKey](#) has been created the actual provisioning methods can be called. Depending on the specific method downloaded data may be confidential or need to be authenticated. For certain operations the SKS needs to prove for the issuer that sent data indeed stems from internal SKS operations which is referred to as attestations.

This section describes the security mechanisms used during a provisioning session. Also see [SessionKeyLimit](#) and [signProvisioningSessionData](#).

Note that all elements featured in the following definitions **must** be supplied “as is” *without* length indicators.

### 6.1 Encrypted Data

During provisioning encrypted data is occasionally exchanged between the issuer and the SKS. The encryption key is created by the following key derivation scheme:

**EncryptionKey** = [HMAC-SHA256](#) ([SessionKey](#), "EncryptionKey")

**EncryptionKey** **must** only be used with the [AES256-CBC](#) algorithm. Note that the IV (Initialization Vector) **must** always be *prepended* to the encrypted data as in [XML Encryption](#).

### 6.2 MAC Operations

In order to verify the integrity of provisioned data, many of the provisioning methods mandate that the data-carrying arguments are included in a MAC (Message Authentication Code) operation as well. MAC operations use the following scheme:

**MAC** = [HMAC-SHA256](#) ([SessionKey](#) || *MethodName* || [MACSequenceCounter](#), *Data*)

*MethodName* is the string literal of the target method like "closeProvisioningSession", while *Data* represents the arguments as specified for the actual method. Note that *individual elements* featured in *Data* **must** use the representation described in [Data Types](#), that is, *include* applicable length-indicators.

After each MAC operation, [MACSequenceCounter](#) **must** be incremented by one. Due the use of a sequence counter, the provisioning system **must** honor the order of objects as defined by the issuer.

### 6.3 Attestations

Attestations created by the SKS are identical to MAC Operations where *MethodName* is set to "DeviceAttestation".

### 6.4 Target Key Reference

In order to perform post provisioning operations the issuer must provide evidence of ownership to keys. *Target Key Reference* denotes a key management authorization signature scheme using the [KeyManagementKey](#) associated with the “owning” provisioning object of the target key (see [Provisioning Objects](#)) according to the following:

**Authorization** = *Sign* ([KeyManagementKey](#)<sub>target</sub>,  
"TargetKeyReference" || [HMAC-SHA256](#) ([SessionKey](#)<sub>current</sub> || [Device ID](#),  
[End-Entity Certificate](#)<sub>target</sub>))

Notes:

- *Sign* **must** use an [PKCS #1](#) RSASSA signature for RSA keys and [ECDSA](#) for EC keys with the *private key* associated with [KeyManagementKey](#), and utilizing [SHA256](#) as hash function
- An SKS **must** verify that the signature validates with respect to the *public key* ([KeyManagementKey](#)) as well as checking that [End-Entity Certificate](#) matches [TargetKeyHandle](#)
- If a [KeyManagementKey](#) is not present in the target key's provisioning object, the key is considered “not updatable” and the provisioning session **must** be aborted
- The provisioning session **must** be aborted if the [PrivacyEnabled](#) flag differs between the original and the updating session.

## 7 Detailed Operation

This chapter describes the SKS API in detail.

### 7.1 Data Types

The table below shows the data types used by the SKS API. Note that multi-byte integers **must** be stored in big-endian fashion whenever they are *serialized* like in [MAC Operations](#). Also see [Method List](#).

Type	Length	Description
byte	1	Unsigned byte (0 - 0xFF)
bool	1	Byte containing 0x01 (true) or 0x00 (false)
short	2	Unsigned two-byte integer (0 - 0xFFFF)
int	4	Unsigned four-byte integer (0 - 0xFFFFFFFF)
byte[]	2 + length	Array of bytes with a leading “short” holding the length of the data
blob	4 + length	Long array of bytes with a leading “int” holding the length of the data
id	2 + length	Special form of byte[] which <b>must</b> contain an 1-32 byte string with a character set restricted to printable ASCII (0x21 - 0x7E)
uri	2 + length	<a href="#">UTF-8</a> encoded <a href="#">URI</a> which <b>must not</b> exceed 1000 bytes
string	2 + length	<a href="#">UTF-8</a> encoded string with arbitrary content

If an array is followed by a number in brackets (byte[32]) it means that the array **must** be exactly of that length.

Variables and literals that represent textual data **must** be [UTF-8](#) encoded and *not* include terminating null characters; they are in this specification considered equivalent to byte[].

Note that length indicators are only applicable to *array objects* when included in [MAC Operations](#), and when they are *serialized*.



## 7.2 Return Values

All methods return a single-byte status code. In case return status is  $\neq 0$  there is an error and any expected succeeding values **must not** be read as they are not supposed to be available. Instead there **must** be a second return value containing a [UTF-8](#) encoded description in *English* to be used for logging and debugging purposes as shown below:

Name	Type	Description
Status	byte	Non-zero (error) value
ErrorMessage	String	A human-readable error-description with length $\leq 2000$ bytes

## 7.3 Error Codes

The following table shows the standard SKS error-codes:

Name	Value	Description
ERROR_AUTHORIZATION	0x01	Non-fatal error returned when there is something wrong with a supplied PIN or PUK code. See <a href="#">getKeyProtectionInfo</a>
ERROR_NOT_ALLOWED	0x02	Operation is not allowed
ERROR_STORAGE	0x03	No persistent storage available for the operation
ERROR_MAC	0x04	MAC does not match supplied data
ERROR_CRYPTO	0x05	Various cryptographic errors
ERROR_NO_SESSION	0x06	Provisioning session not found
ERROR_NO_KEY	0x07	Key not found
ERROR_ALGORITHM	0x08	Unknown or non-matching algorithm
ERROR_OPTION	0x09	Invalid or unsupported option
ERROR_INTERNAL	0x0A	Internal error
ERROR_EXTERNAL	0x0B	External error like communication link failure
ERROR_USER_ABORT	0x0C	User aborted PIN input or similar
ERROR_NOT_AVAILABLE	0x0D	External error when a requested SKS is unavailable

## 7.4 Method List

This section provides a list of the SKS methods. The number in square brackets denotes the *decimal value* used to identify the method in a call. Method calls are formatted as strings of bytes where the first byte holds the method ID and the succeeding bytes the applicable argument data. [User API](#) methods have method IDs  $\geq 100$ .

Note: The described API is adapted for an SKS using low-level byte-streams for communication. However, the SKS design is equally applicable to API schemes using high-level objects and exceptions. The only thing that **must** remain intact are the cryptographic operations including how objects are represented in MACs.

Note that a **KeyHandle** in this specification always refers to a *key entry*. See [Key Entries](#).



# getDeviceInfo [1]

## Input

Name	Type	Description
<i>This method does not have any input arguments</i>		

## Output

Name	Type	Description
<b>Status</b>	byte	See <a href="#">Return Values</a>
<b>APILevel</b>	short	100 (1.00) => Applies to <i>this</i> API specification
<b>DeviceType</b>	byte	Holds basic device data. See <a href="#">DeviceType</a>
<b>UpdateURL</b>	uri	HTTP or HTTPS URL pointing to a firmware update service or a zero length array. See <a href="#">updateFirmware</a>
<b>VendorName</b>	string	String of 1-128 <i>characters</i> holding the name of the vendor
<b>VendorDescription</b>	string	String of 1-1000 <i>characters</i> holding a vendor description of the SKS device
<b>PathLength</b>	short	Non-zero value holding the number of <b>X509Certificate</b> objects
<b>X509Certificate...</b>	byte[]	DER encoded <a href="#">X.509</a> certificate object <i>repeated</i> as defined by <b>PathLength</b>
<b>SupportedAlgorithms</b>	short	Non-zero value holding the number of <b>SupportedAlgorithm</b> objects
<b>SupportedAlgorithm...</b>	uri	Algorithm URI <i>repeated</i> as defined by <b>SupportedAlgorithms</b> . See <a href="#">Algorithm Support</a>
<b>CryptoDataSize</b>	int	Maximum number of bytes in the <b>Data</b> argument of cryptographic methods
<b>ExtensionDataSize</b>	int	Maximum size of <a href="#">ExtensionData</a> objects
<b>DevicePINSupport</b>	bool	True if the SKS supports a device PIN. See <a href="#">createKeyEntry</a>
<b>BiometricSupport</b>	bool	True if the SKS supports biometric authentication options. See <a href="#">Biometric Protection</a>

**getDeviceData** lists the core characteristics of an SKS which is used by provisioning schemes like [KeyGen2](#).

The **X509Certificate** objects **must** form an *ordered* and *contiguous* certificate path so that the *first* object contains the actual SKS [Device Certificate](#). The path does though not have to be complete (include all upper-level CAs).

A compliant SKS **must** support [ExtensionData](#) objects with a size of at least 65536 bytes.

A compliant SKS **must** support a **CryptoDataSize** of at least 16384 bytes.

*Continued on the next page...*

**DeviceType** contains a set of fields according to the following table:

Bit	Value	Label	Description
0-1	0x00	<b>LOCATION_EXTERNAL</b>	Connected device
	0x01	<b>LOCATION_EMBEDDED</b>	Embedded in the client platform
	0x02	<b>LOCATION_SOCKETED</b>	Mounted inside a socket
	0x03	<b>LOCATION_SIM</b>	SIM/USIM card
2-3	0x00	<b>TYPE_SOFTWARE</b>	Software implementation
	0x04	<b>TYPE_HARDWARE</b>	Unqualified hardware implementation
	0x08	<b>TYPE_HSM</b>	Hardware Security Module
	0x0C	<b>TYPE_CPU</b>	Implemented inside of the main CPU
4-7	-	-	-

## createProvisioningSession [2]

### Input

Name	Type	Description
<b>SessionKeyAlgorithm</b>	uri	Session creation algorithm URI. See next page
<b>PrivacyEnabled</b>	bool	If true the PEP ( <a href="#">Privacy Enabled Provisioning</a> ) mode <b>must</b> be honored
<b>ServerSessionID</b>	id	Server-created provisioning ID which <b>should</b> be unique for each session
<b>ServerEphemeralKey</b>	byte[]	Server-created ephemeral ECDH key. See <a href="#">ServerEphemeralKey</a>
<b>IssuerURI</b>	uri	URI associated with the issuer. See <a href="#">IssuerURI</a>
<b>KeyManagementKey</b>	byte[]	Key management key or zero length array. See <a href="#">KeyManagementKey</a>
<b>ClientTime</b>	int	Locally acquired time in UNIX “epoch” format in <i>seconds</i> . See <a href="#">ClientTime</a>
<b>SessionLifeTime</b>	int	Validity of the provisioning session in seconds. See <a href="#">SessionLifeTime</a>
<b>SessionKeyLimit</b>	short	Upper limit of <b>SessionKey</b> operations. See <a href="#">SessionKeyLimit</a>

### Output

Name	Type	Description
<b>Status</b>	byte	See <a href="#">Return Values</a>
<b>ClientSessionID</b>	id	SKS-created provisioning ID which <b>must</b> be unique for each session
<b>ClientEphemeralKey</b>	byte[]	SKS-created ephemeral ECDH key. See <a href="#">ClientEphemeralKey</a>
<b>SessionAttestation</b>	byte[]	Session creation attestation signature
<b>ProvisioningHandle</b>	int	Non-zero local handle to created provisioning session

**createProvisioningSession** establishes a *persistent session key* that is only known by the issuer and the SKS for usage in subsequent provisioning steps. In addition, the SKS is *optionally* authenticated by the issuer.

*Continued on the next page...*

Shown below is the mandatory to support SKS session key creation algorithm:

<http://xmlns.webpki.org/sks/algorithm#session.1>

- Generate a for this SKS *unique* `ClientSessionID`
- Output `ClientSessionID`
- Generate an *ephemeral* ECDH key-pair `EKP` using *the same named curve* as `ServerEphemeralKey`
- Output `ClientEphemeralKey = EKP.PublicKey`
- Apply the [SP800-56A](#) ECC CDH primitive on `EKP.PrivateKey` and `ServerEphemeralKey` creating a shared secret `z`
- Define internal variable: `byte[32] SessionKey`
- Set `SessionKey = HMAC-SHA256 (z, ClientSessionID || // KDF (Key Derivation Function)  
ServerSessionID ||  
IssuerURI ||  
Device ID)`
- Output `SessionAttestation = Sign (AttestationKey, // See remarks  
ClientSessionID ||  
ServerSessionID ||  
IssuerURI ||  
Device ID ||  
SessionKeyAlgorithm ||  
PrivacyEnabled ||  
ServerEphemeralKey ||  
EKP.PublicKey ||  
KeyManagementKey ||  
ClientTime ||  
SessionLifeTime ||  
SessionKeyLimit)`
- Define internal variable: `short MACSequenceCounter` and set it to *zero*
- Store `SessionKey, Algorithm, PrivacyEnabled, MACSequenceCounter, ClientSessionID, ServerSessionID, IssuerURI, KeyManagementKey, ClientTime, SessionLifeTime` and `SessionKeyLimit` in the [Credential Database](#) and return a handle to the database entry in `ProvisioningHandle`
- Output `ProvisioningHandle`

Note that individual elements featured in the *arguments* (e.g. `ClientSessionID`) of the [Sign](#) and HMAC operations **must** be represented as described in [Data Types](#).

Creation of a session key is an *atomic* operation.

Continued on the next page...

## Remarks

If any succeeding operation in the same provisioning session, is regarded as incorrect by the SKS, *the session **must** be terminated and removed from internal storage including all associated data created in the session.*

An SKS **should** only constrain the number of simultaneous sessions due to lack of storage.

A provisioning session **should not** be terminated due to power down of an SKS.

[SessionKeyAlgorithm](#) defines the creation of **SessionKey** but also the integrity, confidentiality, and attestation mechanisms used during the provisioning session. See [Session Security Mechanisms](#).

Using [KeyGen2 IssuerURI](#) is the URL which *invoked* [ProvisioningInitializationRequest](#).

**ServerEphemeralKey** and **ClientEphemeralKey** **must** be in [X.509](#) DER format and **must** match the elliptic curve capabilities given by [getDeviceInfo](#).

