

# u.trust Anchor FIPS 140-3

PKCS#11 p11tool2

Reference Manual



## Imprint

Copyright 2024	Utimaco IS GmbH Germanusstr. 4 D-52080 Aachen Germany
Phone	AMERICAS +1-844-UTIMACO (+1 844-884-6226) EMEA +49 800-627-3081 APAC +81 800-919-1301
Internet e-mail	<a href="https://support.hsm.utimaco.com/">https://support.hsm.utimaco.com/</a> <a href="mailto:support@utimaco.com">support@utimaco.com</a>
Document Version	1.0.2
Product Version	6.0.0
Date	2024-10-24
Document No.	2024-0011
Status	<b>PUBLISHED</b>

All rights reserved	<p>No part of this documentation may be reproduced in any form (printing, photocopy or according to any other process) without the written approval of Utimaco IS GmbH or be processed, reproduced or distributed using electronic systems.</p> <p>Utimaco IS GmbH reserves the right to modify or amend the documentation at any time without prior notice. Utimaco IS GmbH assumes no liability for typographical errors and damages incurred due to them. Any mention of the company name Utimaco in this documents refers to the Utimaco IS GmbH.</p> <p>All trademarks and registered trademarks are the property of their respective owners.</p>
---------------------	--

# Table of Contents

<b>1</b>	<b>Introduction .....</b>	<b>5</b>
1.1	About This Document .....	5
1.1.1	Document Conventions .....	5
<b>2</b>	<b>The PKCS#11 Administration Tool Release 2 .....</b>	<b>7</b>
2.1	Overview (FIPS 140-3) .....	7
2.2	Data Type Notation .....	9
<b>3</b>	<b>Basic Commands .....</b>	<b>11</b>
3.1	Help .....	11
3.2	PrintError .....	11
3.3	Version .....	12
<b>4</b>	<b>PKCS#11 Commands .....</b>	<b>13</b>
4.1	Key Usage in FIPS Mode.....	13
4.2	ListSlots .....	13
4.3	GetInfo.....	14
4.4	GetSlotInfo .....	15
4.5	GetTokenInfo .....	15
4.6	LoginSO .....	16
4.7	LoginUser .....	16
4.8	InitToken .....	17
4.9	InitPIN .....	20
4.10	SetPIN .....	22
4.11	ListObjects.....	22
4.12	DeleteObject .....	25
4.13	ImportP12.....	26
4.13.1	Imported Certified Attributes.....	27
4.13.2	Imported Private Key Attributes .....	28
4.13.3	Imported Public Key Attributes .....	30
4.14	ImportCert .....	32
4.15	ExportCert .....	33
4.16	ExportP10.....	36
4.17	GenerateKeyPair.....	39
4.17.1	Generate Key Pair Based on Default Attribute Template.....	39
4.17.2	Generate Key Pair from Template File.....	41

---

4.18	GenerateKey .....	43
4.18.1	Generate Secret Key Based on Default Attribute Template.....	43
4.18.2	Generate Secret Key from Template File.....	46
<b>5</b>	<b>Configuration Commands .....</b>	<b>48</b>
5.1	ListConfig .....	48
5.2	GetLocalConfig .....	51
5.3	GetGlobalConfig .....	52
5.4	SetGlobalConfig.....	52
5.5	GetSlotConfig .....	57
5.6	SetSlotConfig .....	58
5.7	SecureSlotPass .....	59
5.8	Separated Key Manager and Key User Role .....	60
<b>6</b>	<b>Backup/Restore Commands.....</b>	<b>62</b>
6.1	GetBackupInfo.....	62
6.2	BackupInternalKeys.....	62
6.3	BackupExternalKeys.....	63
6.4	BackupConfig .....	65
6.5	RestoreInternalKeys .....	65
6.6	RestoreExternalKeys .....	66
6.7	RestoreConfig.....	67
6.8	DeleteSO.....	67
6.9	RecryptExternalKeys .....	68
<b>7</b>	<b>Contact Address for Support Queries .....</b>	<b>70</b>
<b>8</b>	<b>References .....</b>	<b>71</b>

# 1 Introduction

Thank you for purchasing our u.trust Anchor security system. We hope you are satisfied with our product. Please do not hesitate to contact us if you have any complaints or other comments.

## 1.1 About This Document

This document provides detailed description of the PKCS#11 Administration Tool Release 2 (p11tool2) commands.

### 1.1.1 Document Conventions

We use the following document conventions:

<i><b>Convention</b></i>	<i><b>Use</b></i>	<i><b>Example</b></i>
<b>Bold</b>	Items of the Graphical User Interface (GUI), e.g., menu options	Press <b>OK</b>
<code>Monospaced</code>	Code that is given for explanation or as an example, file paths	<code>chsm-create</code>
<i>Italic</i>	References and important terms	See <i>Sample Chapter</i> in the <i>CryptoServer - Sample Manual</i>

Table 1: Document conventions

We use special icons to highlight the most important notes and information.



Here, you find important safety information that should be followed.



Here, you find additional notes or supplementary information.



This message marks the result expected after the successful execution of an instruction.

## 2 The PKCS#11 Administration Tool Release 2

p11tool2 is the PKCS#11 Administration Tool Release 2 based on the provided PKCS#11 Library R3. It is a command line utility designed for being called from the command line or in a batch file. The p11tool2 offers functions to execute PKCS#11 commands on the u.trust Anchor and additional commands for backup, restoration and configuration settings.

This document gives detailed command descriptions of the p11tool2. For further information about requirements and configuration, see [PKCS#11 R3 - Developer Guide](#).

### 2.1 Overview (FIPS 140-3)

The following table gives a short overview of the p11tool2 commands.



Certain types of shell processes treat certain characters (for example, commas, colons, semi-colons) differently. If the execution of a p11tool2 command fails with an error message from the shell about a missing parameter or an illegal parameter format, quoting parameter values may be necessary.

The following is an example for a correct p11tool2 command syntax in a Microsoft PowerShell:

```
p11tool2      [Slot=<slot_id>]      Login="<user_name>,<auth_token>"  
<command>
```



The p11tool2 does not support POSIX syntax. Therefore, the use of "~" is not supported. Only relative and absolute path may be specified.

Command	Description
<b>Basic Commands:</b>	
PKCS#11 Commands:	
Help[=]	Show a list of all available commands if called without any parameter or specific help if a command name is given as a parameter
PrintError=	Display the corresponding error message text to an error code.
Version	Show the version number of the p11tool2

<b>Command</b>	<b>Description</b>
<b>Basic Commands:</b>	
<b>PKCS#11 Commands:</b>	
ListSlots[=]	List all slots
GetInfo	Get general information about Cryptoki
GetSlotInfo	Get information about a specific slot
GetTokenInfo	Get information about a specific token
LoginSO=	Login as security officer (SO)
LoginUser=	Login as normal user
Login=	Login as generic user
InitToken=	Initialize a token
InitPIN=	Initialize the normal user PIN
SetPIN=	Change the PIN of the SO or the normal user
ListObjects	List available objects
DeleteObject	Delete a specific object
ImportP12=	Import certificate, public and private key from PKCS#12 file
ImportCert=	Import certificate and public key from certificate file
ExportCert[=]	Write the BER-encoding of a specific certificate to a file or to the standard output if no file name is set
ExportP10=	Export a certificate signing request
GenerateKey=	Generate a secret key or set of domain parameters
GenerateKeyPair=	Generate a public/private key pair
<b>Configuration Commands:</b>	
ListConfig=	List all configuration attributes
GetLocalConfig=	Get local configuration value



<b>Command</b>	<b>Description</b>
<b>Basic Commands:</b>	
<b>PKCS#11 Commands:</b>	
GetGlobalConfig=	Get global configuration value
GetSlotConfig=	Get slot configuration value
SetGlobalConfig=	Set global configuration value
SetSlotConfig=	Set slot configuration value
<b>Backup/Restore Commands:</b>	
GetBackupInfo	Get information about the given backup key
BackupInternalKeys=	Backup all available internal keys within the slot
BackupExternakKeys	Backup all available external keys within the slot
BackupConfig=	Backup the slot configuration object
RestoreInternalKeys=	Restore all keys from the given key backup file to the internal key store
RestoreExternakKeys=	Restore all keys from the given key backup file to the external key store
RestoreConfig=	Restore the slot configuration object from the given configuration backup file
DeleteSO	Delete the SO
RecryptExternalKeys	Creates a backup and recrypt all available external cryptographic keys within the slot with the current MBK

Table 2: p11tool2 commands - overview

## 2.2 Data Type Notation

The following data type notation is used for the attribute list parameters ( `KeyAttr`, `PubKeyAttr`, `PrvKeyAttr`, `CertAttr` ) and the attribute template files.

Data Type	Description
CK_BB00L	CK_TRUE   true   1 CK_FALSE   false   0  Example: CKA_PRIVATE=CK_TRUE
CK_ULONG	Unsigned integer value Example:
RFC2279 String	String Example: CKA_LABEL=ABC CKA_LABEL="A B C"
Byte Array	String or hexadecimal notation with "0x" prefix Example: CKA_ID=ABC CKA_ID=0x414243 CKA_ID="A B C"
Big Integer	Unsigned integer value or hexadecimal notation with "0x" prefix Example: CKA_PUBLIC_EXPONENT=65537 CKA_PUBLIC_EXPONENT=0x010001
Object Type	Object type as string Example: CKA_CLASS=CKO_PRIVATE_KEY CKA_KEY_TYPE=CKK_RSA
CK_DATE	Date of format YYYYMMDD Example: CKA_END_DATE=20141231

Table 3: Data type notations

## 3 Basic Commands

These basic commands are p11tool2 internal functions. No connection to the PKCS#11 API will be established.

### 3.1 Help

If called without any parameter, this command shows a list of all available p11tool2 commands. If a command name is given as a parameter, specific help will be provided.

<b>Syntax</b>	p11tool2 Help
	p11tool2 Help=<command>
<b>Parameter</b>	<b>Description</b>
<command>	specific command of the p11tool2
<b>Example</b>	csadm Dev=10.17.1.9 CSLGetStatus
<b>Output</b>	Lists all available p11tool2 commands

### 3.2 PrintError

This command displays the corresponding error message text to an error code.

<b>Syntax</b>	p11tool2 PrintError=<err>
<b>Parameter</b>	<b>Description</b>
<err>	error code in hexadecimal notation
<b>Example</b>	p11tool2 PrintError=B901306F
<b>Output</b>	Error B901306F CryptoServer API LINUX can't get connection errno = 111

### 3.3 Version

This command shows the version number of the p11tool2 and all built-in libraries.

<b>Syntax</b>	<code>p11tool2 Version</code>
<b>Output</b>	<pre>p11tool2 3.1.1 p11adm_R2 3.1.1 CryptoServer PKCS#11 Library R3 1.19 (Nov 10 2021) cxi_api 1.9.0 (Nov 10 2021) csadm_lib (global) 3.5.1 csapi 1.13.0 (Nov 10 2021) csxapi 1.11.8 (Nov 10 2021) pp_api 1.9.8 (Nov 10 2021) yacl 1.14.4 sdb 2.2.2 (Nov 10 2021 23:32:33) copa 1.1.8 sl 1.1.5</pre>

## 4 PKCS#11 Commands

These commands are based on the standard PKCS#11 commands. A connection to the PKCS#11 API will be established.

Note that, by default, the build-in PKCS#11 Library R3 is used and no shared library is loaded. Thus, the execution of some commands may differ from the standard case. For example, the creation of an SO for token initialization must be authenticated by a user or administrator logged in with a special user type `CKU_CS_GENERIC`. Those special cases are documented in the corresponding command description.



Certain types of shell processes treat certain characters (for example, commas, colons, semi-colons) differently. If the execution of a p11tool2 command fails with an error message from the shell about a missing parameter or an illegal parameter format, quoting parameter values may be necessary.

The following is an example for a correct p11tool2 command syntax in a Microsoft PowerShell:

```
p11tool2 [Slot=<slot_id>] Login="<user_name>,<auth_token>"  
<command>
```

### 4.1 Key Usage in FIPS Mode

Each time an RSA or EC (ECDSA, ECDH or Edwards) key is generated or imported, it must be checked that its usage attribute is exactly one of the { `CKA_SIGN`; `CKA_VERIFY` } usage bit group or exactly one of the { `CKA_ENCRYPT`, `CKA_DECRYPT`, `CKA_DERIVE`, `CKA_WRAP`, `CKA_UNWRAP` } usage bit group. I.e., if key pairs are used for signature generation and verification, they must not be used for any other purpose, see *Key Usage in FIPS Mode* and *Padding Mechanisms in FIPS Mode* in the [CryptoServer PKCS#11 R3 - Developer Guide](#).

### 4.2 ListSlots

This command displays a list of all slots in the system, using the PKCS#11 command `C_GetSlotList`.

<b>Syntax</b>	<code>p11tool2 ListSlots[=status]</code>
---------------	--

Parameter	Description
<code>status</code>	This parameter is optional. If used, the initialization status of each slot is displayed additionally.

<b>Example</b>	p11tool2 ListSlots
<b>Output</b>	0: 00000000 1: 00000001 2: 00000002 3: 00000003 4: 00000004

### 4.3 GetInfo

This command displays general information about Cryptoki, using the PKCS#11 command `C_GetInfo`.

<b>Syntax</b>	p11tool2 GetInfo
<b>Example</b>	p11tool2 GetInfo
<b>Output</b>	CK_INFO:  cryptokiVersion : 2.20 manufacturerID 5574696d 61636f20 53616665 77617265   Utimaco IS GmbH  20414720 20202020 20202020 20202020     flags : 0x00000000  libraryDescription 43727970 746f5365 72766572 20504b43   CryptoServer PKC  53233131 204c6962 72617279 20523220  S#11 Library R3   libraryVersion : 2.13

## 4.4 GetSlotInfo

This command displays the information about a specific slot, using the PKCS#11 command `C_GetSlotInfo`.

<b>Syntax</b>	<code>p11tool2 [Slot=&lt;slot_id&gt;] GetSlotInfo</code>
---------------	--

Parameter	Description
<slot_id>	ID of the slot as number. Default: 0

<b>Example</b>	<code>p11tool2 GetSlotInfo</code>
----------------	-----------------------------------

<b>Output</b>	<pre>CK_SLOT_INFO (slot ID: 0x00000000):    slotDescription      5043493a 30202d20  534c4f54 5f303030  PCI:0 - SLOT_000  0  manufacturerID      5574696d 61636f20  53616665 77617265     Utimaco IS GmbH   flags: 0x00000005    CKF_TOKEN_PRESENT    : CK_TRUE   CKF_REMOVABLE_DEVICE : CK_FALSE   CKF_HW_SLOT          : CK_TRUE    hardwareVersion      : 3.00   firmwareVersion      : 2.01</pre>
---------------	--

## 4.5 GetTokenInfo

This command displays the information about a specific token, using the PKCS#11 command `C_GetTokenInfo`.

<b>Syntax</b>	p11tool2 [Slot=<slot_id>] GetTokenInfo
<b>Parameter</b>	<b>Description</b>
<slot_id>	ID of the slot as number. <u>Default</u> : 0
<b>Example</b>	p11tool2 GetTokenInfo
<b>Output</b>	Returns the token info on success, otherwise an error message.

## 4.6 LoginSO

This command logs the security officer (SO) into a token, using the PKCS#11 command C\_Login with user type `CKU_SO`.

<b>Syntax</b>	p11tool2 [Slot=<slot_id>] LoginSO=<so_pin> <command>
<b>Parameter</b>	<b>Description</b>
<slot_id>	ID of the slot as number (to open a session). <u>Default</u> : 0
<so_pin>	SO PIN or string 'ask' if hidden PIN entry should be used.
<command>	Command which has to be authenticated by the SO
<b>Example</b>	p11tool2 LoginSO=654321 InitPIN=123456
<b>Output</b>	None on success, or error message

## 4.7 LoginUser

This command logs the normal user into a token, using the PKCS#11 command C\_Login with user type `CKU_USER`.



<b>Syntax</b>	p11tool2 [Slot=<slot_id>] LoginUser=<user_pin> <command>
---------------	--

Parameter	Description
<slot_id>	ID of the slot as number (to open a session). Default: 0
<user_pin>	User's PIN in clear text or the string 'ask', if hidden PIN entry is preferred.
<command>	Command which has to be authenticated by the normal user

<b>Example</b>	p11tool2 LoginUser=ask GenerateKeyPair=RSA
----------------	--

<b>Output</b>	None on success, or error message
---------------	-----------------------------------

## 4.8 InitToken

This command initializes a token, using the PKCS#11 command `C_InitToken`.

### Initialization:

If the token has not been initialized, the given PIN becomes the SO initial PIN.




In case of the provided PKCS#11 Library R3 a cHSM administrator with permission mask 0x20000000 or the default administrator ADMIN must be logged in (via the command Login) to create the SO. The Security Officer (permission 00000200) to be created has the name SO\_xxxx with xxxx being a 2-byte decimal representation of the key group/PKCS#11 slot ID. The name may range from SO\_0000 to SO9999.

The security-relevant functions that a Security Officer is permitted to perform are listed in *Permissions and Authentication Status* in the [u.trust Anchor FIPS 140-3 - Containerized Hardware Security Module \(cHSM\) - Administration Manual](#).

### Reinitialization:

If the token has already been initialized, a reinitialization is only performed if the flag `<force>` is set to 1 or y. The given SO PIN is used to authorize the reinitialization operation, which will delete all destructible objects and the normal user.

<b>Syntax</b>	<code>p11tool2 [Slot=&lt;slot_id&gt;] [Label=&lt;label&gt;] [Force=&lt;force&gt;] [Login=&lt;admin_name&gt;,&lt;admin_auth_token&gt;] InitToken=&lt;so_pin&gt;</code>
Parameter	Description
<slot_id>	ID of the slot as number <u>Default:</u> 0
<label>	Label of the token as string or as hexadecimal notation with "0x" prefix <u>Default:</u> "CryptoServer PKCS11 Token"   The label is also automatically assigned to the SO of the PKCS#11 slot as the user attribute <code>L[]</code> , and is displayed on execution of the <code>csadm ListUser</code> command.
<force>	Boolean flag (0/1 or n/y) to force token re-initialization <u>Default:</u> 0 (= refuse re-initialization) Re-initialization is not supported, i.e., the following does not work: <code>p11tool2 Slot=0 Login=ADMIN,MyADMIN.key InitToken=12345678</code> <code>p11tool2 Slot=0 Login=ADMIN,MyADMIN.key Force=1</code> <code>InitToken=11223344</code> If the ADMIN wants to assign a new PIN to the SO, use the <code>csadm ChangeUser</code> command instead.
<admin_name>	Name of a CHSM administrator with permission mask 0x20000000 or the default administrator ADMIN
<admin_auth_token>	Authentication token of the CHSM administrator with <code>&lt;admin_name&gt;</code> : <ul style="list-style-type: none"><li>▪ <b>Case password-based authentication</b> Administrator password or string 'ask' if hidden password entry should be used.</li><li>▪ <b>Case signature-based authentication</b> Key specifier where the private part of the administrator key should be loaded from:<ul style="list-style-type: none"><li>• Smartcard specifier, e.g., <code>' :cs2:cjo:USB0 '</code> See <i>Authentication Mechanisms</i> in the <a href="#">u.trust Anchor FIPS 140-3 - Containerized Hardware Security Module (CHSM) - Administration Manual</a>.</li><li>• <b>RSA signature authentication</b> The PIN pad has to be connected to the computer where <code>p11tool2</code> is running (USB port) Example: <code>' :cs2:cjo:USB0@123.123.123.123/mypwd '</code></li><li>• <b>Keyfile[#password]</b>, e.g., <code>' my.key#pwd '</code> If the keyfile is encrypted, hidden password entry is possible by entering the string 'ask' as password.</li></ul></li></ul>

Parameter	Description
<so_pin>	<p>SO PIN in clear text or the string 'ask' if hidden PIN entry is preferred.</p> <p>If a PKCS#11 Security Officer has been created and this SO has not changed the PIN that was assigned to him/her during creation and if this SO tries to perform an action an authentication is needed for, this action is not performed, but the error message Error B0830091 / CryptoServer module CMDS, Command scheduler / The user credentials need to be updated is shown instead. If this tried action is a PKCS#11 action, this error is mapped to CKR_PIN_TOO_WEAK and an entry Error CKR PIN TOO_WEAK occurred. is created in the PKCS#11 log file cs_pkcs11_R3.log.</p> <p>A PKCS#11 Security Officer has to perform the p11tool2 LoginSO=&lt;Old PIN&gt; SetPIN=&lt;Old PIN&gt;,&lt;New PIN&gt; command to change his/her PIN.</p> <p>A user uses an HMAC password-based key-derived function (HMAC-PBKDF) for authentication. The HMAC-PBKDF according to NIST SP 800-132 does not use the HMAC password itself for authentication but a function derived from the HMAC password. For HMAC-PBKDF, 1000 iterations are used here. This number of iterations, as used for the key derivation from a given password, is fix and not configurable. HMAC-PBKDF is only applied if on both sides, the host side and the firmware side, HMAC-PBKDF is applied. If it is not available on one of these sides, the legacy version of the HMAC password-based mechanism is applied, whereby the user's password is used directly as an HMAC key.</p>

<b>Example</b>	<p>p11tool2 Slot=2 Login=ADMIN,C:/keys/init_prv.key InitToken=123456</p> <p>This command creates a Security Officer with the name SO_0002 in the slot SLOT_0002.</p>
----------------	--

<b>Output</b>	None on success, or error message
---------------	-----------------------------------

## Verifying the result

Example:

```
csadm Dev=3001@127.0.0.1 ListUser
```

Example output:

Name	Permission	Mechanism	Attributes
ADMIN	22000000	RSA sign	Z[0]
SO_0002	00000200	HMAC passwd	I[1]A[CXI_GROUP=SLOT_0002]L[CryptoServer PKCS11 Token]

## Changing the label of a token

To change the label of a token, delete the security officer and initialize a new token with the desired label. Proceed as follows:

1. The token label is shown as the user attribute `L[]` in the output of the `csadm ListUser` command.

Example:

```
csadm Dev=3001@127.0.0.1 ListUser
```

Example output:

Name	Permission	Mechanism	Attributes
ADMIN	22000000	RSA sign	Z[0]
SO_0002	00000200	HMAC passwd	
Z[0]I[1]A[CXI_GROUP=SLOT_0002]L[CryptoServer PKCS11 Token]			

2. Delete the security officer of the slot. For details, see [DeleteSO](#).

Example:

```
p11tool2 Slot=2 Login=ADMIN,ADMIN.key DeleteSO
```

3. Initialize a token with the desired label.

Example:

```
p11tool2 Slot=2 Label=MyLabel Login=ADMIN,ADMIN.key InitToken=123456
```

4. Verify the result.

Example:

```
csadm Dev=3001@127.0.0.1 ListUser
```

Example output:

Name	Permission	Mechanism	Attributes
ADMIN	22000000	RSA sign	Z[0]
SO_0002	00000200	HMAC passwd	
I[1]A[CXI_GROUP=SLOT_0002]L[MyLabel]			

## 4.9 InitPIN

This command initializes the normal user PIN, using the PKCS#11 command `C_InitPIN`.