In the [E2ES](#) mode the *Sign* function's **AttestationKey** is the [Attestation Private Key](#) (see [Architecture](#)) and **must** use [PKCS #1](#) RSASSA signatures for RSA keys and [ECDSA](#) for EC keys with [SHA256](#) as the hash function. The distinction between RSA and ECDSA keys is performed through the [Device Certificate](#) (see [getDeviceInfo](#)) which in [KeyGen2](#) is supplied as well as a part of the response to the issuer.

In the [Privacy Enabled Provisioning](#) mode the *Sign* function **must** use [HMAC-SHA256](#) with **SessionKey** as the **AttestationKey**.

**ProvisioningHandle** **must** be *static, unique* and never be reused.

The **ClientTime** attribute is gathered by the local provisioning middleware and is typically derived from the operating system clock. When **ClientTime** is transferred through a protocol such as [KeyGen2](#) it **must** always as a *minimum* have seconds resolution otherwise serious interoperability issues will occur. Possible milliseconds **must** though be *truncated* during the HMAC calculation. **ClientTime** **should** be interpreted as a *32-bit unsigned integer* to cope with the Y2038 problem.

It is **recommended** setting **SessionLifeTime** as low as possible to enable efficient automatic “cleanup” of possible aborted provisioning sessions.

The **SessionKeyLimit** attribute **must** be large enough to handle all **SessionKey** related operations required during the rest of the provisioning session, otherwise the session **must** be terminated. See [Session Security Mechanisms](#). Note that methods like [importSymmetricKey](#) and [postDeleteKey](#) actually use *two* **SessionKey** operations.

A **KeyManagementKey** **must** be supplied if provisioned objects should be *updatable in a future session* (see [postDeleteKey](#), [postUnlockKey](#), [postUpdateKey](#), and [postCloneKeyProtection](#)), else this item **must** be a zero-length array.

A **KeyManagementKey** **must** either be an RSA or an [ECDSA](#) public key in [X.509](#) DER format, compatible with the SKS [Algorithm Support](#).

*Continued on the next page...*

When using [KeyGen2](#) the *input* to `createProvisioningSession` is expressed as shown (in the [E2ES](#) mode) below:

```
{
  "@context": "http://xmlns.webpki.org/keygen2/1.0",
  "@qualifier": "ProvisioningInitializationRequest",
  "SessionKeyAlgorithm": "http://xmlns.webpki.org/sks/algorithm#session.1",
  "ServerSessionID": "14153858604BE5OTXkwbax23nslxS3gh",
  "ServerTime": "2013-09-20T12:00:17+02:00",
  "SessionKeyLimit": 50,
  "SessionLifeTime": 10000,
  "SubmitURL": "https://issuer.example.com/provsess",
  "ServerEphemeralKey":
    {
      "PublicKey":
        {
          "EC":
            {
              "NamedCurve": "http://xmlns.webpki.org/sks/algorithm#ec.nist.p256",
              "X": "INxNvAUEE8t7DSQBft93LVSXxKCiVjhbWWfyg023FCk=",
              "Y": "LmTIQxXB3LgZrNLmhOfMaCnDizczC/RfQ6Kx8iNwfFA="
            }
          }
        },
      "KeyManagementKey":
        {
          "PublicKey":
            {
              "RSA":
                {
                  "Modulus": "jvct15zkH0lw2OwFCn ... vPFX7K1GqLdnumNHNrY1YQ==",
                  "Exponent": "AQAB"
                }
            }
          }
        }
    }
}
```

#### Notes:

The [KeyManagementKey](#) object is *optional*. Also see [updateKeyManagementKey](#).

**ServerTime** is simply a reference and possible “sanity control” for the client.

**SubmitURL** holds the web-address where the [ProvisioningInitializationResponse](#) is to be POSTed.

*Continued on the next page...*

When using [KeyGen2](#) the *output* from `createProvisioningSession` is translated as shown in the example below:

```
{
  "@context": "http://xmlns.webpki.org/keygen2/1.0",
  "@qualifier": "ProvisioningInitializationResponse",
  "ServerSessionID": "14153858604BE5OTXkwbax23nslxS3gh",
  "ClientSessionID": "QqTlcUH_Md7_i2dP4S5VKYmmYsbUbzGL",
  "SessionAttestation": "Tgzvnr/k266LMXinVm ... 7pkJnYiplf9xjOuUJD6OYs=",
  "ServerTime": "2013-09-20T12:00:17+02:00",
  "ClientTime": "2013-09-20T12:00:19+02:00",
  "ServerCertificateFingerPrint": "HwKCofkqkTFXRmyyb/CnWhAcTbQF7w8rl1OqCwyM4TM=",
  "ClientEphemeralKey":
    {
      "PublicKey":
        {
          "EC":
            {
              "NamedCurve": "http://xmlns.webpki.org/sks/algorithm#ec.nist.p256",
              "X": "INxNvAUEE8t7DSQBft93LVSXxKCiVjhbWWfyg023FCk=",
              "Y": "LmTIQxXB3LgZrNLmhOfMaCnDizczC/RfQ6Kx8iNwfFA="
            }
        }
    },
  "DeviceCertificate":
    {
      "X509CertificatePath":
        [
          "MIIClzCCAX+gAwIBAgI ... uk9W/uNIHdoyQn19w==",
          "MIIDZjCCAk6gAwIBAgI ... xOmZyH10xvpsnmokg==",
          "MIIDZjCCAk6gAwIBAgI ... ObXiOlNygeKdK+Dw=="
        ]
    },
  "Signature":
    {
      "Algorithm": "http://www.w3.org/2001/04/xmldsig-more#hmac-sha256",
      "KeyInfo":
        {
          "KeyID": "derived-session-key"
        },
      "SignatureValue": "wMC28Biv+QuYSMCB27AUz8hqwyHoqT6lob0Wk0nuRFk="
    }
}
```

#### Notes:

In the [E2ES](#) mode the `DeviceCertificate` path **must** be available for verification of the `SessionAttestation` signature as well as for identification of the SKS container. The `DeviceCertificate` holds the path exhibited by [getDeviceInfo](#).

In the [Privacy Enabled Provisioning](#) mode the `DeviceCertificate` **must not** be emitted.

`ServerTime` **must** contain a verbatim copy of the same attribute received in the [ProvisioningInitializationRequest](#).

`ServerCertificateFingerPrint` which constitutes of a [SHA256](#) over the server's certificate **must** be created for [KeyGen2](#) protocol invocations using HTTPS. Also see [Security Considerations](#).

To also bind *external* (non-SKS) parameters to the response, the entire response **must** be signed by the use of an enveloped `Signature` object based on the [JCS](#) (JSON Clear-text Signature) scheme. The signature operation utilizes a derived version of `SessionKey` indirectly provided through the [signProvisioningSessionData](#) method.

*Continued on the next page...*

On the server side the following steps **should** be performed:

#### Server Response Validation

- Decide if the received **DeviceCertificate** featured in the **ProvisioningInitializationResponse** message is to be accepted/trusted
- Run the the same **SP800-56A** procedure and KDF as for the SKS but now using **ClientEphemeralKey** and the saved private key of **ServerEphemeralKey** to obtain **SessionKey**
- Perform a *Verify* (**Device Certificate**.**PublicKey**,  
    **SessionAttestation**,  
    **ClientSessionID** ||  
    **ServerSessionID** ||  
    **IssuerURI** ||  
    **Device ID** ||  
    **SessionKeyAlgorithm** ||  
    **PrivacyEnabled** ||  
    **ServerEphemeralKey** ||  
    **ClientEphemeralKey** ||  
    **KeyManagementKey** ||  
    **ClientTime** ||  
    **SessionLifeTime** ||  
    **SessionKeyLimit**))
  - // Received
  - // Received (holds a signature)
  - // Received
  - // Saved
  - // Saved
  - // Saved
  - // Saved
  - // Saved
  - // Saved
  - // Saved
  - // Received
  - // Saved
  - // Received
  - // Saved
  - // Saved
- Verify that the received enveloped **Signature** match which in turn also verifies that the **SessionKey** is correctly calculated
- Verify the the *optional* **ServerCertificateFingerPrint** match the server's certificate

If all tests above succeed the issuer server may continue with the actual provisioning process.

Note that in the **Privacy Enabled Provisioning** mode the **DeviceCertificate** does not apply, and the asymmetric key *Verify* operation is replaced by a comparison between **SessionAttestation** and the output from the **HMAC-SHA256**.



## closeProvisioningSession [3]

### Input

Name	Type	Description
<b>ProvisioningHandle</b>	int	Local handle to an <i>open</i> provisioning session
<b>Challenge</b>	byte[]	Server generated 1-32 byte nonce value
<b>MAC</b>	byte[32]	Vouches for the integrity and authenticity of the operation

### Output

Name	Type	Description
<b>Status</b>	byte	See <a href="#">Return Values</a>
<b>CloseAttestation</b>	byte[32]	Session terminate success attestation signature. See <a href="#">Attestations</a>

**closeProvisioningSession** terminates a provisioning session and returns a proof of successful operation to the issuer. However, success status **must** only be returned if *all* of the following conditions are valid:

- There is an open provisioning session associated with **ProvisioningHandle**
- The **MAC** computes correctly using the method described in [MAC Operations](#) where *Data* is arranged as follows:  
**Data** = [ClientSessionID](#) || [ServerSessionID](#) || [IssuerURI](#) || **Challenge**
- All generated keys are fully provisioned which means that matching public key certificates have been deployed and checked regarding disallowed duplicates. See [setCertificatePath](#)
- [EndorsedAlgorithm](#) URIs match the provisioned key material with respect to symmetric or asymmetric operations as well as to length. Asymmetric keys are also tested for RSA and EC algorithm compliance
- There are no unreferenced PIN or PUK policy objects. See [createPUKPolicy](#) and [createPINPolicy](#)
- The post provisioning operations succeed during the final *commit*. See [Transaction Based Operation](#)

If verification is successful, **closeProvisioningSession** **must** also *reassign provisioning session ownership* to the current (closing) session for *all* objects belonging to sessions that have been subject to a post provisioning operation. The original session objects **must** subsequently be deleted since they have no mission anymore. Also see [Provisioning Objects](#).

If verification fails, *all* objects created in the session **must** be deleted and post provisioning operations **must** be rolled back.

When a provisioning session has been successfully closed by this method, it remains stored until all associated keys have been deleted.

*Continued on the next page...*

Using `KeyGen2.closeProvisioningSession` is invoked as the *last step* of `ProvisioningFinalizationRequest` processing, where two outermost-level properties hold the associated **MAC** and **Challenge** attributes:

```
{
  "@context": "http://xmlns.webpki.org/keygen2/1.0",
  "@qualifier": "ProvisioningFinalizationRequest",
  "ServerSessionID": "1417fa0e508YzrfxGeX-w2ByTAKDSy8v",
  "ClientSessionID": "fXQrec8rlgUz5XxQkSZKimbipbb7eM3f",
  "SubmitURL": "http://issuer.example.com/finalize",

  Other Message Payload

  "Challenge": "NajebxXBmgs1oNj81KzrQBNiAMts+I90kCMJ41QdZhl=",
  "MAC": "DVhtwgO7fnasR+gouyiReoFGDH2w4Sj6RWZ9SIWJeDQ="
}
```

The `CloseAttestation` object is created by attesting (see [SessionAttestation](#)) the following *Data*:

`Data = Challenge || ProvisioningHandle.SessionKeyAlgorithm`

Also see [SessionKeyLimit](#).

A *successful* `KeyGen2` response would only contain the following:

```
{
  "@context": "http://xmlns.webpki.org/keygen2/1.0",
  "@qualifier": "ProvisioningFinalizationResponse",
  "ServerSessionID": "1417fa0e508YzrfxGeX-w2ByTAKDSy8v",
  "ClientSessionID": "fXQrec8rlgUz5XxQkSZKimbipbb7eM3f",
  "CloseAttestation": "acpN8bVJwKZJadlaOsZ+b+7Ky2WRoltP9pFXFD3Nrlo="
}
```

## enumerateProvisioningSessions [4]

### Input

Name	Type	Description
<b>ProvisioningHandle</b>	int	Input enumeration handle
<b>ProvisioningState</b>	bool	If true list only <i>open</i> provisioning sessions. If false list only <i>closed</i> dittos

### Output

Name	Type	Description
<b>Status</b>	byte	See <a href="#">Return Values</a>
<b>ProvisioningHandle</b>	int	Output enumeration handle
<i>The following elements <b>must not</b> be present if the returned <b>ProvisioningHandle</b> = 0</i>		
<b>SessionKeyAlgorithm</b>	uri	See <a href="#">createProvisioningSession</a>
<b>PrivacyEnabled</b>	bool	
<b>KeyManagementKey</b>	byte[]	
<b>ClientTime</b>	int	
<b>SessionLifeTime</b>	int	
<b>ServerSessionID</b>	id	
<b>ClientSessionID</b>	id	
<b>IssuerURI</b>	uri	

**enumerateProvisioningSessions** is primarily intended to be used by provisioning middleware for retrieving handles to *open* provisioning sessions in sessions that are interrupted due to a certification process or similar.

In addition, users of portable SKSes (like smart cards), may carry out provisioning steps on *different* computers through this method.

**enumerateProvisioningSessions** is also useful for debugging and for “cleaning-up” after failed provisioning sessions.

The input **ProvisioningHandle** **must** initially be set to 0 to start an enumeration round.

Succeeding calls **must** use the output **ProvisioningHandle** as input to the next call.

When **enumerateProvisioningSessions** returns with a **ProvisioningHandle** = 0 there are no more provisioning objects to read.

## abortProvisioningSession [5]

### Input

Name	Type	Description
<b>ProvisioningHandle</b>	int	Local handle to an <i>open</i> provisioning session

### Output

Name	Type	Description
<b>Status</b>	byte	See <a href="#">Return Values</a>

**abortProvisioningSession** is intended to be used by provisioning middleware if an unrecoverable error occurs in the communication with the issuer, or if a user cancels a session. If there is a matching and still *open* provisioning session, all associated data **must** be removed from the SKS, otherwise an error **must** be returned.