The User to be created has the name `USR_xxxx` with `xxxx` being a 2-byte decimal representation of the key group/PKCS#11 slot ID. The name may range from `USR_0000` to `USR_9999`.

<b>Syntax</b>	<code>p11tool2 [Slot=&lt;slot_id&gt;] LoginSO=&lt;so_pin&gt; InitPIN=&lt;user_pin&gt;</code>
---------------	--

Parameter	Description
<slot_id>	ID of the slot as number (to open a session). Default: 0
<so_pin>	SO PIN in clear text or the string 'ask' if hidden PIN entry is preferred.
<user_pin>	<p>User PIN in clear text or the string 'ask' if hidden PIN entry is preferred.</p> <p>If a PKCS#11 user has been created and this user has not changed the PIN that was assigned to him/her during creation and if this user tries to perform an action an authentication is needed for, this action is not performed, but the error message <code>Error B0830091 / CryptoServer module CMDS, Command scheduler / The user credentials need to be updated</code> is shown instead. If this tried action is a PKCS#11 action, this error is mapped to <code>CKR_PIN_TOO_WEAK</code> and an entry <code>Error CKR_PIN_TOO_WEAK occurred.</code> is created in the PKCS#11 log file <code>cs_pkcs11_R3.log</code>.</p> <p>A PKCS#11 user has to perform, for example, the <code>csadm LogonPass=USER_0000, &lt;Old PIN&gt; ChangeUser= USER_0000, &lt;New PIN&gt;</code> command to change his/her PIN.</p> <p>A PKCS#11 user uses an HMAC password-based key-derived function (HMAC-PBKDF) for authentication. The HMAC-PBKDF according to NIST SP 800-132 does not use the HMAC password itself for authentication but a function derived from the HMAC password. For HMAC-PBKDF, 1000 iterations are used here. This number of iterations, as used for the key derivation from a given password, is fix and not configurable. HMAC-PBKDF is only applied if on both sides, the host side and the firmware side, HMAC-PBKDF is applied. If it is not available on one of these sides, the legacy version of the HMAC password-based mechanism is applied, whereby the user's password is used directly as an HMAC key. In FIPS mode, using HMAC-PBKDF is mandatory.</p>

<b>Example</b>	<p><code>p11tool2 Slot=2 LoginSO=12345678 InitPIN=12345678</code></p> <p>This command creates the User with the name <code>USR_0002</code> in the slot <code>SLOT_0002</code>.</p>
----------------	--

<b>Output</b>	None on success, or error message
---------------	-----------------------------------

## Verify the result

Example:

```
csadm Dev=3001@127.0.0.1 ListUser
```

Example output:

Name	Permission	Mechanism	Attributes
ADMIN	22000000	RSA sign	Z[0]I[0]
SO_0002	0000200	HMAC passwd	Z[0]I[0]A[CXI_GROUP=SLOT_0002]L[MyLabel]
USR_0002	00000022	HMAC passwd	I[1]A[CXI_GROUP=SLOT_0002]

### 4.10 SetPIN

This command changes the PIN of the SO or the normal user, using the PKCS#11 command `C_SetPIN`.

<b>Syntax</b>	<ul style="list-style-type: none"><li>for SO: <code>p11tool2 [Slot=&lt;slot_id&gt;] LoginSO=&lt;so_pin&gt; SetPIN=&lt;so_pin&gt;,&lt;new_so_pin&gt;</code></li><li>for normal user: <code>p11tool2 [Slot=&lt;slot_id&gt;] [LoginUser=&lt;user_pin&gt;] SetPIN=&lt;user_pin&gt;,&lt;new_user_pin&gt;</code></li></ul>
---------------	--

Parameter	Description
<slot_id>	ID of the slot as number (to open a session). Default: 0
<so_pin>	(Old) SO PIN in clear text or the string 'ask' if hidden PIN entry is preferred.
<new_so_pin>	New SO PIN in clear text or the string 'ask' if hidden PIN entry is preferred.
<user_pin>	(Old) user PIN in clear text or the string 'ask' if hidden PIN entry is preferred.
<new_user_pin>	New user PIN in clear text or the string 'ask' if hidden PIN entry is preferred.

<b>Example</b>	<ul style="list-style-type: none"><li>for SO: <code>p11tool2 LoginSO=ask SetPIN=ask,ask</code></li><li>for normal user: <code>p11tool2 SetPIN=ask,ask</code></li></ul>
----------------	--

<b>Output</b>	None on success, or error message
---------------	-----------------------------------

### 4.11 ListObjects

This command displays a list of available objects, using the PKCS#11 commands like `C_FindObjects` and `C_GetAttributeValue`.

As described in the PKCS#11 standard, private objects are only available with user login. Without user login only public objects are listed.

<b>Syntax</b>	p11tool2 [Slot=<slot_id>] [LoginUser=<user_pin>] ListObjects
---------------	--

Parameter	Description
<slot_id>	ID of the slot as number (to open a session). Default: 0
<user_pin>	User PIN in clear text or the string 'ask' if hidden PIN entry is preferred.

<b>Example</b>	p11tool2 LoginUser=ask ListObjects
----------------	------------------------------------

<b>Output</b>	CKO_CERTIFICATE:
	<pre> + 1.1    CKA_CERTIFICATE_TYPE      = CKC_X_509   CKA_UNIQUE_ID              = 20F43080-51AE-48C9- B248-0E8BE2AA63304   CKA_LABEL                  = P12 Cert   CKA_ID                     = 0x503132 (P12)   CKA_SUBJECT                =                                  0x3032310B 30090603 55040613 02444531  021 0 U    DE1                                  10300E06 0355040A 13075574 696D6163   0    U Utimac                                  6F311130 0F060355 04031308 73637465  o1 0    U scte                                  73743031 st01                                       CKA_SENSITIVE              = CK_TRUE   CKA_EXTRACTABLE            = CK_FALSE  CKO_PUBLIC_KEY:  + 2.1    CKA_KEY_TYPE               = CKK_RSA   CKA_UNIQUE_ID              = 20F43080-51AE-48C9- B248-0E8BE2AA63304   CKA_LABEL                  = RSA Public Key   CKA_ID                     = 0x503132 (P12)   CKA_SUBJECT                =                                  0x3032310B 30090603 55040613 02444531  021 0 U    DE1                                  10300E06 0355040A 13075574 696D6163   0    U Utimac                                  6F311130 0F060355 04031308 73637465  o1 0    U scte                                  73743031                                   </pre>

st01		
CKA_SENSITIVE	= CK_TRUE	
CKA_EXTRACTABLE	= CK_FALSE	
+ 2.2		
CKA_KEY_TYPE	= CKK_ECDSA	
CKA_UNIQUE_ID	= 20F43080-51AE-48C9-	
B248-0E8BE2AA63304		
CKA_LABEL	= My ECC Public Key	
CKA_ID	= 0x454343 (ECC)	
CKA_SENSITIVE	= CK_TRUE	
CKA_EXTRACTABLE	= CK_FALSE	
CKO_PRIVATE_KEY:		
+ 3.1		
CKA_KEY_TYPE	= CKK_RSA	
CKA_UNIQUE_ID	= 20F43080-51AE-48C9-	
B248-0E8BE2AA63304		
CKA_LABEL	= RSA Private Key	
CKA_ID	= 0x503132 (P12)	
CKA_SUBJECT	=	
0x3032310B 30090603 55040613 02444531  021 0		
U DE1	10300E06 0355040A 13075574 696D6163   0 U	
Utimac	6F311130 0F060355 04031308 73637465  o1 0 U	
scte	73743031	
st01		
CKA_SENSITIVE	= CK_TRUE	
CKA_EXTRACTABLE	= CK_TRUE	
+ 3.2		
CKA_KEY_TYPE	= CKK_ECDSA	
CKA_UNIQUE_ID	= 20F43080-51AE-48C9-	
B248-0E8BE2AA63304		
CKA_LABEL	= My ECC Private Key	
CKA_ID	= 0x454343 (ECC)	
CKA_SENSITIVE	= CK_TRUE	
CKA_EXTRACTABLE	= CK_TRUE	
CKO_SECRET_KEY:		
+ 4.1		
CKA_KEY_TYPE	= CKK_AES	
CKA_UNIQUE_ID	= 20F43080-51AE-48C9-	
B248-0E8BE2AA63304		
CKA_LABEL	= My AES Secret Key	



	CKA_ID	= 0x414553 (AES)
	CKA_SENSITIVE	= CK_TRUE
	CKA_EXTRACTABLE	= CK_FALSE



For objects that are created using a PKCS#11 provider prior to SecurityServer 4.50 the value of the attribute `CKA_UNIQUE_ID` is displayed as `CK_UNAVAILABLE_INFORMATION`.

Only objects of the following classes are listed:

- CKO\_DATA
- CKO\_CERTIFICATE
- CKO\_PUBLIC\_KEY
- CKO\_PRIVATE\_KEY
- CKO\_SECRET\_KEY
- CKO\_DOMAIN\_PARAMETERS

Only the following object attributes are listed (if set):

- CKA\_CERTIFICATE\_TYPE
- CKA\_KEY\_TYPE
- CKA\_UNIQUE\_ID
- CKA\_LABEL
- CKA\_ID
- CKA\_SUBJECT
- CKA\_SENSITIVE
- CKA\_EXTRACTABLE

## 4.12 DeleteObject

This command deletes objects specified by the given label, ID and subject name, using the PKCS#11 commands like `C_FindObjects` and `C_DestroyObject`.

As described in the PKCS#11 specification, private objects can only be deleted with user login. Without user login only public objects can be deleted.

Note that at least one of the label, ID or subject name must be given in order to identify the objects to be deleted.

<b>Syntax</b>	<code>p11tool2 [Slot=&lt;slot_id&gt;] [LoginUser=&lt;user_pin&gt;] [Label=&lt;label&gt;] [Id=&lt;id&gt;] [Subject=&lt;subject&gt;] DeleteObject</code>
---------------	--

Parameter	Description
<slot_id>	ID of the slot as number (to open a session). Default: 0
<user_pin>	User PIN in clear text or the string 'ask' if hidden PIN entry is preferred.
<label>	Object label as string or as hexadecimal notation with "0x" prefix or '*' for all labels
<id>	Object ID as string or as hexadecimal notation with "0x" prefix or '*' for all IDs
<subject>	Object subject name as string or as hexadecimal notation with "0x" prefix or '*' for all subject names

<b>Example</b>	<code>p11tool2 LoginUser=ask Label="RSA Public Key" Id="P12" DeleteObject</code>
----------------	--

<b>Output</b>	<code>1 Objects deleted</code>
---------------	--------------------------------

### 4.13 ImportP12

This command imports an X.509 certificate, a public and a private key from the given PKCS#12 file, using the OpenSSL library, and save them as private objects, using the PKCS#11 command `C_CreateObject`.

The object attributes can be overwritten and extended by the attribute list parameters.

<b>Syntax</b>	<code>p11tool2 [Slot=&lt;slot_id&gt;] LoginUser=&lt;user_pin&gt; [CertAttr=&lt;cert_attr&gt;] [PubKeyAttr=&lt;pub_key_attr&gt;] [PrvKeyAttr=&lt;prv_key_attr&gt;] ImportP12=&lt;filename&gt;,&lt;password&gt;</code>
---------------	--

Parameter	Description
<slot_id>	ID of the slot as number (to open a session). Default: 0
<user_pin>	User PIN in clear text or the string 'ask' if hidden PIN entry is preferred.
<cert_attr>	List of certificate attributes in format <attribute_name_1>=<value_1>,<attribute_name_2>=<value_2>,...
<pub_key_attr>	List of public key attributes in format <attribute_name_1>=<value_1>,<attribute_name_2>=<value_2>,...
<prv_key_attr>	Private key attribute list of format <attribute_name_1>=<value_1>,<attribute_name_2>=<value_2>,...
<filename>	PKCS#12 file
<password>	PKCS#12 file password or string 'ask' if hidden password entry is preferred.

<b>Example</b>	p11tool2 LoginUser=ask CertAttr=CKA_LABEL="P12 Cert",CKA_ID=P12 PubKeyAttr=CKA_LABEL="P12 Public Key",CKA_ID=P12 PrvKeyAttr=CKA_LABEL="P12 Private Key",CKA_ID=0x503132 ImportP12=C:/p12/sctest01.p12,ask
----------------	--

<b>Output</b>	None on success, or error message
---------------	-----------------------------------

### 4.13.1 Imported Certified Attributes

The certificate object is created with the following attributes (which can be overwritten or extended by the attribute list `CertAttr`):

Attribute	Value
CKA_CLASS	CKO_CERTIFICATE
CKA_TOKEN	CK_TRUE
CKA_PRIVATE	CK_TRUE
CKA_CERTIFICATE_TYPE	CKC_X_509
CKA_LABEL	"X509 Certificate"
CKA_VALUE	Parsed value from file

Attribute	Value
CKA_SUBJECT	Parsed subject name from file if set or NULL

Table 4: Attributes of a X.509 certificate

### 4.13.2 Imported Private Key Attributes

The private key object is created with the following attributes (which can be overwritten or extended by the attribute list `PrvKeyAttr`):

RSA Private Key:

Attribute	Value
CKA_CLASS	CKO_PRIVATE_KEY
CKA_TOKEN	CK_TRUE
CKA_PRIVATE	CK_TRUE
CKA_SIGN	CK_TRUE
CKA_EXTRACTABLE	CK_TRUE
CKA_SENSITIVE	CK_TRUE
CKA_KEY_TYPE	CKK_RSA
CKA_LABEL	"RSA Private Key"
CKA_MODULUS	Parsed from file
CKA_PUBLIC_EXPONENT	Parsed from file
CKA_PRIVATE_EXPONENT	Parsed from file
CKA_PRIME_1	Parsed from file
CKA_PRIME_2	Parsed from file
CKA_COEFFICIENT	Parsed from file
CKA_EXPONENT_1	Parsed from file

Attribute	Value
CKA_EXPONENT_2	Parsed from file
CKA_SUBJECT	Parsed certificate subject name from file if set or NULL

Table 5: Attributes of an RSA private key

#### DSA Private Key:

Attribute	Value
CKA_CLASS	CKO_PRIVATE_KEY
CKA_TOKEN	CK_TRUE
CKA_PRIVATE	CK_TRUE
CKA_SIGN	CK_TRUE
CKA_EXTRACTABLE	CK_TRUE
CKA_SENSITIVE	CK_TRUE
CKA_KEY_TYPE	CKK_DSA
CKA_LABEL	"DSA Private Key"
CKA_PRIME	Parsed from file
CKA_SUBPRIME	Parsed from file
CKA_BASE	Parsed from file
CKA_VALUE	Parsed from file
CKA_SUBJECT	Parsed certificate subject name from file if set or NULL

Table 6: Attributes of a DSA private key

#### ECC Private Key:

Attribute	Value
CKA_CLASS	CKO_PRIVATE_KEY
CKA_TOKEN	CK_TRUE
CKA_PRIVATE	CK_TRUE

Attribute	Value
CKA_SIGN	CK_TRUE
CKA_EXTRACTABLE	CK_TRUE
CKA_SENSITIVE	CK_TRUE
CKA_KEY_TYPE	CKK_EC
CKA_LABEL	"ECC Private Key"
CKA_ECDSA_PARAMS	Parsed from file
CKA_VALUE	Parsed from file
CKA_SUBJECT	Parsed certificate subject name from file if set or NULL

Table 7: Attributes of an ECC private key

### 4.13.3 Imported Public Key Attributes

The public key object is created with the following attributes (which can be overwritten or extended by the attribute list `PubKeyAttr`):

**RSA Public Key:**

<i>Attribute</i>	<i>Value</i>
CKA_CLASS	CKO_PUBLIC_KEY
CKA_TOKEN	CK_TRUE
CKA_PRIVATE	CK_TRUE
CKA_VERIFY	CK_TRUE
CKA_KEY_TYPE	CKK_RSA
CKA_WRAP	CK_TRUE
CKA_LABEL	"RSA Public Key"
CKA_MODULUS	Parsed from file
CKA_PUBLIC_EXPONENT	Parsed from file

<i>Attribute</i>	<i>Value</i>
CKA_SUBJECT	Parsed certificate subject name from file if set or NULL

Table 8: Attributes of an RSA public key

**DSA Public Key:**

<b>Attribute</b>	<b>Value</b>
CKA_CLASS	CKO_PUBLIC_KEY
CKA_TOKEN	CK_TRUE
CKA_PRIVATE	CK_TRUE
CKA_VERIFY	CK_TRUE
CKA_KEY_TYPE	CKK_DSA
CKA_LABEL	"DSA Public Key"
CKA_PRIME	Parsed from file
CKA_SUBPRIME	Parsed from file
CKA_BASE	Parsed from file
CKA_VALUE	Parsed from file
CKA_SUBJECT	Parsed certificate subject name from file if set or NULL

Table 9: Attributes of a DSA public key

**ECC Public Key:**

<b>Attribute</b>	<b>Value</b>
CKA_CLASS	CKO_PUBLIC_KEY
CKA_TOKEN	CK_TRUE
CKA_PRIVATE	CK_TRUE
CKA_VERIFY	CK_TRUE
CKA_KEY_TYPE	CKK_EC

Attribute	Value
CKA_LABEL	"ECC Public Key"
CKA_ECDSA_PARAMS	Parsed from file
CKA_EC_POINT	Parsed from file
CKA_SUBJECT	Parsed certificate subject name from file if set or NULL

Table 10: Attributes of an ECC public key

--

### 4.14 ImportCert

This command imports an X.509 certificate and a public key from the given certificate file, using the OpenSSL library, and save them as private objects, using the PKCS#11 command `C_CreateObject`.

The objects' attributes can be overwritten and extended by the attribute list parameters.

<b>Syntax</b>	<code>p11tool2 [Slot=&lt;slot_id&gt;] LoginUser=&lt;user_pin&gt; [CertAttr=&lt;cert_attr&gt;] [PubKeyAttr=&lt;pub_key_attr&gt;] ImportCert=&lt;filename&gt;</code>
---------------	--

Parameter	Description
<slot_id>	ID of the slot as number (to open a session). Default: 0
<user_pin>	User PIN clear text or the string 'ask' if hidden PIN entry is preferred.
<cert_attr>	List of certificate attributes in format <attribute_name_1>=<value_1>,<attribute_name_2>= <value_2>,...
<pub_key_attr>	List of public key attributes in format <attribute_name_1>=<value_1>,<attribute_name_2>= <value_2>,...
<filename>	Name of the certificate file to be imported



**Example**

```
p11tool2 LoginUser=ask CertAttr=CKA_LABEL="My Cert",CKA_ID=ABC
PubKeyAttr=CKA_LABEL="My Public Key",CKA_ID=0x414243
ImportCert=C:/cert/x509.der
```

**Output**

None on success, or error message

The certificate object is created with the same attributes as for ImportP12.

## 4.15 ExportCert

This command writes the BER-encoding (attribute CKA\_VALUE) of the certificate object which is specified by the given label, ID and subject name to a file or to the standard output if no file name is set. The PKCS#11 commands like `C_FindObjects` and `C_GetAttributeValue` are used.

Note that at least one of the label, ID or subject name must be given in order to identify the certificate object.

**Syntax**

```
p11tool2 [Slot=<slot_id>] LoginUser=<user_pin> [Label=<label>]
[Id=<id>] [Subject=<subject>] [Force=<force>]
ExportCert[=<filename>]
```

Parameter	Description
<slot_id>	ID of the slot as number (to open a session). Default: 0
<user_pin>	User PIN in clear text or the string 'ask' if hidden PIN entry is preferred.
<label>	Label of the certificate object as string or as hexadecimal notation with "0x" prefix
<id>	ID of the certificate object as string or as hexadecimal notation with "0x" prefix
<subject>	certificate subject name as string or as hexadecimal notation with "0x" prefix
<force>	Boolean flag (0/1 or n/y) to overwrite file if already exists. Default: 0 (Cancel command if file already exists)
<filename>	Output file (default: standard output)