## signProvisioningSessionData [6]

### Input

Name	Type	Description
<b>ProvisioningHandle</b>	int	Local handle to an <i>open</i> provisioning session
<b>Data</b>	byte[]	Data to be signed

### Output

Name	Type	Description
<b>Status</b>	byte	See <a href="#">Return Values</a>
<b>Signature</b>	byte[32]	Signed data

**signProvisioningSessionData** signs *arbitrary data* that is supplied *by the provisioning middleware*.

The purpose of **signProvisioningSessionData** is adding data integrity to provisioning messages from clients to issuers.

The signature scheme is as follows:

**Signature** = HMAC-SHA256 (SessionKey || "ExternalSignature", Data)

Note that **Data** element **must** be used “as is” in the HMAC operation, *excluding* length information, while the derived key **must** use the representation described in [Data Types](#).

A *relying party* **must** distinguish between such signatures and [Attestations](#) since only the latter are actually vouched for by the SKS.

Also see [SessionKeyLimit](#) and [ProvisioningInitializationResponse](#).

# updateKeyManagementKey [7]

## Input

Name	Type	Description
<b>ProvisioningHandle</b>	int	Local handle to an existing ( <i>closed</i> ) provisioning session object holding a <a href="#">KeyManagementKey</a> that needs to be updated to support post-operations using a new <a href="#">KeyManagementKey</a> . See <a href="#">Provisioning Objects</a>
<b>KeyManagementKey</b>	byte[]	The <i>new</i> <a href="#">KeyManagementKey</a>
<b>Authorization</b>	byte[]	Authorization signature performed by the <i>old</i> <a href="#">KeyManagementKey</a>

## Output

Name	Type	Description
<b>Status</b>	byte	See <a href="#">Return Values</a>

**updateKeyManagementKey** associates an existing provisioning session object with an updated **KeyManagementKey**. The update **must** be cryptographically secured by the **Authorization** signature which is created as follows:

$$\text{Authorization} = \text{Sign}(\text{KeyManagementKey}_{\text{existing}}, \text{"RollOverAuthorization"} \parallel \text{KeyManagementKey}_{\text{new}})$$

For details on allowed signature algorithms and data representation, see [Target Key Reference](#).

The operation **must** be aborted if the **Authorization** signature does not verify or if the target provisioning object lacks a **KeyManagementKey**.

Also see [enumerateProvisioningSessions](#).

*Continued on the next page...*

The following request shows how `updateKeyManagementKey` is integrated in `KeyGen2`:

```
{
  "@context": "http://xmlns.webpki.org/keygen2/1.0",
  "@qualifier": "ProvisioningInitializationRequest",
  "SessionKeyAlgorithm": "http://xmlns.webpki.org/sks/algorithm#session.1",
  "ServerSessionID": "14182a80df8_4YcBFZmNkVUnAw9losHa",
  "ServerTime": "2013-10-04T10:49:13+02:00",
  "SubmitURL": "http://issuer.example.com/provsess",
  "SessionKeyLimit": 50,
  "SessionLifeTime": 10000,
  "ServerEphemeralKey":
  {
    "PublicKey":
    {
      "EC":
      {
        "NamedCurve": "http://xmlns.webpki.org/sks/algorithm#ec.nist.p256",
        "X": "chrt0S6C3eLbKzbV4R8n1+kKNKHogqbAi4FH3fsDiaQ=",
        "Y": "WcW6PlkSj3+1GYNu++cdlljTjYtjuhIGEOK6/vv1kTc="
      }
    }
  },
  "KeyManagementKey":
  {
    "PublicKey":
    {
      "EC":
      {
        "NamedCurve": "http://xmlns.webpki.org/sks/algorithm#ec.nist.p256",
        "X": "INxNvAUEE8t7DSQBft93LVsXxKCiVjhbWWfyg023FCk=",
        "Y": "LmTIQxXB3LgZrNLmhOfMaCnDizczC/RfQ6Kx8iNwFFA="
      }
    }
  },
  "UpdatableKeyManagementKeys":
  [[
    {
      "PublicKey":
      {
        "RSA":
        {
          "Modulus": "kCNcOpatALB21jHrPlv1BgXIUIJ . . . pqNo75jsAZlucG9w==",
          "Exponent": "AQAB"
        }
      }
    },
    {
      "Authorization": "Xjzloz0muM8AMjFafySIR . . . 3sLm1Bfkm4XbbdbrvJw=="
    }
  ]]
}
```

`UpdatableKeyManagementKeys` holds an array of old `KeyManagementKeys` which can be upgraded to the heading (*current*) `KeyManagementKey` if a matching key is found through calls to `enumerateProvisioningSessions`.

The `UpdatableKeyManagementKeys` array can in turn (*recursively*) also hold an `UpdatableKeyManagementKeys` array making it possible to have any number of `KeyManagementKey` generations deployed. To make this feasible, updates **must** be performed in *steps*, starting at the oldest level (leaf `UpdatableKeyManagementKeys` array).

`KeyManagementKey` updates **must** be done *before* calling `createProvisioningSession` since open sessions cannot be updated.

## createPUKPolicy [8]

### Input

Name	Type	Description
<b>ProvisioningHandle</b>	int	Local handle to an <i>open</i> provisioning session
<b>ID</b>	id	<i>External name</i> of the PUK policy object. See <a href="#">Object IDs</a>
<b>EncryptedPUK</b>	byte[]	Encrypted PUK value. See <a href="#">Encrypted Data</a>
<b>Format</b>	byte	Format of PUK strings. See <a href="#">PIN and PUK Formats</a>
<b>RetryLimit</b>	short	Value [0..10000] holding the number of incorrect PUK values ( <i>in a sequence</i> ), forcing the PUK object to permanently lock up. A zero value indicates that there is no limit but that the SKS will introduce an <i>internal</i> 1-10 second delay <i>before</i> acting on an unlock operation in order to thwart exhaustive attacks
<b>MAC</b>	byte[32]	Vouches for the integrity and authenticity of the operation

### Output

Name	Type	Description
<b>Status</b>	byte	See <a href="#">Return Values</a>
<b>PUKPolicyHandle</b>	int	Non-zero handle to created PUK policy object

**createPUKPolicy** creates a PUK policy object in the [Credential Database](#) to be referenced by subsequent calls to the [createPINPolicy](#) method.

The **MAC** uses the method described in [MAC Operations](#) where *Data* is arranged as follows:

*Data* = **ID** || **EncryptedPUK** || **Format** || **RetryLimit**

Note that **EncryptedPUK** is MACed in encrypted form and *then* decrypted by the SKS before storing.

The purpose of a PUK is to facilitate a master key for unlocking keys that have locked-up due to faulty PIN entries. See [unlockKey](#).

PUK policy objects are not directly addressable after provisioning; in order to read PUK policy data, you need to use an associated key handle as input. See [getKeyProtectionInfo](#).



# createPINPolicy [9]

## Input

Name	Type	Description
<b>ProvisioningHandle</b>	int	Local handle to an <i>open</i> provisioning session
<b>ID</b>	id	<i>External name</i> of the PIN policy object. See <a href="#">Object IDs</a>
<b>PUKPolicyHandle</b>	int	Handle to a governing PUK policy object or zero
<b>UserDefined</b>	bool	True if PINs belonging to keys governed by the PIN policy are supposed to be set by the user or by the issuer. See <a href="#">PINValue</a>
<b>UserModifiable</b>	bool	True if PINs can be changed by the user after provisioning
<b>Format</b>	byte	Format of PIN strings. See <a href="#">PIN and PUK Formats</a>
<b>RetryLimit</b>	short	Value [1..10000] holding the number of incorrect PIN values ( <i>in a sequence</i> ), forcing a key to lock up
<b>Grouping</b>	byte	See <a href="#">PIN Grouping</a>
<b>PatternRestrictions</b>	byte	See <a href="#">PIN Patterns</a>
<b>MinLength</b>	short	Minimum <i>decoded</i> PIN length in bytes. See <a href="#">PIN and PUK Formats</a>
<b>MaxLength</b>	short	Maximum <i>decoded</i> PIN length in bytes. See <a href="#">PIN and PUK Formats</a>
<b>InputMethod</b>	byte	See <a href="#">PIN Input Methods</a>
<b>MAC</b>	byte[32]	Vouches for the integrity and authenticity of the operation

## Output

Name	Type	Description
<b>Status</b>	byte	See <a href="#">Return Values</a>
<b>PINPolicyHandle</b>	int	Non-zero handle to created PIN policy object

**createPINPolicy** creates a PIN policy object in the [Credential Database](#) to be referenced by subsequent calls to the [createKeyEntry](#) method.

The **MAC** uses the method described in [MAC Operations](#) where *Data* is arranged as follows:

```
Data = ID || PUKReference || UserDefined || UserModifiable || Format || RetryLimit ||  
      Grouping || PatternRestrictions || MinLength || MaxLength || InputMethod
```

*PUKReference* is set to "#N/A" if **PUKPolicyHandle** is zero, else it is set to the **ID** of the referenced PUK policy object.

If **PUKPolicyHandle** is zero no PUK is associated with the PIN policy object.

PIN policy objects are not directly addressable after provisioning; in order to read PIN policy data, you need to use an associated key handle as input. See [getKeyProtectionInfo](#).

# createKeyEntry [10]

## Input

Name	Type	Description
<b>ProvisioningHandle</b>	int	Local handle to an <i>open</i> provisioning session
<b>ID</b>	id	<i>External name</i> of the key. See <a href="#">Object IDs</a>
<b>KeyEntryAlgorithm</b>	uri	Key generation and attestation algorithm URI. See next page
<b>ServerSeed</b>	byte[]	Server input to the random number generation process. See <a href="#">ServerSeed</a>
<b>DevicePINProtection</b>	bool	True if the key is to be protected by a <i>device PIN</i> . See <a href="#">PIN and PUK Objects</a>
<b>PINPolicyHandle</b>	int	Handle to a governing PIN policy object or zero. See <a href="#">createPINPolicy</a>
<b>PINValue</b>	byte[]	See <a href="#">PINValue</a> , <a href="#">PIN Patterns</a> and <a href="#">PIN Grouping</a>
<b>EnablePINCaching</b>	bool	True if middleware <b>may</b> cache PINs for this key. See <a href="#">EnablePINCaching</a>
<b>BiometricProtection</b>	byte	See <a href="#">Biometric Protection</a>
<b>ExportProtection</b>	byte	See <a href="#">Export Protection</a>
<b>DeleteProtection</b>	byte	See <a href="#">Delete Protection</a>
<b>AppUsage</b>	byte	See <a href="#">Application Usage</a>
<b>FriendlyName</b>	string	String of 0-100 <i>characters</i> that will be associated with this key for use in GUIs
<b>KeyAlgorithm</b>	uri	Algorithm of the key to be created. See <a href="#">Asymmetric Key Generation</a>
<b>KeyParameters</b>	byte[]	Optional parameter data needed for some algorithms. See <a href="#">KeyParameters</a>
<b>EndorsedAlgorithms</b>	short	Value [0..255] holding the number of <b>EndorsedAlgorithm</b> URIs
<b>EndorsedAlgorithm...</b>	uri	Endorsed algorithm URI <i>repeated</i> as defined by <b>EndorsedAlgorithms</b>
<b>MAC</b>	byte[32]	Vouches for the integrity and authenticity of the operation

## Output

Name	Type	Description
<b>Status</b>	byte	See <a href="#">Return Values</a>
<b>KeyHandle</b>	int	Non-zero local handle to created key entry
<b>PublicKey</b>	byte[]	Generated public key in <a href="#">X.509</a> DER representation
<b>KeyAttestation</b>	byte[32]	See <a href="#">KeyAttestation</a>

**createKeyEntry** generates an asymmetric key-pair according to the issuer's specification. In addition, **createKeyEntry** creates a *key entry* (see [Key Entries](#)) in the [Credential Database](#) where the key-pair and its protection attributes are stored.

*Continued on the next page...*

The following operations match the mandatory to support key generation and attestation algorithm:

<http://xmlns.webpki.org/sks/algorithm#key.1>

The **MAC** uses the method described in [MAC Operations](#) where *Data* is arranged as follows:

*Data* = ID || KeyEntryAlgorithm || ServerSeed || PINPolicyReference || PINValueReference ||  
EnablePINCaching || BiometricProtection || ExportProtection ||  
DeleteProtection || AppUsage || FriendlyName ||  
KeyAlgorithm || KeyParameters || EndorsedAlgorithm...]

*PINPolicyReference* is set to "#DevicePIN" if *DevicePINProtection* is true, to "#N/A" if *PINPolicyHandle* is zero, else it is set to the ID of the referenced PIN policy object.

*PINValueReference* is set to "#N/A" if *PINPolicyHandle* is zero, or if *DevicePINProtection* is true, or if the PIN is [UserDefined](#), else it is set to the *encrypted PINValue*.

**KeyAttestation** vouches for that generated key-pairs actually reside in the SKS by attesting (see [Attestations](#)) keys according to the following *Data* scheme:

*Data* = ID || PublicKey

#### Remarks

**KeyHandle** **must** be *static, unique and never be reused*. Note that a **KeyHandle** returned by **createKeyEntry** **must not** be featured in [User API](#) operations until the associated provisioning session has been closed (see [closeProvisioningSession](#)).

Object IDs for [createKeyEntry](#), [createPINPolicy](#) and [createPUKPolicy](#) *share a common namespace* but the namespace is entirely local to the *provisioning session*. Although only static identifiers are used in the examples, Object IDs *may be randomized* to increase entropy of [MAC Operations](#).

**ServerSeed** **must** be a 0-64 byte binary string holding a *random number seed*. How **ServerSeed** is applied to the random number generation process is *unspecified*. The only requirement is that it **must not** be able *reducing* the entropy.

For RSA keys with *variable* exponent **KeyParameters** **must** be 1-8 bytes holding a positive big-endian integer, else **KeyParameters** **must** be of zero length.