**Example**

```
p11tool2 LoginUser=ask Label="P12 Cert" Id="P12" ExportCert
```

Output	Certificate value:	
	CKA_VALUE	=
	0x3082026C 308201D5 A0030201 02020106	0 10
	300D0609 2A864886 F70D0101 05050030	0 * H 0
	2E310D30 0B060355 04031304 726F6F74	.1 0 U root
	310B3009 06035504 06130244 45311030	1 0 U DE1 0
	0E060355 040A1307 5574696D 61636F30	U Utimaco0
	1E170D30 34303130 31313230 3030305A	040101120000Z
	170D3037 30313031 31323030 30305A30	070101120000Z0
	32310B30 09060355 04061302 44453110	21 0 U DE1
	300E0603 55040A13 07557469 6D61636F	0 U Utimaco
	3111300F 06035504 03130873 63746573	1 0 U sctes
	74303130 819F300D 06092A86 4886F70D	t010 0 * H
	01010105 0003818D 00308189 02818100	0
	B8AC59FF 544BF8EA 4791300A 70B9420C	Y TK G 0 p B
	648DAA23 0BB1A5BA 71C8D5FD 094F728F	d # q Or
	F740393B 3BF0752D 16D06C5B 57E83555	@9;; u- l[W 5U
	E40EBB63 7B8BCC6B 6ADDD9F7 78A56AF5	c{ kj x j
	43AFB193 ED5E40E0 6E663A82 E5BB6FA3	C ^@ nf: o
	8D933445 15932465 C8977CAF E6865ED0	4E \$e   ^
	FE822B7D 8A287761 3F110EFF A9FAAF8E	+} (wa?
	3A293EA3 DC890996 5BA830FF 27BB350B	:.)> [ 0 ' 5
	02030100 01A38195 30819230 09060355	0 0 U
	1D130402 3000300E 0603551D 0F0101FF	0 0 U
	04040302 04B0301D 0603551D 0E041604	0 U
	14919DFD 50486F78 0FB51520 7C1CDCEC	PHox
	9B1F19FF 86305606 03551D23 044F304D	0V U # 00M
	80141309 CE05C9CE 632381DB B8DB65D1	c# e
	EFABAA84 34FFA132 A430302E 310D300B	4 2 00.1 0

```
06035504 03130472 6F6F7431 0B300906 | U    root1 0 |
03550406 13024445 3110300E 06035504 | U    DE1 0  U |
0A130755 74696D61 636F8201 01300D06 |  Utimaco  0 |
092A8648 86F70D01 01050500 03818100 | * H          |
66352161 049026CE 31E26F7A B2BA1B3E |f5!a  & 1 oz  >|
DD03E263 0879371A 91E6FF89 D5DD9316 |  c y7          |
8FCF4C98 B025B98D 7DACF7C8 66C0F73E |  L %  }    f  >|
25947245 9FF451BA C0B729B7 D9B88B94 |% rE  Q    )    |
FAF133B0 208A5FB9 BBFB7382 B8B209A0 |  3    _    s    |
B7C94ED3 62624BBC 7C6CEA84 337071D3 |  N bbK |l  3pq |
418025A1 19D0E90E 50A034E7 D00E76AD |A %      P 4    v |
B12A22EA 9E309CEE 3294CEA6 05CABF0A | *"   0  2          |
F7E4E701 00000000 03C70040 01000000 |              @    |
B8FD1200 00000000 F7E4E701 00000000 |              |
01000000 00000000 3045E801 00000000 |              0E    |
FEFFFFFF FFFFFFFF B07BE701 00000000 |              {    |
00000000 00000000 8094E701 00000000 |              |
7079E701 00000000 01000000 00000000 |py              |
80961C40 01000000 00000000 00000000 |    @              |
B8FD1200 00000000 F09EE701 00000000 |              |
B4AB6B01 00000000 5D8D0340 01000000 |  k      ]  @    |
00000000 00000000 02000000 00000000 |              |
F7E4E701 00000000 F7E4E701 F7E4E701 |              |
009BE701 00000000 009BE701 00000000 |              |
10FE1200 00000000 E09AE701 00000000 |              |
FEFFFFFF FFFFFFFF 68FE1200 00000000 |              h    |
00000000 00000000 00000000 00000000 |              |
00000000 00000000 0F000000 00000000 |              |
0F000000 00000000 0043493A 30000000 |              CI:0 |
```

	38010000	00000000	00000000	00000000	8		
	68FE1200	00000000	A7A80440	01000000	h	@	
	01000000	00000000	0079E701	00000000		y	
	00000000	00000000	00000000	00000000			
	0F000000	00000000	8DE70040	01000000		@	
	006C6F74	00000000	F06CE701	00000000	lot	1	
	00000000	00000000	0F000000	00000000			
	FEFFFFFF	FFFFFFFF	F0F45174	00000000		Qt	

4.16 ExportP10

This command exports a certificate request for a cryptographic key in ASN.1 encoded PKCS#10 format into a CSR file (certificate signing request).

Syntax	p11tool2 [Slot=<slot_id>] LoginUser=<user_pin> [PubKeyAttr=<pub_key_attr>] [PrvKeyAttr=<prv_key_attr>] [Mech=<mech>] [Config=<cfgfile>] [DN=<dn>] [Force=<force>] ExportP10=<filename>
--------	--

Parameter	Description
<slot_id>	ID of the slot as number (to open a session). Default: 0
<user_pin>	User PIN in clear text or the string ask if hidden PIN entry is preferred.
<pub_key_attr>	List of public key attributes in format <attribute_name_1>=<value_1>,<attribute_name_2>=<value_2>,...
<prv_key_attr>	List of private key attributes in format <attribute_name_1>=<value_1>,<attribute_name_2>=<value_2>,...
<mech>	Mechanism

Parameter	Description
<cfgfile>	<p>The absolute path and/or name of the distinguished name configuration file. If no path is specified, the file is searched in the current directory. Either the <code>Config</code> parameter or the <code>DN</code> parameter must be available. The following distinguished name fields are supported:</p> <ul style="list-style-type: none"> <li>▪ <code>commonName</code> Specifies an identifier of an object.</li> <li>▪ <code>serialNumber</code> Serial number of the distinguished name. Must be a hexadecimal value without a leading "0x" but with up to 40 digits.</li> <li>▪ <code>countryName</code> The ISO code consisting of two capital letters for the country where the organization is located, for example, <code>GB</code>, <code>FR</code> or <code>US</code>.</li> <li>▪ <code>localityName</code> Town or city</li> <li>▪ <code>stateOrProvinceName</code> Province, region, county or state, for example, <code>Sussex</code>, <code>Normandy</code> or <code>New Jersey</code>. Do not use abbreviations here.</li> <li>▪ <code>organizationName</code> Company name including suffixes such as <code>Inc.</code> or <code>Corp.</code></li> <li>▪ <code>organizationalUnitName</code> Department name, for example, <code>HR</code>, <code>Finance</code> or <code>IT</code></li> <li>▪ <code>title</code></li> <li>▪ <code>description</code></li> <li>▪ <code>emailAddress</code> An email address to contact the organization</li> </ul> <p>The order of the fields is irrelevant. At least one field must be available. Each field may be available several times.</p> <p>Example 1 of the contents of the configuration file:</p> <pre>commonName=1234_Key25 serialNumber=123 countryName=DE localityName=Aachen stateOrProvinceName=Rhineland organizationName=Utimaco IS GmbH organizationalUnitName=Support title=Support description=Test emailAddress=support@utimaco.com</pre> <p>Example 2:</p> <pre>organizationName=Utimaco IS GmbH CommonName=test</pre> <p>The following short distinguished names can be used:</p>

Parameter	Description
	CN: CommonName L: localityName C: countryName ST: stateOrProvinceName O: organizationName OU: organizationalUnitName  Example 3: O=Utimaco IS GmbH CN=test
<dn>	Sequence of distinguished name fields separated by a comma. Either the <code>Config</code> parameter or the <code>DN</code> parameter must be available. The description of the <code>&lt;cfgfile&gt;</code> parameter applies to the <code>&lt;dn&gt;</code> parameter in an analog way. If a distinguished name field value contains a blank, the complete DN value must be set in quotation marks. Example 1: DN="organizationName=Utimaco IS GmbH,CommonName=test"  Example 2 (with short distinguished names): DN="O=Utimaco IS GmbH,CN=test"
<force>	Boolean flag ( <code>0</code> / <code>1</code> or <code>n</code> / <code>y</code> ) to overwrite file if already exists. Default: <code>0</code> (Cancel command if file already exists)
<filename>	The absolute path and/or name of the certificate request file to be generated. The <code>&lt;force&gt;</code> parameter decides whether a file with this name is overwritten. If a path is specified, a filename must be specified as well. If no path is specified, the file is created in the current directory.

Example	p11tool2 LoginUser=123456 PubKeyAttr=CKA_LABEL="My RSA Public Key", CKA_ID=0x525341 PrvKeyAttr=CKA_LABEL="My RSA Private Key", CKA_ID=RSA Mech=CKM_SHA256_RSA_PKCS_PSS Config=my.cfg ExportP10=test.csr
---------	--

Output	Upon successful execution of the command, no output is given.  Example for the output if the output file already exists: Error: Command canceled. File test.csr already exists. Set parameter Force=1 (or y) in front of the command to overwrite this file.
--------	--

The result can be verified by using the `openssl` command.

Verifying the example:

```
openssl req -text -inform der -in test.csr | grep "Subject:"
```

## 4.17 GenerateKeyPair

This command generates a public/private key pair, using the PKCS#11 command `C_GenerateKeyPair`.

The key pair can be generated in two different ways:

- Key pair based on default attribute template
- Key pair from template file

### 4.17.1 Generate Key Pair Based on Default Attribute Template

A key pair with the given mechanism will be generated using default templates, which can be overwritten and extended by the attribute list parameters.

<b>Syntax</b>	<pre>p11tool2 [Slot=&lt;slot_id&gt;] LoginUser=&lt;user_pin&gt; [PubKeyAttr=&lt;pub_key_attr&gt;] [PrvKeyAttr=&lt;prv_key_attr&gt;] GenerateKeyPair=&lt;mech&gt;</pre>
---------------	--

<b>Example</b>	<pre>p11tool2 LoginUser=ask PubKeyAttr=CKA_LABEL="My RSA Public Key",CKA_ID=0x525341 PrvKeyAttr=CKA_LABEL="My RSA Private Key",CKA_ID=RSA GenerateKeyPair=RSA  p11tool2 Slot=1 LoginUser =212223 PubKeyAttr=CKA_LABEL="My ECC Public Key",CKA_ID=0x454343303032,CKA_EC_PARAMS="secp256r1" PrvKeyAttr=CKA_LABEL="new ECC priv002",CKA_ID=ECC generatekeypair=ECC</pre>
----------------	---

<b>Output</b>	None on success, or error message
---------------	-----------------------------------

Default RSA Public Key Template:

Attribute	Value
CKA_TOKEN	CK_TRUE
CKA_PRIVATE	CK_TRUE

Attribute	Value
CKA_VERIFY	CK_TRUE
CKA_ENCRYPT	CK_TRUE
CKA_WRAP	CK_TRUE
CKA_MODULUS_BITS	2048
CKA_PUBLIC_EXPONENT	0x010001
CKA_LABEL	"RSA Public Key"

Table 11: Default attribute values for an RSA public key

Default RSA Private Key Template:

Attribute	Value
CKA_TOKEN	CK_TRUE
CKA_PRIVATE	CK_TRUE
CKA_SENSITIVE	CK_TRUE
CKA_EXTRACTABLE	CK_TRUE
CKA_SIGN	CK_TRUE
CKA_DECRYPT	CK_TRUE
CKA_UNWRAP	CK_TRUE
CKA_LABEL	"RSA Private Key"

Table 12: Default attribute values for an RSA private key

Default ECC Public Key Template:

Attribute	Value
CKA_TOKEN	CK_TRUE
CKA_PRIVATE	CK_TRUE



Attribute	Value
CKA_VERIFY	CK_TRUE
CKA_EC_PARAMS	secp256r1
CKA_LABEL	"ECC Public Key"

Table 13: Default attribute values for an ECC public key

#### Default ECC Private Key Template:

Attribute	Value
CKA_TOKEN	CK_TRUE
CKA_PRIVATE	CK_TRUE
CKA_SENSITIVE	CK_TRUE
CKA_EXTRACTABLE	CK_TRUE
CKA_SIGN	CK_TRUE
CKA_LABEL	"ECC Private Key"

Table 14: Default attribute values for an ECC private key

### 4.17.2 Generate Key Pair from Template File

A key pair will be generated using the given template file.

<b>Syntax</b>	<code>p11tool2 [Slot=&lt;slot_id&gt;] LoginUser=&lt;user_pin&gt; GenerateKeyPair=&lt;template_file&gt;</code>
---------------	---

Parameter	Description
<slot_id>	ID of the slot as number (to open a session). Default:
<user_pin>	User PIN in clear text or the string 'ask' if hidden PIN entry is preferred.

Parameter	Description
<template_file>	Template file with sections [Mechanism], [PublicKey] and [PrivateKey]
Example	p11tool2 LoginUser=ask GenerateKeyPair=C:/rsa_keypair_template.txt
Output	None on success, or error message

Template File:

The template file must contain the following sections:

Section	Description
[Mechanism]	Contains only one variable: CK_MECHANISM_TYPE Example: CK_MECHANISM_TYPE = CKM_RSA_PKCS_KEY_PAIR_GEN
[PublicKey]	Contains public key attributes Example: CKA_TOKEN = CK_TRUE  CKA_LABEL = "RSA Public Key"  ...
[PrivateKey]	Contains private key attributes Example: CKA_TOKEN = CK_TRUE  CKA_LABEL = "RSA Private Key"  ...

Table 15: Sections of a template file for key pair generation

Example:

```
[Mechanism]

CK_MECHANISM_TYPE = CKM_RSA_PKCS_KEY_PAIR_GEN

[PublicKey]

CKA_TOKEN = CK_TRUE

CKA_PRIVATE = CK_TRUE
```

```
CKA_ENCRYPT = CK_TRUE
CKA_VERIFY = CK_TRUE
CKA_WRAP = CK_TRUE
CKA_MODULUS_BITS = 2048
CKA_PUBLIC_EXPONENT = 0x010001
CKA_LABEL = "My RSA Public Key"
CKA_ID = 0x525341
```

[PrivateKey]

```
CKA_TOKEN = CK_TRUE
CKA_PRIVATE = CK_TRUE
CKA_SENSITIVE = CK_TRUE
CKA_DECRYPT = CK_TRUE
CKA_EXTRACTABLE = CK_TRUE
CKA_SIGN = CK_TRUE
CKA_UNWRAP = CK_TRUE
CKA_LABEL = "My RSA Private Key"
CKA_ID = RSA
```

## 4.18 GenerateKey

This command generates a secret key or set of domain parameters, using the PKCS#11 command C\_GenerateKey.

The secret key can be generated in two different ways:

- Secret key based on default attribute template
- Secret key or domain parameters from template file.

### 4.18.1 Generate Secret Key Based on Default Attribute Template

A key pair with the given mechanism will be generated using default templates which can be overwritten and extended by the attribute list parameters.

<b>Syntax</b>	p11tool2 [Slot=<slot_id>] LoginUser=<user_pin> [KeyAttr=<key_attr>] GenerateKey=<mech>
---------------	---

<b>Parameter</b>	<b>Description</b>
<slot_id>	ID of the slot as number (to open a session). Default: 0
<user_pin>	User PIN in clear text or the string 'ask' if hidden PIN entry is preferred.
<key_attr>	Secret key attribute list of format <attribute_name_1>=<value_1>,<attribute_name_2>=<value_2>,...
<mech>	Mechanism type: AES   DES   DES2   DES3

<b>Example</b>	p11tool2 LoginUser=ask KeyAttr=CKA_LABEL="My AES Secret Key",CKA_ID=0x414553 GenerateKey=AES
----------------	---

<b>Output</b>	None on success, or error message
---------------	-----------------------------------

Default AES Key Template

<b>Attribute</b>	<b>Value</b>
CKA_TOKEN	CK_TRUE
CKA_PRIVATE	CK_TRUE
CKA_DECRYPT	CK_TRUE
CKA_SIGN	CK_TRUE
CKA_ENCRYPT	CK_TRUE
CKA_WRAP	2048
CKA_LABEL	"AES Secret Key"
CKA_VALUE_LEN	32

Table 16: Default attribute values for an AES key

Default DES Key Template

<i><b>Attribute</b></i>	<i><b>Value</b></i>
CKA_TOKEN	CK_TRUE
CKA_PRIVATE	CK_TRUE
CKA_DECRYPT	CK_TRUE
CKA_SIGN	CK_TRUE
CKA_ENCRYPT	CK_TRUE
CKA_WRAP	CK_TRUE
CKA_LABEL	"DES Secret Key"

Table 17: Default attribute values for an DES key

### Default DES 2 Key Template

<i><b>Attribute</b></i>	<i><b>Value</b></i>
CKA_TOKEN	CK_TRUE
CKA_PRIVATE	CK_TRUE
CKA_DECRYPT	CK_TRUE
CKA_SIGN	CK_TRUE
CKA_ENCRYPT	CK_TRUE
CKA_WRAP	CK_TRUE
CKA_LABEL	"DES2 Secret Key"

Table 18: Default attribute values for an DES2 key

### Default DES 2 Key Template

<i><b>Attribute</b></i>	<i><b>Value</b></i>
CKA_TOKEN	CK_TRUE
CKA_PRIVATE	CK_TRUE
CKA_DECRYPT	CK_TRUE
CKA_SIGN	CK_TRUE

Attribute	Value
CKA_ENCRYPT	CK_TRUE
CKA_WRAP	CK_TRUE
CKA_LABEL	"DES3 Secret Key"

Table 19: Default attribute values for an DES3 key

### 4.18.2 Generate Secret Key from Template File

A secret key or set of domain parameters will be generated using the given template file.

<b>Syntax</b>	p11tool2 [Slot=<slot_id>] LoginUser=<user_pin> GenerateKey=<template_file>
---------------	---

Parameter	Description
<slot_id>	ID of the slot as number (to open a session). Default: 0
<user_pin>	User PIN in clear text or the string 'ask' if hidden PIN entry is preferred.
<template_file>	Template file with sections [Mechanism] and [Key]

<b>Example</b>	p11tool2 LoginUser=123456 GenerateKey=C:/aes_key_template.txt
----------------	---

<b>Output</b>	None on success, or error message
---------------	-----------------------------------

#### Template File

The template file must contain the following sections:

Section	Description
[Mechanism]	Contains only one variable: CK_MECHANISM_TYPE Example: CK_MECHANISM_TYPE = CKM_AES_KEY_GEN

Section	Description
[Key]	Contains key attributes Example: CKA_CLASS=CKO_SECRET_KEY CKA_KEY_TYPE = CK_DES2CKK_AES CKA_LABEL = "RSA Public Key"

Table 20: Sections of a template file for the generation of secret key

### Example

```
[Mechanism]
CK_MECHANISM_TYPE = CKM_AES_KEY_GEN
[Key] CKA_CLASS = CKO_SECRET_KEY
CKA_KEY_TYPE = CKK_AES
CKA_TOKEN = CK_TRUE
CKA_PRIVATE = CK_TRUE
CKA_DECRYPT = CK_TRUE
CKA_SIGN = CK_TRUE
CKA_ENCRYPT = CK_TRUE
CKA_VERIFY = CK_TRUE
CKA_WRAP = CK_TRUE
CKA_VALUE_LEN = 32
CKA_LABEL = "My AES Secret Key"
CKA_ID = 0x414553
```

# 5 Configuration Commands

These configuration commands are proprietary and not part of PKCS#11. They only work with the PKCS#11 Library R3 which has vendor defined extensions.

The PKCS#11 Library R3 provides special PKCS#11 objects called the configuration objects:

- Local Configuration Object - used for configurations that affect the instance of the PKCS#11 API
- Global Configuration Object - used for configurations that affect the whole cHSM. These configuration objects can be modified by using the p11tool2 configuration command `SetGlobalConfig`.
- Slot Configuration Object - Used for configurations that affect the current slot. These configuration objects can be modified using the p11tool2 configuration command `SetSlotConfig`.

Changes on the attributes of the global and slot configuration objects are deleted on alarm occurrence. Therefore, we highly recommend to create a backup of the configuration objects:

- To back up the Slot Configuration Object, use the p11tool2 command `BackupConfig`.
- To back up the Global Configuration Object, use the csadm command `BackupDatabase` as described *BackupDatabase* in the [u.trust Anchor FIPS 140-3 - csadm Manual](#) or use the `BackupKey` function described in detail in the [u.trust Anchor FIPS 140-3 - cxitool Manual](#) so you can easily restore your global PKCS#11 configuration. To back up the global configuration objects, you need one User Administrator role (min. permission 2 in the user group 7, 20000000). To restore it, you need two User Administrator roles (summarized min. permission 4 in the user group 7, 40000000).

## 5.1 ListConfig

This command displays a list of all configuration attributes that are described in more detail in `SetGlobalConfig`.

<b>Syntax</b>	<code>p11tool2 ListConfig</code>
---------------	----------------------------------



**Example**

```
p11tool2 ListConfig
```

<b>Output</b>	a) Local Configuration Object:	
	Supported attributes	type:
	CKA_UTIMACO_CFG_PATH	<string>
	b) Global CryptoServer Configuration Object:	
	Supported attributes	type:
	CKA_CFG_ALLOW_SLOTS	<bool>
	CKA_CFG_CHECK_VALIDITY_PERIOD	<bool>
	CKA_CFG_AUTH_PLAIN_MASK	<unsigned integer (hex)>
	CKA_CFG_WRAP_POLICY	<bool>
	CKA_CFG_AUTH_KEYM_MASK	<unsigned integer (hex)>
	CKA_CFG_SECURE_DERIVATION	<bool>
	CKA_CFG_SECURE_IMPORT	<bool>
	CKA_CFG_SECURE_RSA_COMPONENTS	<bool>
	CKA_CFG_P11R3_BACKWARDS_COMPATIBLE	<bool>
	CKA_CFG_ENFORCE_BLINDING	<bool>
	CKA_CFG_SECURE_SLOT_BACKUP	<bool>

c) Slot CryptoServer Configuration Object:

Supported attributes	type:
CKA_CFG_CHECK_VALIDITY_PERIOD	<bool>
CKA_CFG_AUTH_PLAIN_MASK	<unsigned integer (hex)>
CKA_CFG_WRAP_POLICY	<bool>
CKA_CFG_AUTH_KEYM_MASK	<unsigned integer (hex)>
CKA_CFG_SECURE_DERIVATION	<bool>
CKA_CFG_SECURE_IMPORT	<bool>
CKA_CFG_SECURE_RSA_COMPONENTS	<bool>
CKA_CFG_P11R3_BACKWARDS_COMPATIBLE	<bool>
CKA_CFG_ENFORCE_BLINDING	<bool>
CKA_CFG_SECURE_SLOT_BACKUP	<bool>
CKA_CFG_SLOT_BACKUP_PASS_HASH	<string>

5.2 GetLocalConfig

This command displays the value of the local configuration object attribute with the given name.