A non-zero **BiometricProtection** value presumes that the target SKS supports [Biometric Protection](#), otherwise an *error must be* returned. See [getDeviceInfo](#).

**EndorsedAlgorithm** URIs **must** be *sorted in ascending alphabetical order* before calling **createKeyEntry**.

**EndorsedAlgorithm** URIs **must** be checked for compatibility with [Algorithm Support](#).

**EndorsedAlgorithm** compliance **must** be *enforced* by the [User API](#).

**EndorsedAlgorithm** URIs **must not** be checked against actual key material during **createKeyEntry**. This check **must** be *deferred* to [closeProvisioningSession](#).

If no **EndorsedAlgorithm** URIs are specified, *the key is only constrained by the key material*.

With the special algorithm <http://xmlns.webpki.org/sks/algorithm#none> (which is only permitted as a single **EndorsedAlgorithm** item), keys **must** be *disabled* from executing cryptographic operations through the [User API](#).

A set **DevicePINProtection** presumes that the target SKS supports a "device PUK/PIN", otherwise an *error must be* returned. The characteristics of device PINs are out of scope for the SKS specification. See [getDeviceInfo](#).

**DevicePINProtection** **must not** be combined with local PIN policy objects.

**EnablePINCaching** **must** only be used with keys protected by local PIN policy objects having the [InputMethod](#) set to "trusted-gui".

**PINValue** objects **must** be set by the *caller* as illustrated by the following pseudo code:

```
if (PINPolicyHandle == 0) // No PIN or device PIN
{
    PINValue = zero length array;
}
else if (PINPolicyHandle.UsedDefined) // see UserDefined
{
    PINValue = user-defined clear text PIN value; // taken from a local provisioning GUI
}
else
{
    PINValue = encrypted issuer-set PIN value; // see Encrypted Data
}
```

*Continued on the next page...*

The following JSON object shows a typical key generation (initialization) request in [KeyGen2](#):

```
{
  "@context": "http://xmlns.webpki.org/keygen2/1.0",
  "@qualifier": "KeyCreationRequest",
  "KeyEntryAlgorithm": "http://xmlns.webpki.org/sks/algorithm#key.1",
  "ServerSessionID": "1417fa0bedb7rjEFGS-BL3RnJoDyh5UZ",
  "ClientSessionID": "PpZRTVq2wa-TLvsFJE7GZPASEeEqk4Yz",
  "SubmitURL": "http://issuer.example.com/keyinit",
  "PUKPolicySpecifiers":
    [{
      "ID": "PUK.1",
      "RetryLimit": 3,
      "Format": "numeric",
      "EncryptedPUK": "xkELvWmx+nHdemfJltY+KmcArGNTsusM7jATLHKHC5U=",
      "MAC": "oNTuaVBPqgOGJE7xs1tNtICuzviE2wskcoW1kiuZIKg=",
      "PINPolicySpecifiers":
        [{
          "ID": "PIN.1",
          "MinLength": 6,
          "MaxLength": 8,
          "RetryLimit": 3,
          "Grouping": "shared",
          "Format": "numeric",
          "PatternRestrictions": ["three-in-a-row", "sequence"],
          "MAC": "Z3IMErjv6varAj5Ww31AAj8e/0QZjkYgFdtquDSf4G0=",
          "KeyEntrySpecifiers":
            [{
              "ID": "Key.1",
              "AppUsage": "authentication",
              "KeyAlgorithm": "http://xmlns.webpki.org/sks/algorithm#rsa2048",
              "MAC": "ksg1ZwSfGrUjWPWpbK6wrhOKRH7TlwMc/V9N51GhFCc="
            },
            {
              "ID": "Key.2",
              "AppUsage": "signature",
              "KeyAlgorithm": "http://xmlns.webpki.org/sks/algorithm#ec.nist.p256",
              "MAC": "dC++5J1yQ1SnP4WyRQv4sZJG9gPlq29wO4E2nnX5sFk="
            }
          ]
        }
      ]
    }
  ]
}
```

This sequence should be interpreted as a request for an EC key and an RSA key where both keys are protected by a single (shared) *user-defined* (within the specified policy limits) PIN. The PIN is in turn governed by an issuer-defined, *protocol-wise secret* PUK.

Note that the actual linkage of PUK, PIN and key-specifiers is accomplished through *object embedding* in the protocol which the [KeyGen2 Proxy](#) **must** be honoring.

In the sample [KeyGen2](#) *default values* have been utilized which is why there are few *visible* key generation attributes.

*Continued on the next page...*

When using [KeyGen2](#) the *output* from `createKeyEntry` is translated as shown below:

```
{
  "@context": "http://xmlns.webpki.org/keygen2/1.0",
  "@qualifier": "KeyCreationResponse",
  "ServerSessionID": "1417fa0bedb7rjEFGS-BL3RnJoDyh5UZ",
  "ClientSessionID": "PpZRTVq2wa-TLvsFJE7GZPASEeEqk4Yz",
  "GeneratedKeys":
    [{
      "ID": "Key.1",
      "PublicKey":
        {
          "RSA":
            {
              "Modulus": "sol7DCkNaGZtMP8QLMCu . . . TzTPWM6qFKWLzR45+3DWcPw==",
              "Exponent": "AQAB"
            }
        },
      "KeyAttestation": "bYNI0YTCnVXvuNUM1Im/grDC9U2c63nRbqchnpaoUVg="
    },
    {
      "ID": "Key.2",
      "PublicKey":
        {
          "EC":
            {
              "NamedCurve": "http://xmlns.webpki.org/sks/algorithm#ec.nist.p256",
              "X": "nGIEGlaJp0aSJzD3aNsq1QC3CCSGDgPTVG/2pFLQ6w=",
              "Y": "XOa0+BbXVqqcvwBBOMvV1fs5BzbC9rLdBnXigWNy97o="
            }
        },
      "KeyAttestation": "TtScC3wolB/hGt3SmSvpggIB2Z33S87vSI94hCFFsSE="
    }
  ]
}
```

A conforming server **must** after receipt of the response verify that the number and IDs of returned keys match the request. In addition, each returned key **must** be checked for correctness regarding attestation data and that the generated public key actually complies with that of the request.

## getKeyHandle [11]

### Input

Name	Type	Description
<b>ProvisioningHandle</b>	int	Local handle to an <i>open</i> provisioning session
<b>ID</b>	id	See <a href="#">createKeyEntry</a>

### Output

Name	Type	Description
<b>Status</b>	byte	See <a href="#">Return Values</a>
<b>KeyHandle</b>	int	Local handle to a key belonging to an <i>open</i> provisioning session

**getKeyHandle** returns a **KeyHandle** based on the provisioning session specific key ID.

An invalid key **ID** **must** return an error and abort the provisioning session.

## setCertificatePath [12]

### Input

Name	Type	Description
<b>KeyHandle</b>	int	Local handle to a key-pair belonging to an <i>open</i> provisioning session
<b>PathLength</b>	short	Non-zero value holding the number of <b>X509Certificate</b> objects in the call
<b>X509Certificate...</b>	byte[]	DER encoded <a href="#">X.509</a> certificate object <i>repeated</i> as defined by <b>PathLength</b>
<b>MAC</b>	byte[32]	Vouches for the integrity and authenticity of the operation

### Output

Name	Type	Description
<b>Status</b>	byte	See <a href="#">Return Values</a>

**setCertificatePath** attaches an [X.509](#) certificate path to an already created key-pair. See [createKeyEntry](#).

The **X509Certificate** objects **must** form an *ordered* and *contiguous* certificate path so that the *first* object contains the [End-Entity Certificate](#) *usually* holding the public key of the target key-pair. The path does though not have to be complete (include all upper-level CAs). Path validity **should** be verified by the provisioning middleware before calling this method.

Individual **X509Certificate** objects **must not** exceed [CryptoDataSize](#).

Note that an SKS **must not** attempt to verify that the [End-Entity Certificate](#) and **KeyHandle.PublicKey** match because that would disable the [importPrivateKey](#) method. It is the **MAC** operation that is facilitating a cryptographically verifiable binding between the certificate path and the designated key entry.

The **MAC** uses the method described in [MAC Operations](#) where *Data* is arranged as follows:

*Data* = **KeyHandle.PublicKey** || **KeyHandle.ID** || **X509Certificate...**

A compliant SKS **must not** accept multiple key entries being associated by the same [End-Entity Certificate](#) unless the conflicting key is subject to a [postUpdateKey](#) or [postDeleteKey](#) operation.

A compliant SKS **must** verify that the public key of the [End-Entity Certificate](#) matches the [Asymmetric Key Generation](#) capabilities of the SKS.

*Continued on the next page...*



The following [KeyGen2](#) object shows its interaction with `setCertificatePath`:

```
{
  "@context": "http://xmlns.webpki.org/keygen2/1.0",
  "@qualifier": "ProvisioningFinalizationRequest",
  "ServerSessionID": "1417fa0ad90cEhH32g3fqhY_6EbeenIK",
  "ClientSessionID": "jPGg77Uqp_A59u7Yo4laSRBZMxmoeLay",
  "SubmitURL": "http://issuer.example.com/finalize",
  "IssuedCredentials":
    [{
      "ID": "Key.1",
      "X509CertificatePath":
        [
          "MIIDbDCCAISgAwIBAgIGAUF/oLFEMA0GC..S . . . LNTAajQcWBwAmvX5dvlzg==",
          "MIIDYTCCAkmGAwIBAgIGAUGCqAG . . . qqN3fG5GMaTCZNuJfRQJyU="
        ],
      "MAC": "b3hr4Rc6pHo+MuJYGvvAzdV3knV6tVLphdzDUTEfa9w="
    }],
  "Challenge": "DGfjSX3JaLVeWd2Q+PS7pKvKwlbOvlqZR0hlu2GSVIs=",
  "MAC": "6RYr+Lech+bMdtEWJP/cyPNPt0lw/YXVqx3UuCouNE="
}
```

The `x509CertificatePath` array **must** hold a *sorted* certificate path.

The owning `ProvisioningHandle` and local `KeyHandle` can be retrieved by calling [enumerateProvisioningSessions](#) and [getKeyHandle](#) using the `ClientSessionID`, `ServerSessionID` and `ID` attributes respectively.

## importSymmetricKey [13]

### Input

Name	Type	Description
<b>KeyHandle</b>	int	Local handle to a key belonging to an <i>open</i> provisioning session
<b>SymmetricKey</b>	byte[]	Symmetric key encrypted as described in <a href="#">Encrypted Data</a>
<b>MAC</b>	byte[32]	Vouches for the integrity and authenticity of the operation

### Output

Name	Type	Description
<b>Status</b>	byte	See <a href="#">Return Values</a>

**importSymmetricKey** imports and links a symmetric key to an already created key-pair and certificate.

The **MAC** uses the method described in [MAC Operations](#) where *Data* is arranged as follows:

*Data* = [End-Entity Certificate](#) || **SymmetricKey**

Note that **SymmetricKey** objects **must be** MACed in *encrypted form* and *then* decrypted by the SKS before storing.

Symmetric keys **must not** exceed 128 bytes.

With the special [EndorsedAlgorithm](#) `http://xmlns.webpki.org/sks/algorithm#none` arbitrary static shared secrets can be specified. When used together with [exportKey](#), a suitable PIN policy and a [PropertyBags](#) object holding site information, an SKS could then also serve as a *browser password store*.

After **importSymmetricKey** has been called the key entry is marked as “symmetric”. That is, *the private key is disabled* as well as all operations associated with it. See [getKeyAttributes](#).

The [KeyBackup](#).**IMPORTED** flag of the key **must** be set after execution of **importSymmetricKey**.

*Continued on the next page...*

The following [KeyGen2](#) steps show how symmetric keys are provisioned. First the server issues a key-pair request:

```
{
  "@context": "http://xmlns.webpki.org/keygen2/1.0",
  "@qualifier": "KeyCreationRequest",
  "KeyEntryAlgorithm": "http://xmlns.webpki.org/sks/algorithm#key.1",
  "ServerSessionID": "1417fa0c061hwoiSTca_BwhHjI7tm5yj",
  "ClientSessionID": "yCW200bErAF8DFFmzWWOIphYa2GuFHis",
  "SubmitURL": "http://issuer.example.com/keyinit",
  "PINPolicySpecifiers":
    [{
      "ID": "PIN.1",
      "MinLength": 4,
      "MaxLength": 8,
      "RetryLimit": 3,
      "Format": "numeric",
      "MAC": "OvfnCQy7y0v3C234ESYu3KE0iQ1We9JWAipQ+1J0A64=",
      "KeyEntrySpecifiers":
        [{
          "ID": "Key.1",
          "AppUsage": "authentication",
          "KeyAlgorithm": "http://xmlns.webpki.org/sks/algorithm#rsa2048",
          "EndorsedAlgorithms": ["http://www.w3.org/2000/09/xmlsig#hmac-sha1"],
          "MAC": "5s7dC3SX+jZxjPN7Gg3ssvfX+gOYjcsMEWUn8P3dU7g="
        }]
    }]
}
```

The request above is identical to requests for PKI except for the *optional* [EndorsedAlgorithm](#) declaration which in the sample limit symmetric key operations to [HMAC-SHA1](#).