<b>Syntax</b>	p11tool2 GetLocalConfig=<attribute>
---------------	-------------------------------------

Parameter	Description
<attribute>	Name of the local configuration attribute or '*' to get all local configuration attribute values

<b>Example</b>	p11tool2 GetLocalConfig=CKA_UTIMACO_CFG_PATH
----------------	--

<b>Output</b>	CKA_UTIMACO_CFG_PATH = C:\ProgramData\Utimaco\PKCS11_R3\cs_pkcs11_R3.cfg
---------------	--

### 5.3 GetGlobalConfig

This command displays the value of the global configuration object attribute with the given name.

<b>Syntax</b>	<code>p11tool2 [Slot=&lt;slot_id&gt;] &lt;login_command&gt; GetGlobalConfig=&lt;attribute&gt;</code>
---------------	--

<b>Parameter</b>	<b>Description</b>
<code>&lt;slot_id&gt;</code>	ID of the slot as number (to open a session). Default: 0
<code>&lt;login_command&gt;</code>	<ul style="list-style-type: none"><li>▪ Login as SO (via LoginSO) or</li><li>▪ Login as normal user (via LoginUser) or</li><li>▪ Login as administrator, key manager or key user (via Login)</li></ul>
<code>&lt;attribute&gt;</code>	Name of the global configuration attribute or '*' to get all global configuration attribute values; See SetGlobalConfig for the list of available attributes and values.

<b>Example</b>	<code>p11tool2 LoginUser=ask GetGlobalConfig=CKA_CFG_ALLOW_SLOTS</code>
----------------	---

<b>Output</b>	<code>CKA_CFG_ALLOW_SLOTS = CK_FALSE</code>
---------------	---

### 5.4 SetGlobalConfig

This command sets the value of the global configuration object attribute with the given name to the given value.

The execution of this command has an immediate effect. No restart of the device is needed.

<b>Syntax</b>	<code>p11tool2 [Slot=&lt;slot_id&gt;] Login=&lt;admin_name&gt;,&lt;admin_auth_token&gt; SetGlobalConfig=&lt;attribute&gt;,&lt;value&gt;</code>
---------------	--

Parameter	Description
<slot_id>	ID of the slot as number (to open a session). Default: 0
<admin_name>	Name of a u.trust Anchor cHSM administrator with permission mask 0x20000000
<admin_auth_token>	Authentication token of the u.trust Anchor cHSM administrator with <admin_name>: <ul style="list-style-type: none"> <li>▪ Case password-based authentication: Administrator password or string 'ask' if hidden password entry should be used.</li> <li>▪ Case signature-based authentication: Key specifier where the private part of the administrator key should be loaded from: <ul style="list-style-type: none"> <li>• Smartcard specifier, e.g., 'cs2:cjo:USB0' See <i>Authentication Mechanisms</i> in the u.trust Anchor FIPS 140-3 - Containerized Hardware Security Module (cHSM) - Administration Manual.</li> <li>• RSA signature authentication The PIN pad has to be connected to the computer where p11tool2 is running (USB port). Example: 'cs2:cjo:USB0@123.123.123.123/mypwd'</li> <li>• Keyfile[#password], e.g., 'my.key#pwd' If the keyfile is encrypted, hidden password entry is possible by entering string 'ask' as password.</li> </ul> </li> </ul>
<attribute>	Name of the global configuration attribute; see table below for the list of available attributes and values.
<value>	Value of the global configuration attribute to be set; see table below for the list of available global configuration attributes and possible values.

<b>Example</b>	p11tool2 Login=ADMIN,C:/keys/init_prv.key SetGlobalConfig=CKA_CFG_ALLOW_SLOTS,CK_TRUE
----------------	--

<b>Output</b>	none on success, or error message
---------------	-----------------------------------

The following table provides a list of all available configuration objects and their possible values.

Attribute	Description
CKA_CFG_ALLOW_SLOTS	This attribute enables the Security Officer (SO) to configure slots. Type: CK_BBOOL <ul style="list-style-type: none"> <li>▪ CK_TRUE - the Security Officer is permitted to configure slots.</li> <li>▪ CK_FALSE (default) - the Security Officer (SO) is not permitted to configure slots.</li> </ul>

Attribute	Description
CKA_CFG_CHECK_VALIDITY_PERIOD	<p>This attribute checks the validity period of the key. Type: CK_BBOOL The validity period of a key is only checked, if the following functions are to be performed using the key: C_SignInit (), C_EncryptInit (), C_DecryptInit (), C_DeriveInit (), C_WrapKey (), C_UnwrapKey () Possible values:</p> <ul style="list-style-type: none"> <li>CK_TRUE - the validity period of a key is checked, if the key has the attributes CKA_START_DATE and CKA_END_DATE.</li> <li>CK_FALSE (default) - the validity period of a key is not checked.</li> </ul>
CKA_CFG_AUTH_PLAIN_MASK	<p>This attribute defines the permissions required to import and export a key in plaintext. Type: CK_ULONG Default value: 0x00000002 - corresponds to the permissions of the Cryptographic User, who is already set up in the cHSM. <b>IMPORTANT:</b> If you change the default setting, you must also use the csadm administration tool to set up the corresponding user in your cHSM. This user must be assigned the permissions specified here. Examples for creating different users with csadm are provided in <i>AddUser</i> in the u.trust Anchor FIPS 140-3 - csadm Manual.</p>
CKA_CFG_WRAP_POLICY	<p>This attribute applies a key wrapping policy specifying how keys are encrypted so they can be securely exported outside the cHSM. Type: CK_BBOOL Possible values:</p> <ul style="list-style-type: none"> <li>CK_TRUE - a strong key (for example, 256-bit AES) cannot be encrypted with a weak key (for example, 1024-bit RSA).</li> <li>CK_FALSE (default) - a strong key can be encrypted with a weak key.</li> </ul>
CKA_CFG_AUTH_KEYM_MASK	<p>This attribute defines the minimum required authentication status of the key manager. Type: CK_ULONG</p> <ul style="list-style-type: none"> <li>0x00000020 (default value) The role is split into two roles, the key user and the key manager. Because this is always the case, this value cannot be changed. The steps in <a href="#">Separated Key Manager and Key User Role</a> must be performed.</li> <li>00000002 The key manager has the same permissions as the User (0000000200000002). This value cannot be applied.</li> </ul>

Attribute	Description
CKA_CFG_SECURE_DERIVATION	<p>This attribute prohibits the use of the following key derivation mechanisms, and prevents Reduced Key Space attacks:</p> <ul style="list-style-type: none"><li>▪ CKM_XOR_BASE_AND_DATA</li><li>▪ CKM_CONCATENATE_DATA_AND_BASE</li><li>▪ CKM_CONCATENATE_BASE_AND_DATA</li><li>▪ CKM_CONCATENATE_BASE_AND_KEY</li><li>▪ CKM_EXTRACT_KEY_FROM_KEY</li></ul> <p>For a detailed description of the mechanisms see PKCS #11 Cryptographic Token Interface Current Mechanisms Specification Version 2.40. Type: CK_BBOOL Possible values:</p> <ul style="list-style-type: none"><li>▪ CK_TRUE – none of the key derivation mechanisms listed above can be used by the function C_Derive ().</li><li>▪ CK_FALSE (default) – the key derivation mechanisms listed above can be used by the function C_Derive () for key derivation.</li></ul>
CKA_CFG_SECURE_IMPORT	<p>This attribute prevents simple Key Extraction attacks by performing additional strict checks on wrapping keys. Type: CK_BBOOL Possible values:</p> <ul style="list-style-type: none"><li>▪ CK_TRUE – the key wrapping and unwrapping functions perform additional strict checks on wrapping keys. For more details about the additional checks, see <i>Global CryptoServer Configuration Object</i> in the <a href="#">PKCS#11 R3 - Developer Guide</a>.</li><li>▪ CK_FALSE (default) – no additional strict checks on wrapping keys are performed.</li></ul>
CKA_CFG_SECURE_RSA_COMPONENTS	<p>This attribute applies restrictions on the length of the public exponent used for the generation of RSA keys. Type: CK_BBOOL Possible values:</p> <ul style="list-style-type: none"><li>▪ CK_TRUE (default) – new RSA keys cannot be created with very low, smaller than 0x10001, public exponents.</li><li>▪ CK_FALSE – new RSA keys can be created with very low public exponents.</li></ul>

Attribute	Description
CKA_CFG_P11R3_BACKWARDS_COMPATIBLE	<p>This attribute determines whether keys can be used by default as base keys for key derivation or not. Type: CK_BBOOL</p> <ul style="list-style-type: none"><li>▪ CK_TRUE – keys generated by using an ECC scheme or Diffie-Hellman algorithm can be used as base keys for key derivation (PKCS#11 standard non-compliant legacy); may be necessary for some integrations.</li><li>▪ CK_FALSE (default) – newly generated or imported keys cannot be used by default as base keys for key derivation.</li></ul>
CKA_CFG_ENFORCE_BLINDING	<p>This attribute prevents side-channel analysis (SCA) attacks by enabling/disabling cHSM-specific software measures for SCA resistance. These software measures imply changing the internal computations of RSA and ECC keys in a way that Simple and Differential Power Analysis (also referred to as SPA and DPA), Electro Magnetic Analysis (EMA) and Timing Analysis (TA) measurements on cryptographic keys do not reveal information any longer. However, the measures for SCA resistance negatively affect the performance of the cryptographic operations on RSA and ECDSA keys. Therefore, they are disabled by default, and can be enabled, if necessary. Type: CK_BBOOL</p> <ul style="list-style-type: none"><li>▪ CK_TRUE – software measures for SCA resistance are used for cryptographic operations on RSA and ECDSA keys.</li><li>▪ CK_FALSE (default) – normal (without software measures for SCA resistance) cryptographic operations on RSA and ECDSA keys are used.</li></ul>




Attribute	Description
CKA_CFG_SECURE_SLOT_BACKUP	<p>This attribute enforces the usage of an individual backup key (Tenant Backup Key, TBK) per slot instead of the MBK to protect key backups. By default, only MBK-protected external key storage and key backup is enabled.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>CK_TRUE – use slot-individual backup keys (TBKs) derived from the cHSM's MBK to encrypt key backups.</li> <li>CK_FALSE (default) – use the cHSM's MBK to encrypt key backups.</li> </ul> <p>Make sure you have set this configuration attribute according to your security policy before your cHSM production environment gets operational.</p> <p>It is optional, but recommended, to use a passphrase for the derivation of a slot-individual backup key. This is done by setting the CKA_CFG_SLOT_BACKUP_HASH_PASS configuration attribute.</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;">  If you use the CKA_CFG_SLOT_BACKUP_HASH_PASS configuration attribute, make sure you have set it before you set the CKA_CFG_SECURE_SLOT_BACKUP configuration attribute, see (1.0.6) 2021-0072 SecureSlotPass (GPCC). </div>

Table 21: List of global configuration attributes

## 5.5 GetSlotConfig



See the table in [SetSlotConfig](#) for the list of available attributes and values.

This command displays the value of the slot configuration object attribute with the given name.