After receiving the request the client generates a compatible key-pair and a response which is *identical* to that of PKI:

```
{
  "@context": "http://xmlns.webpki.org/keygen2/1.0",
  "@qualifier": "KeyCreationResponse",
  "ServerSessionID": "1417fa0c061hwoiSTca_BwhHjI7tm5yj",
  "ClientSessionID": "yCW200bErAF8DFFmzWWOIphYa2GuFHis",
  "GeneratedKeys":
    [{
      "ID": "Key.1",
      "PublicKey":
        {
          "RSA":
            {
              "Modulus": "u6peYjs2LQjo3EiaYK4XlvRdMxLMA7 . . . VCsoAgDVfo8vf3RNmWH53Fw==",
              "Exponent": "AQAB"
            }
        }
      },
      "KeyAttestation": "grWmZzeyah1OjlvT8KJ3+hOZHx599fnKH4RtbEysiKI="
    }]
}
```

*Continued on the next page...*

The server then responds with a PKI-compliant certified public key including an encrypted “piggybacked” symmetric key:

```
{
  "@context": "http://xmlns.webpki.org/keygen2/1.0",
  "@qualifier": "ProvisioningFinalizationRequest",
  "ServerSessionID": "1417fa0c061hwoiSTca_BwhHjI7tm5yj",
  "ClientSessionID": "yCW200bErAF8DFFmzWWOIphYa2GuFHis",
  "SubmitURL": "http://issuer.example.com/finalize",
  "IssuedCredentials":
    [{
      "ID": "Key.1",
      "X509CertificatePath":
        [
          "MIIDFjCCAf6gAwIBAgI GAUF/oMFSMA0G . . . EJwsqSLO88IVL5jpwW036AVtW3BhILP/Q="
        ],
      "MAC": "go5cioJmIzyNROKfrA0jGZEmoq/6w15YeLdz8QYq8ns=",
      "ImportKey":
        {
          "SymmetricKey": "oh1J/luDY0jfQYVokvhRvSMw3nfOxiGAVu/x9qAg3RJtwt6uhLtNNmukVb4gqx6a",
          "MAC": "y0T2uVwaJrUQVPna9CtpgdNxzPdvjRYr//dx8uaDyTc="
        }
    }],
  "Challenge": "R7sXoLU2vYoETzmeO6cTNiWJADILyUso+2dZhzhgDBM=",
  "MAC": "Ks9BCNsBQ407Bv1wa4pAx7WqWXeyttbLEyzARZ7sOH4="
}
```

For details on how to map keys and sessions, see [setCertificatePath](#).

Note that the [X.509](#) certificate serves as a universal key ID. That is, *SKS/KeyGen2 treats asymmetric and symmetric keys close to identically for provisioning, management and user-selection operations*

## importPrivateKey [14]

### Input

Name	Type	Description
<b>KeyHandle</b>	int	Local handle to a key belonging to an <i>open</i> provisioning session
<b>PrivateKey</b>	byte[]	Private key in <a href="#">PKCS #8</a> format wrapped as described in <a href="#">Encrypted Data</a>
<b>MAC</b>	byte[32]	Vouches for the integrity and authenticity of the operation

### Output

Name	Type	Description
<b>Status</b>	byte	See <a href="#">Return Values</a>

**importPrivateKey** replaces a generated private key with a key supplied by the issuer.

The purpose of **importPrivateKey** (preceded by [setCertificatePath](#)), is to install a certificate and private key that the issuer have generated or have a backup of.

The **MAC** uses the method described in [MAC Operations](#) where *Data* is arranged as follows:

*Data* = [End-Entity Certificate](#) || **PrivateKey**

Note that **PrivateKey** objects **must** be MACed in *encrypted form* and *then* decrypted by the SKS before storing.

A compliant SKS **must** verify that the imported private key matches the [Asymmetric Key Generation](#) capabilities of the SKS.

The [KeyBackup](#) . **IMPORTED** flag of the key **must** be set after execution of **importPrivateKey**.

If **importPrivateKey** is executed over a networked protocol such as [KeyGen2](#) (rather than locally), it is **recommended** alerting the user unless the key is having [AppUsage](#) = **encryption**

*Continued on the next page...*

The following [KeyGen2](#) object shows how a `PrivateKey` is “piggybacked” to a credential to be restored:

```
{
  "@context": "http://xmlns.webpki.org/keygen2/1.0",
  "@qualifier": "ProvisioningFinalizationRequest",
  "ServerSessionID": "1417fa0dcd8PY8_OldKNfCrGh-PPdsXG",
  "ClientSessionID": "m5BeY94pU9hqB0h_MgQl69ITlYD06eRg",
  "SubmitURL": "http://issuer.example.com/finalize",
  "IssuedCredentials":
    [{
      "ID": "Key.1",
      "X509CertificatePath":
        [
          "MIIc5DCCAcygAwIBAgI GAUF/oN3/MA0G . . . T71wQ5pkQ67eZwqcfGjwmS9H0vVU"
        ],
      "MAC": "vg5TluFnxyqyVILcEqwRdjA/y/eBOh+s1R3hkQ5/mE8=",
      "ImportKey":
        {
          "PrivateKey": "uyplo2qEvSzxjkkjtygEhM3e3o . . . clfyK9jyvvhDpUuxKO1PRXR44maaU=",
          "MAC": "+iu+iiigjqZAYQRvYA0oq3aN/r87SVzImD3HQwlB0/el="
        }
    }],
  "Challenge": "nUEdz6aKN5e8ggLmlp631Lr1gizXe57kE0MM2H05XEE=",
  "MAC": "l1KxKKns4+9GUnKp6pcTYdK6YxLFncHsSKY7D9cnb2U="
}
```

For details on how to map keys and sessions, see [setCertificatePath](#).

## addExtension [15]

### Input

Name	Type	Description
<b>KeyHandle</b>	int	Local handle to a key belonging to an <i>open</i> provisioning session
<b>Type</b>	uri	Type URI. Holds a unique name identifying the extension type
<b>SubType</b>	byte	See table below
<b>Qualifier</b>	string	See table below
<b>ExtensionData</b>	blob	Extension object. Regarding size constraints see <a href="#">getDeviceInfo</a>
<b>MAC</b>	byte[32]	Vouches for the integrity and authenticity of the operation

### Output

Name	Type	Description
<b>Status</b>	byte	See <a href="#">Return Values</a>

**addExtension** adds attribute (extension) data to an already created key-pair and certificate.

The **MAC** uses the method described in [MAC Operations](#) where *Data* is arranged as follows:

*Data* = [End-Entity Certificate](#) || **Type** || **SubType** || **Qualifier** || **ExtensionData**

The following table shows **SubType**, **Qualifier** and **ExtensionData** mapping using [KeyGen2](#):

Property Name (Array of)	SubType (Implicit)	Qualifier	ExtensionData
<b>Extensions</b>	0x00	N/A	Binary data extracted from <a href="#">Base64</a> encoded strings
<b>EncryptedExtensions</b>	0x01	N/A	Encrypted binary data extracted from <a href="#">Base64</a> encoded strings
<b>PropertyBags</b>	0x02	N/A	See <a href="#">PropertyBags</a> canonicalization
<b>Logotypes</b>	0x03	<b>MIMEType</b>	Binary image data extracted from <a href="#">Base64</a> encoded strings

### Remarks

N/A = zero-length string.

Note the handling of the **EncryptedExtension**: **ExtensionData** which is encrypted as described in [Encrypted Data](#) **must** be MACed in *encrypted form* and *then* decrypted by the SKS before storing.

A compliant SKS **must not** allow a given key to be associated with multiple extensions of the same **Type**. *If multiple objects of the same type are needed, you must define a container type holding these.*

**Type** URIs *do not have to be recognized by the SKS*, since they are intended for interpretation by external applications.

Although not a part of the current SKS specification, an extension *could* be created for consumption by the SKS only, like downloaded [JavaCard](#) code. In that case the associated extension **Type** URI **must** be featured in the SKS *supported algorithm list*. See [getDeviceInfo](#) and [getExtension](#).

**Qualifier** strings **must not** exceed 128 bytes.

When extensions are featured through [KeyGen2](#) they **must** be read and applied to SKS by calling **addExtension** in the order specified in the table above.

*Continued on the next page...*

Using [KeyGen2](#) an optional **PropertyBags** array holds typed collections of name-value pairs which are referred to as **Properties**. The following BNF-like definitions outline the syntax:

*Optional Property Bags*

```
"PropertyBags" : [ Typed Properties Collection1-n ]
```

*Typed Properties Collection*

```
{ "Type" : "URI", "Properties" : [ Name-Value Pair1-n ], "MAC" : "MAC" }
```

*Name-Value Pair*

```
{ "Name" : "Name", "Value" : "Value", "Writable" : true | false }
```

Notes:

A **Name** **must not** exceed 255 bytes.

If **Writable** is absent **false** is assumed.

A **Properties** name-value collection **must** be converted to a *binary blob* before storage in SKS and MACing according to the following:

- Each name-value pair is translated into a composite object consisting of the following attributes and transformed representation:

Name	Writable	Value
byte[]	bool	byte[]

See [Data Types](#)

- The resulting objects are *concatenated* in the order they occur in the collection.

Note that there are no delimiters added between attributes or objects. The assembled blob holds the actual [ExtensionData](#).

Enforcement of name uniqueness **may** be delegated to the middleware layer. Also see [setProperty](#).

*Continued on the next page...*



The following [KeyGen2](#) sample shows the **Properties** and **Logotypes** objects added to a symmetric key for usage by a **HOTP** (RFC 4226) application:

```
{
  "@context": "http://xmlns.webpki.org/keygen2/1.0",
  "@qualifier": "ProvisioningFinalizationRequest",
  "ServerSessionID": "14182a7f9f7u8bTUUFaTJVLo29TxtUpG",
  "ClientSessionID": "1SJaeriZ6sdL_PT3a8qcZ66d2gyW0QpU",
  "SubmitURL": "http://issuer.example.com/finalize",
  "IssuedCredentials":
    [{
      "ID": "Key.1",
      "X509CertificatePath":
        [
          "MIIDYDCCAkigAwIBAgIGAUGCp/w4MA0GCS . . BR0UoFDeHc4NH8ZmJgd/dmnyw=="
        ],
      "MAC": "UX1urB8mPPEo5rFwVGL5Sm0zO2zeXnZJtumCSOn7KjU=",
      "ImportKey":
        {
          "SymmetricKey": "Kx6TU7TwRF65a4ufQdz48fmrABt7ZByc6uK6mkoj6HeY9fdU0axZDf06MqHH",
          "MAC": "63iclM4SP393yHTNpYW4sqxy7TPXe96uffH/NzvTvs="
        },
      "PropertyBags":
        [{
          "Type": "urn:ietf:rfc:4226",
          "Properties":
            [{
              "Name": "Counter",
              "Value": "0",
              "Writable": true
            },
            {
              "Name": "Digits",
              "Value": "8"
            }
          ],
          "MAC": "C0bNbjOePsFdYRcvlc3LKISskYKPwW2Ce4ql3egOqhE="
        }],
      "Logotypes":
        [{
          "Type": "http://xmlns.webpki.org/keygen2#logotype.application",
          "MimeType": "image/png",
          "ExtensionData": "P3k0jz0ZilZf9U5Ag1l . . . Mq1mW1XUF/KrhPxs8Aoe3lrrx ==",
          "MAC": "lr70oK0dGBYa9ilSp2QC14V5YznFmfne2o0+5DWHmSo="
        }],
      "Challenge": "OX4VP9NrelBDs4YvF6aBuPUJdUtkqm6G1DMnwKKNZJU=",
      "MAC": "5aS0+MmYweTUAu1dZxYyPZifrZyP9062ELv++labH5Q="
    }
}
```

For **HOTP** the corresponding [KeyCreationRequest](#) operation would preferably include an endorsement algorithm definition as well.

*Continued on the next page...*

Below is a [KeyGen2](#) sample showing an **Extension** object holding a [Base64](#) encoded [Information Card](#):

```
{
  "@context": "http://xmlns.webpki.org/keygen2/1.0",
  "@qualifier": "ProvisioningFinalizationRequest",
  "ServerSessionID": "14182a7f517qhCEyqav1suQZTmKPLF1V",
  "ClientSessionID": "oWPA9nCj1_uWy0Ax41tsIoVDA_L4cAE0",
  "SubmitURL": "http://issuer.example.com/finalize",
  "IssuedCredentials":
    [{
      "ID": "Key.1",
      "X509CertificatePath":
        [
          "MIIcNjCCAYagAwIBAgIGAUGCp/VGMA0 . . . w4q16pugWr7CFW4fu3bP4KI="
        ],
      "MAC": "pr/dgwUNZXBe2v1DKz7m5WUITihosyR2sG/9MKuWuFs=",
      "Extensions":
        [{
          "Type": "http://schemas.xmlsoap.org/ws/2005/05/identity",
          "ExtensionData": "iiBlbmHVy85cZS . . . B4bWxuczd3dy53My5vc",
          "MAC": "dl3/3anZBaPQcW4ZofhTlgO9WRpEF9HbBcmbFwbMYAE="
        }]
    }],
  "Challenge": "0/DxfSgk4uuA3HRBI87zr0RiWQQLLIXeNc+0+ox1VpY=",
  "MAC": "yItV0QfOg+ZjDEz3YvvEjWlbg0t1vjLFYQXGUVmWxjY="
}
```

For details on how to map keys and sessions, see [setCertificatePath](#).

In the Information Card sample the primary authentication key (for authenticating to the IDP), would preferable be the PKI key associated by the issued credential. That is, the issuance of a managed Information Card and its primary key *can be fully synchronized* making both usage and middleware design straightforward.

## postDeleteKey [50]

### Input

Name	Type	Description
<b>ProvisioningHandle</b>	int	Local handle to an <i>open</i> provisioning session
<b>TargetKeyHandle</b>	int	Local handle to the target key
<b>Authorization</b>	byte[]	Key management authorization signature
<b>MAC</b>	byte[32]	Vouches for the integrity and authenticity of the operation

### Output

Name	Type	Description
<b>Status</b>	byte	See <a href="#">Return Values</a>

**postDeleteKey** deletes a key created in an earlier provisioning session.

The **MAC** uses the method described in [MAC Operations](#) where *Data* is arranged as follows:

*Data* = **Authorization**

A conforming SKS **must** abort the provisioning session if **postDeleteKey** is mixed with other post provisioning operations referring to the same **TargetKeyHandle**.

This method is *independent* of [Delete Protection](#) settings.

Note that the *execution* of this method **must** be *deferred* to [closeProvisioningSession](#).

*Continued on the next page...*

The following request shows how `postDeleteKey` operations are integrated in the [KeyGen2](#) protocol:

```
{
  "@context": "http://xmlns.webpki.org/keygen2/1.0",
  "@qualifier": "ProvisioningFinalizationRequest",
  "ServerSessionID": "14186f4ce39zKRAGUE0trW6DrhGgZ58L",
  "ClientSessionID": "cXV1TPgFdmTnvFRXhDX6_6a7FAD9Z8fJ",
  "SubmitURL": "http://issuer.example.com/finalize",

  Other Message Payload

  "DeleteKeys":
  [{
    "FingerPrint": "M/7NT9IYHtcClty2eBqZiddvsoxmQzZ0kzmVcg6IIPs=",
    "ServerSessionID": "14186f4cbd8JwNfYUivrkFyrU5asnmkg",
    "ClientSessionID": "u1tVxuCW-ux2TyZlkkq1Rdq732GbpZiV",
    "Authorization": "LsWkDWhwcmSXVkuoqeNj0mQ+Vdpb . . . bch7Lr5J22rdtciaFRLHGxZxUK6gZhqw==",
    "MAC": "pZb5fXDp0hYVOKVXqzW0oP6g11i6Ckw54Wzz0NRVkJJo="
  }],
  "Challenge": "d8AsJSmNPTGf2iV9Hikl6nVIY8Cqkt+AyCHCTAGOqts=",
  "MAC": "xG5Q9tDNc1V/nO7IQZakQQaAKDL1wdoyP1uoSRBiwp0="
}
```

Before invoking `postDeleteKey` the provisioning middleware needs to perform a number of steps:

1. Find the the *old* provisioning session associated with the `ClientSessionID` and `ServerSessionID` attributes of each `DeleteKeys` element by calling [enumerateProvisioningSessions](#).
2. Find possible keys by calling [enumerateKeys](#) and ignoring all but those belonging to the provisioning session found in step #1.
3. For the set of keys found in step #2 call [getKeyAttributes](#) while looking for a key having an [End-Entity Certificate](#) matching the [SHA256 FingerPrint](#).
4. If step #3 is successful `TargetKeyHandle` is recovered and `postDeleteKey` can be invoked.

If any of these steps fail the provisioning session **must** be aborted. Also see [Remote Key Lookup](#).

# postUnlockKey [51]

## Input

Name	Type	Description	
ProvisioningHandle	int	Local handle to an <i>open</i> provisioning session	
TargetKeyHandle	int	Local handle to the target key	See <a href="#">Target Key Reference</a>
Authorization	byte[]	Key management authorization signature	
MAC	byte[32]	Vouches for the integrity and authenticity of the operation	

## Output

Name	Type	Description
Status	byte	See <a href="#">Return Values</a>

`postUnlockKey` works like `unlockKey` except that authorization is derived from a [Target Key Reference](#) instead of a PUK. The **MAC** uses the method described in [MAC Operations](#) where *Data* is arranged as follows:

*Data* = **Authorization**

If the target key is associated with a PUK object the PUK error count **must** be cleared as well. Note that the *execution* of this method **must** be *deferred* to `closeProvisioningSession`.

The following request shows how `postUnlockKey` operations are integrated in the [KeyGen2](#) protocol:

```
{
  "@context": "http://xmlns.webpki.org/keygen2/1.0",
  "@qualifier": "ProvisioningFinalizationRequest",
  "ServerSessionID": "14186f4d4ccdaW-Z_IHEFW3xVLJ6kpKV",
  "ClientSessionID": "qP5ioSdpeGxnJFmo6rE9G9pAUUfnc1cO",
  "SubmitURL": "http://issuer.example.com/finalize",

  Other Message Payload

  "UnlockKeys":
  [{
    "FingerPrint": "E0zdqsaxi7GOyBQxdaMeOZKKp4Gv90TLfgNwt7Z9Btw=",
    "ServerSessionID": "14186f4d44aEEI_KtcKAnyLQpnVt3dVa",
    "ClientSessionID": "KHdZHnyod54nd9TMixTWDnOtfUVpZW1A",
    "Authorization": "f4xmvt30boYtKpNA4nP . . . rslfnrEen5PJrq0DQPiZNa1Fo8Y6A==",
    "MAC": "nCTL88llkr2a/gHtiUP3yBuDQZ7HB15T5yzixmzBYA="
  }],
  "Challenge": "+EZE7S11okxMhgCNxpZBQ2WCmRPdDMNdjoYnkYmR5M0=",
  "MAC": "AUy8CWloq32diolOhHYGpZNRxWJoN/kZ6G/G7QZSmW4="
}
```

Before invoking `postUnlockKey` the provisioning middleware must perform the same steps as for `postDeleteKey`.

## postUpdateKey [52]

### Input

Name	Type	Description
<b>KeyHandle</b>	int	Local handle to a <i>new</i> key belonging to an <i>open</i> provisioning session
<b>TargetKeyHandle</b>	int	Local handle to the target key
<b>Authorization</b>	byte[]	Key management authorization signature
<b>MAC</b>	byte[32]	Vouches for the integrity and authenticity of the operation

### Output

Name	Type	Description
<b>Status</b>	byte	See <a href="#">Return Values</a>

**postUpdateKey** updates (replaces) a key created in an earlier provisioning session.

The **MAC** uses the method described in [MAC Operations](#) where *Data* is arranged as follows:

*Data* = [End-Entity Certificate](#) || **Authorization**

The new key **must** be *fully provisioned* (fitted with a certificate and optional attributes), *before* this method is called. However, the new key **must not** be PIN-protected since it supposed to *inherit* the old key's PIN protection scheme (if there is one). Inheritance does not mean “copying” but *linking* the new key to an existing PIN object. See [PIN and PUK Objects](#).

The target key and the new key **must** have identical [Application Usage](#).

Note that updating a key involves *all related data* (see [Key Entries](#)), with PIN protection as the only exception.

The **KeyHandle** of the updated key **must** after a successful update be set equal to **TargetKeyHandle**.

A conforming SKS **must** allow a (single) **postUpdateKey** combined with an arbitrary number of [postCloneKeyProtection](#) calls referring to the same **TargetKeyHandle**.

Note that the *execution* of this method **must** be *deferred* to [closeProvisioningSession](#).

*Continued on the next page...*

The following request shows how **postUpdateKey** is integrated in the [KeyGen2](#) protocol:

```
{
  "@context": "http://xmlns.webpki.org/keygen2/1.0",
  "@qualifier": "ProvisioningFinalizationRequest",
  "ServerSessionID": "14186f4c622d2ixzQBPpRoUe9PR7jC3D",
  "ClientSessionID": "YME9J37aH1Xo7tQifFpa9nkiyyMcGESQ",
  "SubmitURL": "http://issuer.example.com/finalize",
  "IssuedCredentials":
    [{
      "ID": "Key.1",
      "X509CertificatePath":
        [
          "MIIDYTCCAkmgAwIBAgIGAUGG9McmMA0GCSq . . . lz9C0sc5Ak1jNYzvd8GpS4X6C6J3Uys="
        ],
      "MAC": "J/RnFJtv7SjP5ZPudqVW6wQnqGmKZ66bWBjQCoESgKk=",
      "UpdateKey":
        {
          "FingerPrint": "PqCoZBJfCvRgikF1oqHa/MOJ/ZTXrIMFn6RvXCgGwps=",
          "ServerSessionID": "14186f4c405V9Z4dm6knbREoEA8EhQV8",
          "ClientSessionID": "ALHIRvpj39AuDCag1qXj8TQOWc9i3Bor",
          "Authorization": "dqJAh+ScttwnPN2Tu3Xy7m4zqmC . . . 0Qe92GoDHR0pes4prWn2rKUrsgw==",
          "MAC": "EZ0L4kaemzFtHSvSIFatYIC9rU4oXVKowQVTuRBMwNA="
        }
    ]},
  "Challenge": "nv1TZ1Z+BZfCjgmLzCZB+y1qSiAM8Ch0P93kPLTpHNQ=",
  "MAC": "Y/luPsb9JncrLKYmeEPKSqwADluXEAy9Yf6oZnDJQU="
}
```

Before invoking **postUpdateKey** the provisioning middleware must perform the same steps as for [postDeleteKey](#).

**KeyHandle** is the handle associated with the issued credential embedding the **UpdateKey** operation.

## postCloneKeyProtection [53]

### Input

Name	Type	Description
<b>KeyHandle</b>	int	Local handle to a <i>new</i> key belonging to an <i>open</i> provisioning session
<b>TargetKeyHandle</b>	int	Local handle to the target key
<b>Authorization</b>	byte[]	Key management authorization signature
<b>MAC</b>	byte[32]	Vouches for the integrity and authenticity of the operation

### Output

Name	Type	Description
<b>Status</b>	byte	See <a href="#">Return Values</a>

**postCloneKeyProtection** clones the *protection scheme* of a key created in an earlier provisioning session and applies it to a newly created key.

The **MAC** uses the method described in [MAC Operations](#) where *Data* is arranged as follows:

*Data* = [End-Entity Certificate](#) || **Authorization**

The new key **must** be *fully provisioned* (fitted with a certificate and optional attributes), *before* this method is called. However, the new key **must not** be PIN-protected since it supposed to *inherit* the old key's PIN protection scheme (if there is one). Inheritance does not mean “copying” but *linking* the new key to an existing PIN object. See [PIN and PUK Objects](#).

An inherited custom PIN protection scheme **must** have its grouping attribute set to **shared** (see [PIN Grouping](#)).

A conforming SKS **must** allow multiple **postCloneKeyProtection** calls referring to the same **TargetKeyHandle**.

Note that the *execution* of this method **must** be *deferred* to [closeProvisioningSession](#).

*Continued on the next page...*



The following request shows how **postCloneKeyProtection** is integrated in the **KeyGen2** protocol:

```
{
  "@context": "http://xmlns.webpki.org/keygen2/1.0",
  "@qualifier": "ProvisioningFinalizationRequest",
  "ServerSessionID": "14186f4c20a3Iy83wJZoJMA3x_hZ2gKo",
  "ClientSessionID": "j3CcN3e8UI5XKN1exKqcF19dBi8eGD78",
  "SubmitURL": "http://issuer.example.com/finalize",
  "IssuedCredentials":
    [{
      "ID": "Key.1",
      "X509CertificatePath":
        [
          "MIIDajCCAIAgAwIBAgIGAUGG9MPKM . . . KUtYzmixtnCrPb6NveG0x9yrothzHd9k="
        ],
      "MAC": "zwGCYuuKoiLR5n/OyufcS1Z9sABX4W4dI2dRmyBd8gE=",
      "CloneKeyProtection":
        {
          "FingerPrint": "cnEQwl7hGtfqNgtXeCqG/dSN1KOkW1amRx2t6RcPQY0=",
          "ServerSessionID": "14186f4bfeeibYVPx01I0VbbqspZ0NAY",
          "ClientSessionID": "uENhOyeLZjhXo9CT5dqdTC0H4LtEEDqm",
          "Authorization": "MEYCIQC5BTwVz8VbrwPo7ujLx . . . HJzsDemjamO6r9yyR15Cw241w",
          "MAC": "yViSzGjqcnVpAvkLzkxs5QwoccX+3lVr3/2lbdWJjOg="
        }
    ]},
  "Challenge": "o3iWxmuLyGNGhMHxEP22At0R5QhvRm2bGK4kzc/btJQ=",
  "MAC": "KGcta9GWH/gCnZzcz/dUwqxt8YVBq2/lwUJEX/dDTxk="
}
```

Before invoking **postCloneKeyProtection** the provisioning middleware must perform the same steps as for **postDeleteKey**.

**KeyHandle** is the handle associated with the issued credential embedding the **CloneKeyProtection** operation.

## enumerateKeys [70]

### Input

Name	Type	Description
<b>KeyHandle</b>	int	Input enumeration handle

### Output

Name	Type	Description
<b>Status</b>	byte	See <a href="#">Return Values</a>
<b>KeyHandle</b>	int	Output enumeration handle
<i>The following element <b>must not</b> be present if the returned <b>KeyHandle</b> = 0</i>		
<b>ProvisioningHandle</b>	int	Handle to the associated provisioning session object

**enumerateKeys** enumerate keys for *closed* provisioning sessions. Closed provisioning session means that the key is ready for usage by *applications*.

The input **KeyHandle** **must** initially be set to 0 to start an enumeration round.

Succeeding calls **must** use the output **KeyHandle** as input to the next call.

When **enumerateKeys** returns with a **KeyHandle** = 0 there are no more key objects to read.

## getKeyAttributes [71]

### Input

Name	Type	Description
<b>KeyHandle</b>	int	Local handle to the target key

### Output

Name	Type	Description
<b>Status</b>	byte	See <a href="#">Return Values</a>
<b>SymmetricKeyLength</b>	short	Length of symmetric key in <i>bytes</i> . If <b>SymmetricKeyLength</b> > 0 the active key is symmetric. See <a href="#">importSymmetricKey</a>
<b>PathLength</b>	short	See <a href="#">setCertificatePath</a>
<b>X509Certificate...</b>	byte[]	
<b>AppUsage</b>	byte	See <a href="#">createKeyEntry</a>
<b>FriendlyName</b>	string	
<b>EndorsedAlgorithms</b>	short	
<b>EndorsedAlgorithm...</b>	uri	
<b>Extensions</b>	short	Number of <b>Type</b> URIs
<b>Type...</b>	uri	Extension <b>Type</b> URI. <i>Repeated</i> object
		See <a href="#">addExtension</a>

**getKeyAttributes** returns attribute data for provisioned keys.

For asymmetric keys the public key of the [End-Entity Certificate](#) signifies RSA or EC algorithm.

Also see [getKeyProtectionInfo](#).

## getKeyProtectionInfo [72]

### Input

Name	Type	Description
<b>KeyHandle</b>	int	Local handle to the target key

### Output

Name	Type	Description
<b>Status</b>	byte	See <a href="#">Return Values</a>
<b>ProtectionStatus</b>	byte	See <a href="#">ProtectionStatus</a> table on the next page
<b>PUKFormat</b>	byte	Copy of <b>Format</b> defined by <a href="#">createPUKPolicy</a> [1]
<b>PUKRetryLimit</b>	short	Copy of <b>RetryLimit</b> defined by <a href="#">createPUKPolicy</a> [1]
<b>PUKErrorCount</b>	short	Current PUK error count for keys protected by a local PUK policy object [1]
<b>UserDefined</b>	bool	Copies of the corresponding <a href="#">createPINPolicy</a> parameters for keys protected by a local PIN policy object [1]
<b>UserModifiable</b>	bool	
<b>Format</b>	byte	
<b>RetryLimit</b>	short	
<b>Grouping</b>	byte	
<b>PatternRestrictions</b>	byte	
<b>MinLength</b>	short	
<b>MaxLength</b>	short	
<b>InputMethod</b>	byte	
<b>PINErrorCount</b>	short	Current PIN error count for keys protected by a local PIN policy object [1] See <a href="#">ProtectionStatus</a> table on the next page
<b>EnablePINCaching</b>	bool	Exact copies of the corresponding <a href="#">createKeyEntry</a> parameters
<b>BiometricProtection</b>	byte	
<b>ExportProtection</b>	byte	
<b>DeleteProtection</b>	byte	
<b>KeyBackup</b>	byte	Tells if there exists a <i>copy</i> of the key. See <a href="#">KeyBackup</a> table on the next page

**getKeyProtectionInfo** returns information about the protection scheme for a key including possible biometric options. In addition, the call retrieves the current protection status for the key.

Note 1: Fields **must** be set to zero if they do not apply to the key in question.

*Continued on the next page...*

The following table illustrates how the **ProtectionStatus** bit field should be interpreted:

Name	Value	Description
<b>PIN_PROTECTED</b>	0x01	The key is protected by a local PIN policy object
<b>PUK_PROTECTED</b>	0x02	The key is protected by a local PUK policy object. This bit <b>must</b> be <i>combined</i> with bit <b>PIN_PROTECTED</b>
<b>PIN_BLOCKED</b>	0x04	The key has locked-up due to PIN errors. This bit <b>must</b> be <i>combined</i> with bit <b>PIN_PROTECTED</b>
<b>PUK_BLOCKED</b>	0x08	The key has locked-up due to PUK errors. This bit <b>must</b> be <i>combined</i> with bit <b>PUK_PROTECTED</b>
<b>DEVICE_PIN</b>	0x10	The key is protected by a device PIN. Information about device PINs is out of scope for the SKS API. This bit <b>must</b> be the only active bit if applicable

If all bits are zero the key is not PIN protected.

The following table illustrates how the **KeyBackup** bit field should be interpreted:

Name	Value	Description
<b>IMPORTED</b>	0x01	The IMPORTED bit <b>must</b> be set if the key has been supplied through <a href="#">importPrivateKey</a> or <a href="#">importSymmetricKey</a>
<b>EXPORTED</b>	0x02	The EXPORTED bit <b>must</b> be set if the key has been subject to an <a href="#">exportKey</a> operation

## getExtension [73]

### Input

Name	Type	Description
<b>KeyHandle</b>	int	Local handle to the target key
<b>Type</b>	uri	Type URI. See <a href="#">addExtension</a>

### Output

Name	Type	Description
<b>Status</b>	byte	See <a href="#">Return Values</a>
<b>SubType</b>	byte	Exact copies of the corresponding <a href="#">addExtension</a> parameters
<b>Qualifier</b>	string	
<b>ExtensionData</b>	blob	

**getExtension** returns a typed extension object associated with a key.

Note that encrypted extensions are decrypted during provisioning.

If the extension is intended to be consumed by the SKS, **ExtensionData** **must** be returned as a zero-length array.

## setProperty [74]

### Input

Name	Type	Description
<b>KeyHandle</b>	int	Local handle to the target key
<b>Type</b>	uri	Type URI which <b>must</b> identify a <b>Properties</b> extension. See <a href="#">addExtension</a>
<b>Name</b>	string	Property name. String of 1-255 <i>characters</i>
<b>Value</b>	string	Property value. Note <a href="#">ExtensionData</a> size limit

### Output

Name	Type	Description
<b>Status</b>	byte	See <a href="#">Return Values</a>

**setProperty** sets a named property value in a **Properties** collection linked to a key.

If the named property does not exist or is not *writable*, an error **must** be returned.

## deleteKey [80]

### Input

Name	Type	Description
<b>KeyHandle</b>	int	Local handle to the target key
<b>Authorization</b>	byte[]	Zero-length array, PIN, or PUK depending on <a href="#">Delete Protection</a>

### Output

Name	Type	Description
<b>Status</b>	byte	See <a href="#">Return Values</a>

**deleteKey** removes a key from the [Credential Database](#).

If the key is the last belonging to a provisioning session, the session data objects are removed as well.

Invalid **Authorization** data to the key **must** return [ERROR\\_AUTHORIZATION](#) status.

A conforming SKS **may** introduce physical presence methods like GPIO-based buttons, *circumventing* [Delete Protection](#) settings.

Regarding delete of PIN and PUK policy objects, see [PIN and PUK Objects](#).



## exportKey [81]

### Input

Name	Type	Description
<b>KeyHandle</b>	int	Local handle to the target key
<b>Authorization</b>	byte[]	Zero-length array, PIN, or PUK depending on <a href="#">Export Protection</a>

### Output

Name	Type	Description
<b>Status</b>	byte	See <a href="#">Return Values</a>
<b>Key</b>	byte[]	Unencrypted key. For type information see <a href="#">getKeyAttributes</a>

**exportKey** exports a private or symmetric key from the [Credential Database](#).

Invalid **Authorization** data to the key **must** return [ERROR\\_AUTHORIZATION](#) status.

Private (asymmetric) keys **must** be exported in [PKCS #8](#) format.

If a **non-exportable** key is referred to, **exportKey** **must** return [ERROR\\_NOT\\_ALLOWED](#) status.

Note that the [KeyBackup](#).**EXPORTED** flag of the key **must** be set after execution of **exportKey**.

## unlockKey [82]

### Input

Name	Type	Description
<b>KeyHandle</b>	int	Local handle to the target key
<b>Authorization</b>	byte[]	PUK

### Output

Name	Type	Description
<b>Status</b>	byte	See <a href="#">Return Values</a>

**unlockKey** re-enables a key that has been locked due to erroneous PIN entries.

Note that this method only applies to keys that are protected by local PIN and PUK policy objects.

Invalid **Authorization** data (PUK) to the key **must** return [ERROR\\_AUTHORIZATION](#) status.

If **unlockKey** succeeds all keys sharing the PIN object will be unlocked. See [PIN Grouping](#).

## changePIN [83]

### Input

Name	Type	Description
<b>KeyHandle</b>	int	Local handle to the target key
<b>Authorization</b>	byte[]	Original PIN
<b>NewPIN</b>	byte[]	The requested new PIN

### Output

Name	Type	Description
<b>Status</b>	byte	See <a href="#">Return Values</a>

**changePIN** modifies a PIN for a key.

Note that the key **must** be protected by a local PIN policy object having the [UserModifiable](#) attribute set.

Invalid **Authorization** data (PIN) to the key **must** return [ERROR\\_AUTHORIZATION](#) status.

If **changePIN** succeeds all keys sharing the PIN object will be updated. See [PIN Grouping](#).

## setPIN [84]

### Input

Name	Type	Description
<b>KeyHandle</b>	int	Local handle to the target key
<b>Authorization</b>	byte[]	PUK string
<b>NewPIN</b>	byte[]	The requested new PIN

### Output

Name	Type	Description
<b>Status</b>	byte	See <a href="#">Return Values</a>

**setPIN** sets a PIN for a key *regardless of PIN block status* since it uses a PUK as authorization.

Note that the key **must** be protected by local PUK and PIN policy objects where the latter have the [UserModifiable](#) attribute set.

Invalid **Authorization** data (PUK) **must** return [ERROR\\_AUTHORIZATION](#) status.

If **setPIN** succeeds all keys sharing the PIN object will be updated and *unlocked*. See [PIN Grouping](#).

## updateFirmware [90]

### Input

Name	Type	Description
<b>Chunk</b>	blob	Firmware code chunk

### Output

Name	Type	Description
<b>Status</b>	byte	See <a href="#">Return Values</a>
<b>NextURL</b>	uri	Next URL or zero-length string

**updateFirmware** is an *optional* method that performs a firmware update operation. The method is only available if the [UpdateURL](#) is non-zero. To perform an update, the SKS management system issues an HTTP GET operation to the service pointed out by [UpdateURL](#). If the service returns a content of zero length, the SKS device is assumed to be up-to-date, else **updateFirmware** should be called with the content in **Chunk**. The return value from the call is either a new URL to be used analogous to [UpdateURL](#), or a zero-length string indicating that the update is ready.

A conforming update service **must** use the MIME-type **application/octet-stream**.

The **updateFirmware** method **must** be implemented in such a way that the SKS container cannot be made inoperable due to network errors or aborted update operations. In addition, the SKS container **must** be able to *securely authenticate* the update service's **Chunk** data

# signHashedData [100]

## Input

Name	Type	Description
<b>KeyHandle</b>	int	Local handle to the target key
<b>Algorithm</b>	uri	Signature algorithm URI. See <a href="#">Asymmetric Key Signatures</a>
<b>Parameters</b>	byte[]	Parameters needed by some signature algorithms
<b>Authorization</b>	byte[]	Holds a PIN or is of zero length if no PIN is supplied
<b>Data</b>	byte[]	Hashed data to be signed. Also see <a href="#">CryptoDataSize</a>

## Output

Name	Type	Description
<b>Status</b>	byte	See <a href="#">Return Values</a>
<b>Result</b>	byte[]	Signed data including algorithm-specific padding

**signHashedData** performs an asymmetric key signature operation on the input **Data** object.

**Data** **must** be hashed *as required by the signature algorithm*.

The **Parameters** object **must** be of zero length for algorithms not needing additional input.

Invalid **Authorization** data (PIN) to the key **must** return [ERROR\\_AUTHORIZATION](#) status.

The length of **Data** **must** match the hash algorithm. Note that signature algorithms that do not define a specific hash algorithm impose no tests on **Data** length. The `http://xmlns.webpki.org/sks/algorithm#rsa.pkcs1.none` signature algorithm **must** format the signature packet according to [PKCS #1](#) but without hash algorithm identifiers:

EMSA = 0x00 || 0x01 || PS || 0x00 || Data

# asymmetricKeyDecrypt [101]

## Input

Name	Type	Description
<b>KeyHandle</b>	int	Local handle to the target key
<b>Algorithm</b>	uri	Encryption algorithm URI. See <a href="#">Asymmetric Key Encryption</a>
<b>Parameters</b>	byte[]	Parameters needed by some encryption algorithms
<b>Authorization</b>	byte[]	Holds a PIN or is of zero length if no PIN is supplied
<b>Data</b>	byte[]	Encrypted data

## Output

Name	Type	Description
<b>Status</b>	byte	See <a href="#">Return Values</a>
<b>Result</b>	byte[]	Decrypted data

**asymmetricKeyDecrypt** performs an asymmetric key decryption operation on the input **Data** object.

**Data** **must** be padded *as required by the encryption algorithm* like [PKCS #1](#) for [http://xmlns.webpki.org/sks/algorithm#rsa.pkcs1\\_5](http://xmlns.webpki.org/sks/algorithm#rsa.pkcs1_5).

The **Parameters** object **must** be of zero length for algorithms not needing additional input.

Invalid **Authorization** data (PIN) to the key **must** return [ERROR\\_AUTHORIZATION](#) status.

# keyAgreement [102]

## Input

Name	Type	Description
<b>KeyHandle</b>	int	Local handle to the target key
<b>Algorithm</b>	uri	Key agreement algorithm URI. See <a href="#">Diffie-Hellman Key Agreement</a>
<b>Parameters</b>	byte[]	Parameters needed by some key agreement algorithms
<b>Authorization</b>	byte[]	Holds a PIN or is of zero length if no PIN is supplied
<b>PublicKey</b>	byte[]	The other party's public key

## Output

Name	Type	Description
<b>Status</b>	byte	See <a href="#">Return Values</a>
<b>Result</b>	byte[]	Shared secret

**keyAgreement** performs an asymmetric key agreement operation resulting in a shared secret.

**PublicKey** **must** be an EC public key in [X.509](#) DER format using the same curve as **KeyHandle**. **PublicKey** **must** match the elliptic curve capabilities given by [getDeviceInfo](#).

The **Parameters** object **must** be of zero length for algorithms not needing additional input.

Invalid **Authorization** data (PIN) to the key **must** return [ERROR\\_AUTHORIZATION](#) status.



## performHMAC [103]

### Input

Name	Type	Description
<b>KeyHandle</b>	int	Local handle to the target key
<b>Algorithm</b>	uri	HMAC algorithm URI. See <a href="#">HMAC Operations</a>
<b>Parameters</b>	byte[]	Parameters needed by some HMAC algorithms
<b>Authorization</b>	byte[]	Holds a PIN or is of zero length if no PIN is supplied
<b>Data</b>	blob	Data to be HMACed. Also see <a href="#">CryptoDataSize</a>

### Output

Name	Type	Description
<b>Status</b>	byte	See <a href="#">Return Values</a>
<b>Result</b>	byte[]	HMACed data

**performHMAC** performs a symmetric key HMAC operation on the input **Data** object.

The **Parameters** object **must** be of zero length for algorithms not needing additional input.

Invalid **Authorization** data (PIN) to the key **must** return [ERROR\\_AUTHORIZATION](#) status.

# symmetricKeyEncrypt [104]

## Input

Name	Type	Description
<b>KeyHandle</b>	int	Local handle to the target key
<b>Algorithm</b>	uri	Encryption algorithm URI. See <a href="#">Symmetric Key Encryption</a>
<b>Mode</b>	bool	True for encryption, false for decryption
<b>Parameters</b>	byte[]	Parameters needed by some encryption algorithms
<b>Authorization</b>	byte[]	Holds a PIN or is of zero length if no PIN is supplied
<b>Data</b>	blob	Data to be encrypted or decrypted. Also see <a href="#">CryptoDataSize</a>

## Output

Name	Type	Description
<b>Status</b>	byte	See <a href="#">Return Values</a>
<b>Result</b>	blob	Encrypted or decrypted data

**symmetricKeyEncrypt** performs a symmetric key encryption or decryption operation on the input **Data** object.

Note that if an IV (Initialization Vector) is required by the encryption algorithm it **must** be supplied in **Parameters** unless it is supposed to be supplied as a part of **Data** like for [XML Encryption](#).

The **Parameters** object **must** be of zero length for algorithms not needing additional input.

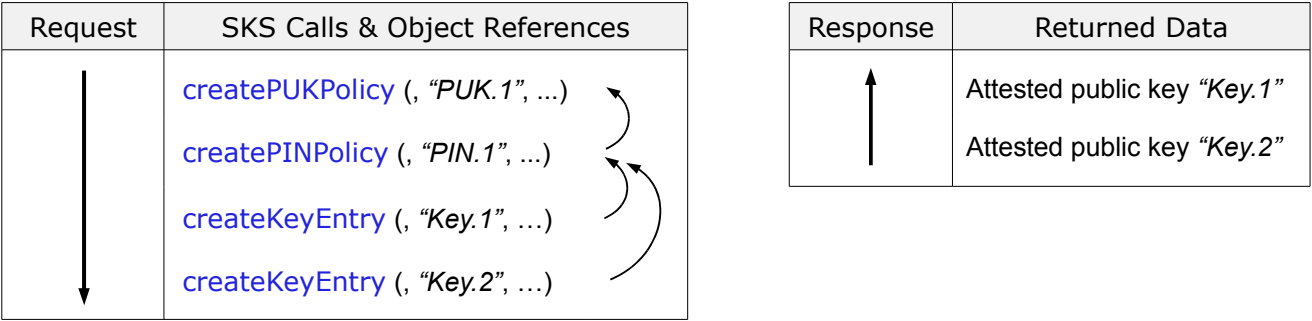
Invalid **Authorization** data (PIN) to the key **must** return [ERROR\\_AUTHORIZATION](#) status.

# Appendix A. KeyGen2 Proxy

SKS departs from most other SE (Security Element) designs by relying on a “Semi-Trusted Proxy” for the provisioning and management of keys. Introducing a proxy in a scheme which is claimed supporting *true end-to-security* may sound like a contradiction. However, any alterations to the data flowing between the two end-points (the issuing service and the SKS) will be detected by one of them due to the use of *stateful sessions*, *sequence counters* and *MAC operations*. The picture below shows the SKS/KeyGen2 provisioning architecture:



Since SKS methods *by design* are low-level, most of the comparatively high-level provisioning operations result in multiple SKS calls. In addition, there is a need for referencing objects created by preceding calls. As it would be quite inefficient if every call forced a network “round-trip”, a core proxy task is *aggregating and linking SKS calls and return data*. This is facilitated through the SKS virtual namespace concept which relieves issuers from ever dealing with raw (and device-dependent) object handles or worrying about name collisions. See [Object IDs](#). The following graph outlines content aggregation and linking when applied to the KeyGen2 example on page 37:



Another provisioning activity orchestrated by the proxy is requesting (and validating according to the issuer's policy), user-defined PINs, because SKS depends on that all initial PIN values are set during key entry creation.

## Appendix B. Sample Session

The following provisioning sample session shows the *sequence* for creating an X.509 certificate with a matching PIN and PUK protected private key:

```
ProvisioningHandle, ... = createProvisioningSession (...)  
PUKPolicyHandle = createPUKPolicy (ProvisioningHandle, ...)  
PINPolicyHandle = createPINPolicy (ProvisioningHandle, ... , PUKPolicyHandle, ...)  
KeyHandle, ... = createKeyEntry (ProvisioningHandle, ... , PINPolicyHandle, ...)  
  
    External certification of the generated public key happens here...  
  
setCertificatePath (KeyHandle, ...)  
closeProvisioningSession (ProvisioningHandle, ...)
```

Note that **Handle** variables are only used by local middleware, while (not shown) variables like **SessionKey**, **MAC**, **ID**, etc. are primarily used in the communication between an issuer and the SKS.

If keys are to be created entirely locally, this requires local software emulation of an issuer.

## Appendix C. Reference Implementation

To further guide implementers, an open source SKS reference implementation in java® is available including a JUnit suite.

URL: <http://code.google.com/p/openkeystore>

## Appendix D. Remote Key Lookup

In order to update keys and related data, SKS supports post provisioning operations like [postDeleteKey](#) where issuers are securely shielded from each other by the use of a [KeyManagementKey](#).

However, depending on the use-case, an issuer may need to get a list of applicable keys, *before* launching post provisioning operations. Such a facility is available in [KeyGen2](#) as illustrated by the JSON fragment below:

```
{
  "@context": "http://xmlns.webpki.org/keygen2/1.0",
  "@qualifier": "CredentialDiscoveryRequest",
  "ServerSessionID": "14184c1f09eqCkPtjqY54Ehalc2_EjFN",
  "ClientSessionID": "Qn7o4xCRp1sewDrpqMJEDieZHp2hego",
  "SubmitURL": "http://issuer.example.com/credisc",
  "LookupSpecifiers":
  [{
    "ID": "Lookup.1",
    "Nonce": "eG3XgquTRh6ASFpcUpEe0gc1qnIL/I2CoPx8xqJTvQ0=",
    "SearchFilter":
    {
      "EmailRegEx": "\\Qjohn.doe@example.com\\E"
    },
    "Signature":
    {
      "Algorithm": "http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha256",
      "KeyInfo":
      {
        "PublicKey":
        {
          "EC":
          {
            "NamedCurve": "http://xmlns.webpki.org/sks/algorithm#ec.nist.p256",
            "X": "INxNvAUee8t7DSQBft93LVsXxKCiVjhbWWfyg023FCk=",
            "Y": "LmTIQxXB3LgZrNLmhOfMaCnDizczC/RfQ6Kx8iNwfFA="
          }
        }
      },
      "SignatureValue": "MEUCIHWCPcD9DMY . . . Av7Px3bfwvagWcQYI6kea4kVrdeT38clzhiKnpiLuigY="
    }
  ]
}
```

The example works as follows:

1. Verify that the **signature** is *technically* valid while the origin of the signing key is *ignored* since the [KeyGen2 Proxy](#) has no opinion about those .
2. Verify that the freshness **Nonce** matches [SHA256](#) (**ClientSessionID** || **ServerSessionID**). See [createProvisioningSession](#) and [Data Types](#).
3. Enumerate all sessions having a [KeyManagementKey](#) matching the public key of the **Signature**. This serves as an *Issuer Filter*. See [enumerateProvisioningSessions](#).
4. From step #3 enumerate all matching SKS keys and related certificates. See [enumerateKeys](#) and [getKeyAttributes](#).
5. Collect the keys from step #4 that also feature the e-mail addresss "john.doe@example.com" in the [End-Entity Certificate](#).

*Continued on the next page...*

The result is sent back to the issuer in the form of a list of [End-Entity Certificate](#) paths and session IDs:

```
{
  "@context": "http://xmlns.webpki.org/keygen2/1.0",
  "@qualifier": "CredentialDiscoveryResponse",
  "ServerSessionID": "14184c1f09eqCkPtjqY54Ehalc2_EjFN",
  "ClientSessionID": "Qn7o4xCRp1sewDrpqMJEDieZHp2hego",
  "LookupResults":
    [{
      "ID": "Lookup.1",
      "MatchingCredentials":
        [{
          "ClientSessionID": "wmdVVHWjI666GvHnwmlALFRJQ-GC3Scr",
          "ServerSessionID": "14184c1f0438OwdjLnmGglx2c8245rDH",
          "X509CertificatePath":
            [
              "MIICijCCAX6gAwIBAgI GAUGEwfB4MA0GCSq . . . rGnyW8pnGcQ1U2clYD6vWN28GEup"
            ],
          "Locked": true
        }]
    }]
}
```

#### Notes:

Remote key lookups are performed at the *middleware level* since they are passive, JSON-centric, and do not access private or secret keys.

The primary purpose with credential lookups is *improving provisioning robustness*, while the *Issuer Filter protects user privacy* by constraining lookup data to the party to where it belongs.

If a matching credential is locked (presumably due to user authorization failures), this information will also be available as shown in sample.

## Appendix E. Security Considerations

Note: The following section only *partially* applies to the [Privacy Enabled Provisioning](#) mode.

This document does not cover the *physical* security of the key-store since SKS does not differ from other schemes in this respect.

However, the provisioning concept has some specific security characteristics. One of the most critical operations in SKS is the creation of a shared [SessionKey](#) because if such a key is intercepted or guessed by an attacker, the integrity of the entire session is potentially jeopardized.

If you take a peek at [createProvisioningSession](#) you will note that the [SessionKey](#) depends on issuer-generated and SKS-generated ephemeral public keys. It is pretty obvious that malicious middleware could replace such a key with one it has the private key to and the issuer wouldn't notice the difference. This is where the attestation signature comes in because it is computationally infeasible creating a matching signature since the both of the ephemeral public keys are enclosed as a part of the signed attestation object. That is, the issuer can when receiving the response to the provisioning session request, easily detect if it has been manipulated and *cease the rest of the operation*.

As earlier noted, the randomness of the [SessionKey](#) is crucial for all provisioning operations.

Missing or repeated objects are indirectly monitored by the use of [MACSequenceCounter](#), while the SKS “book-keeping” functions will detect other possible irregularities during [closeProvisioningSession](#). This means that an issuer **should not** consider issued credentials as valid unless it has received a successful response from [closeProvisioningSession](#).

The [SessionKeyLimit](#) attribute defined in [createProvisioningSession](#) is another security measure which aims to limit exhaustive attacks on the [SessionKey](#).

For algorithms that are considered as vulnerable to brute-force key searches, a simple workaround is adding a short *initial delay* to the applicable [User API](#) method. Since SKS is exclusively intended for user authentication a 1-100 ms delay imposes a (from the user's point of view), *hardly noticeable* impact on the performance.

By using the [EndorsedAlgorithm](#) option, issuers can specify exactly which algorithms that are permitted for a given key.

A significant feature of SKS is that it is identified by a digital certificate, preferably issued by a known vendor of trusted hardware. This enables the issuer to securely identify the key-container both from a cryptographic point of view (brand, type etc) and as a specific unit. The latter also makes it possible to communicate the container identity as an SHA1 fingerprint of the [Device Certificate](#) which facilitates novel and secure enrollment procedures, *typically eliminating the traditional sign-up password*.

That any issuer (after the user's consent), can provision keys may appear a bit scary but *keys do not constitute of executable code* making it less interesting in tricking users accepting “bad” issuers. In addition, the provisioning middleware is also able to validate incoming data for “sanity” and even abort unreasonable requests, such as asking for 10 keys or more to be created.

Although not a part of SKS, [KeyGen2](#) puts a signature derived from the [SessionKey](#) over the provisioning session response. The latter holds an HTTPS [Error: Reference source not found](#) giving the issuer an opportunity verifying that there actually is a “straight line” between the client and server.

One might suspect that the [VSD](#) scheme by relying on a static, *potentially issuance-wide* [KeyManagementKey](#) could introduce client-side vulnerabilities but that is unlikely to be the case: If a key management signature is intercepted by an attacker, the inclusion of a high entropy [SessionKey](#) and the [Device Certificate](#) renders it useless in another session or device. It is also worth noting that the post provisioning operations *by design* do not expose secret or private key data.

There is no protection against DoS (Denial of Service) attacks on SKS storage space due to malicious middleware.

SKS does not have any built-in policy, it is up to the individual *issuer* deciding about suitable key protections options, key sizes, and private key imports.

## Appendix F. Intellectual Property Rights

This document contains several constructs that *could* be patentable but the author has no such interests and therefore puts the entire design in *public domain* allowing anybody to use all or parts of it at their discretion. In case you adopt something you found useful in this specification, feel free mentioning where you got it from ☺

Note: it is possible that there are pieces that already are patented by *other parties* but the author is currently unaware of any IPR encumbrances.

Some of the core concepts have been submitted to <http://defensivepublications.org> and subsequently been published in IP.COM's *prior art database*.

## Appendix G. References

KeyGen2	TBD
PKCS #1	TBD
PKCS #8	TBD
ECDSA	TBD
AES256-CBC	TBD
HMAC-SHA1	TBD
HMAC-SHA256	TBD
X.509	TBD
SHA256	TBD
TPM 1.2	TBD
Diffie-Hellman	TBD
S/MIME	TBD
UTF-8	TBD
XML Encryption	TBD
RFC 3447	TBD
RFC 5639	TBD
XML Signature	TBD
FIPS 197	TBD
FIPS 186-3	TBD
Information Card	TBD
Base64	TBD
HOTP	TBD
JavaCard	TBD
JCE	TBD
CryptoAPI	TBD
PKCS #11	TBD
GlobalPlatform	TBD
TLS	TBD
XML Schema	TBD



SP800-56A	TBD
Kerberos	TBD
Blind Signatures	TBD
DAA	TBD
URI	TBD
JCS	JSON Clear-text Signature

## Appendix H. Acknowledgments

SKS and KeyGen2 heavily build on schemes pioneered by other individuals and organizations, most notably:

- *CT-KIP by RSA Security*: KeyGen2 format and basic operation
- *ObC by Nokia*: Key management through dynamic deployment of issuer-specific symmetric keys ([VSD](#)), and support for keys bound to downloaded data (in ObC code)
- *SCP80 by GlobalPlatform*: Secure messaging including “rolling MACs”
- *CertEnroll by Microsoft*: Processes

There is also a bunch of individuals that have been instrumental for the creation of SKS. I need to check who would accept to be mentioned :-)

KeyGen2 is an “homage” to Netscape Communications Corp. who created the first on-line provisioning system called KeyGen.

## Appendix I. Author

Anders Rundgren  
[anders.rundgren.net@gmail.com](mailto:anders.rundgren.net@gmail.com)

## To Do List

Although it would be nice to say “it is 100% ready” there are still a few things missing:

- Investigating “physical presence” GPIO options
- Language proofing
- Filling in the references