<b>Syntax</b>	<pre>p11tool2 [Slot=&lt;slot_id&gt;] &lt;login_command&gt; GetSlotConfig=&lt;attribute&gt;</pre>
---------------	--

Parameter	Description
<slot_id>	ID of the slot as number (to open a session). Default: 0

Parameter	Description
<login_command>	<ul style="list-style-type: none"><li>▪ Login as SO (via <code>LoginSO</code>) or</li><li>▪ Login as normal user (via <code>LoginUser</code>)</li><li>▪ Login as key manager or key user (via <code>Login</code>)</li></ul>
<attribute>	Name of the slot configuration attribute or '*' to get all slot configuration attribute values.

Example	p11tool2 LoginUser=ask GetSlotConfig=CKA_CFG_WRAP_POLICY
---------	--

Output	CKA_CFG_WRAP_POLICY = CK_FALSE
--------	--------------------------------

## 5.6 SetSlotConfig



See the table in [SetSlotConfig](#) for the list of available attributes and values.

This command sets the value of the slot configuration object attribute with the given name to the given value.

The execution of this command has an immediate effect. No restart of the device is needed.



The global configuration object attribute `CKA_CFG_ALLOW_SLOTS` must be set to `CK_TRUE`.

Only a Security Officer is allowed to change the attributes of the slot configuration object. These attributes are the same as for the global configuration object, except for the `CKA_CFG_ALLOW_SLOTS` attribute.

Syntax	p11tool2 [Slot=<slot_id>] LoginSO=<so_pin> SetSlotConfig=<attribute>,<value>
--------	--

Parameter	Description
<slot_id>	ID of the slot as number (to open a session). Default: 0
<so_pin>	SO PIN in clear text or string 'ask' if hidden PIN entry is preferred.
<attribute>	Name of the slot configuration attribute
<value>	Value of the slot configuration attribute to be set

<b>Example</b>	p11tool2 LoginSO=ask SetSlotConfig=CKA_CFG_WRAP_POLICY,CK_TRUE
----------------	--

<b>Output</b>	None on success, or error message
---------------	-----------------------------------

## 5.7 SecureSlotPass

This command sets the optional, but recommended, passphrase to be used for the derivation of a slot-individual backup key as the `CKA_CFG_SLOT_BACKUP_HASH_PASS` slot configuration attribute.

The execution of this command has an immediate effect. No restart of the device is needed.



The slot-individual backup key is not used by default, but only if the `CKA_CFG_SECURE_SLOT_BACKUP` configuration attribute is set to `CK_TRUE`. It is very important to first set the required passphrase ( `CKA_CFG_SLOT_BACKUP_PASS_HASH` ) and then enable the device to use slot-individual backup keys for protecting key backups created with P11CAT and p11tool2.



Changing the `CKA_CFG_SLOT_BACKUP_PASS_HASH` configuration attribute for a slot that is currently in use causes previously generated external key databases and their key backups to become inaccessible.



The `CKA_CFG_SLOT_BACKUP_HASH_PASS` configuration attribute can be set up independently from the configuration of the `CKA_CFG_ALLOW_SLOTS` attribute.

Only a Security Officer is allowed to change the attributes of the slot configuration object. The specified passphrase is only used if the `CKA_CFG_SECURE_SLOT_BACKUP` attribute is set to `CK_TRUE`.

<b>Syntax</b>	<code>p11tool2 [Slot=&lt;slot_id&gt;] LoginSO=&lt;so_pin&gt; SecureSlotPass=&lt;passphrase&gt;</code>
---------------	---

Parameter	Description
<slot_id>	ID of the slot as number (to open a session). Default:
<so_pin>	SO PIN in clear text or the string 'ask' if hidden PIN entry is preferred.
<passphrase>	A passphrase string to be used for the derivation of the slot-individual backup key that is used for protecting key backups. For a hidden passphrase entry, enter the string 'ask' instead of the passphrase in clear text.

<b>Example</b>	<code>p11tool2 Slot=1 LoginSO=ask SecureSlotPass=ask</code>
----------------	---

<b>Output</b>	None on success, or error message
---------------	-----------------------------------

To remove the currently used passphrase, enter an empty passphrase string, e.g.:

`p11tool2 Slot=1 LoginSO=ask SecureSlotPass=`

### 5.8 Separated Key Manager and Key User Role

In PKCS#11 the USER has, by default, the permissions/tasks to manage keys (create, delete, import, export, etc.) and to use them in cryptographic operations. These tasks can also be split into two groups and assigned to different PKCS#11 users:

- Key manager (KM) with permission mask 00000020 to manage cryptographic keys
- Key user (KU) with the permission mask 00000002 to use cryptographic keys.

Splitting the key manager and the key user into two separate roles can be achieved by setting the global or local configuration object `CKA_CFG_AUTH_KEYM_MASK`, `SetGlobalConfig`.

Initialize the slot as usual using `p11tool2`, see [InitToken](#), or `P11CAT`, see *Setting up a Slot (Init Token)* in the [CryptoServer – PKCS#11 P11CAT Manual](#).

However, the key manager and the key user have to be created manually. For example, perform these steps for slot 1 to do so:

1. Create a key manager (user KM\_0001) with the permission mask 0000020 and the attribute CXI\_GROUP=SLOT\_0001. This command requires authentication by a user with the user administrator role (minimum permissions 20000000). This key manager must be created out of the scope of the CryptoServer PKCS#11 API and tools with the CHSM's administration tools csadm.

Example:

```
csadm Dev=3001@127.0.0.1 LogonSign=ADMIN,:cs2:cjo:USB0  
AddUser=KM_0001,00000020{CXI_GROUP=SLOT_0001},hmacpwd,123456
```

For details on how to create a user, see *AddUser* in the [u.trust Anchor FIPS 140-3 – csadm - Manual](#).

2. Perform the analog step to create the USR\_0001 user of slot 1.

Example:

```
csadm Dev=3001@127.0.0.1 LogonSign=ADMIN,:cs2:cjo:USB0  
AddUser=USR_0001,00000002{CXI_GROUP=SLOT_0001},hmacpwd,123456
```



Do not initialize the slot PIN using p11tool2 or P11CAT. The "Init PIN" step would create a USR\_000<x> user with the permission mask of a key manager and a key user (00000022) instead of the permission mask of a key user (00000002).



Now the key manager can log in as user KM\_0001 with the C\_Login function and user type CKU\_CS\_GENERIC, see Login, to perform key management functions. The key user can log in as usual with user type CKU\_USER.

## 6 Backup/Restore Commands

These backup/restore commands are proprietary and not part of the PKCS#11 standard. They only work with the PKCS#11 Library R3 which has vendor defined extensions. For further information, see *Vendor Defined PKCS#11 Extensions* in the [PKCS#11 R3 - Developer Guide](#) provided within the product bundle at `\Documentation\Crypto_APIS\PKCS11_R3.`

If you use a u.trust Anchor for a special certification, such as FIPS or Common Criteria, the needed authentication status might differ. See the documentations for the certified u.trust Anchor for more details.

### 6.1 GetBackupInfo

This command displays information about the given backup file.

<b>Syntax</b>	<code>p11tool2 GetBackupInfo=&lt;filename&gt;</code>
---------------	--

<b>Parameter</b>	<b>Description</b>
<code>&lt;filename&gt;</code>	Name of the backup file

<b>Example</b>	<code>p11tool2 GetBackupInfo=C:/backup/internal_keys.bak</code>
----------------	---

<b>Output</b>	<pre>BACKUP_INFO: File version      : 2 Creation date     : 20130327 144454 Slot ID          : 0x00000000 Slot Description  : CryptoServer Device 'PCI:0' - SLOT_0000 Object count      : 16 internal key(s)</pre>
---------------	--

### 6.2 BackupInternalKeys

This command backs up all available internal keys within a PKCS#11 slot.



Perform the `csadm MBKListKeys` command to determine which Master Backup Key (MBK) is currently in use in MBK slot 3 by the CHSM. This MBK is used by the `p11tool2 BackupInternalKeys` command to encrypt the backup file to be generated. If the MBK in MBK slot 3 is the autogenerated MBK named `AUTO-GEN`, the `p11tool2 BackupInternalKeys` command cannot be performed. Import a different MBK into MBK slot 3 using the `csadm MBKImportKey` command.

It is important to note down which MBK has been used because for a successful restoring of this backup file at a later date it is necessary that the same MBK is in MBK slot 3 or after an MBK rollover in an MBK slot  $\geq 3$ .

Otherwise, the backup file is inaccessible. This might be the result of the execution of a `csadm MBKImportKey` command.

It is not possible to retrieve the MBK by which a backup file has been generated from this backup file.

<b>Syntax</b>	<code>p11tool2 [Slot=&lt;slot_id&gt;] [Force=&lt;force&gt;] &lt;login_key_manager&gt; BackupInternalKeys=&lt;filename&gt;</code>
---------------	--

Parameter	Description
<slot_id>	ID of the PKCS#11 slot as number Default: 0
<force>	Boolean flag (0/1 or n/y) to overwrite file if already exists. Default: 0 (Cancel command if file already exists)
<login_key_manager>	Login as key manager (via Login). Note: By default the key manager and the key user have the same permission mask. In that case the normal user can also be logged in (via LoginUser).
<filename>	Name of the key backup file to be created

<b>Example</b>	<code>p11tool2 Slot=1 Login=keyM,ask BackupInternalKeys=C:/backup/internal_keys_p11slot1.bak</code>
----------------	---

<b>Output</b>	16 internal key(s) backed up
---------------	------------------------------

## 6.3 BackupExternalKeys

This command backs up all available external keys within a PKCS#11 slot.



Perform the `csadm MBKListKeys` command to determine which Master Backup Key (MBK) is currently in use in MBK slot 3 by the CryptoServer. This MBK is used by the `p11tool2 BackupExternalKey s` command to encrypt the backup file to be generated. If the MBK in MBK slot 3 is the autogenerated MBK named `AUTO-GEN`, the `p11tool2 BackupExternalKey s` command cannot be performed. Import a different MBK into MBK slot 3 using the `csadm MBKImportKey` command described in the u.trust Anchor - csadm Manual.

It is important to note down which MBK has been used because for a successful restoring of this backup file at a later date it is necessary that the same MBK is in MBK slot 3 or after an MBK rollover in an MBK slot  $\geq 3$ .

Otherwise, the backup file is inaccessible. This might be the result of the execution of a `csadm MBKImportKey` command., see *Master Backup Key Rollover* in the u.trust Anchor - csadm Manual for details.

It is not possible to retrieve the MBK by which a backup file has been generated from this backup file.

<b>Syntax</b>	<code>p11tool2 [Slot=&lt;slot_id&gt;] [Force=&lt;force&gt;] &lt;login_key_manager&gt; BackupExternalKeys=&lt;filename&gt;</code>
---------------	--

Parameter	Description
<slot_id>	ID of the PKCS#11 slot as number Default: 0
<force>	Boolean flag (0/1 or n/y) to overwrite file if already exists. Default: 0 (Cancel command if file already exists)
<login_key_manager>	Login as key manager (via Login). NOTE: By default, the key manager and the key user have the same permission mask. In that case, the normal user can also be logged in (via LoginUser).
<filename>	Name of the key backup file to be created

<b>Example</b>	<code>p11tool2 Slot=1 Login=keyM,ask BackupExternalKeys=C:/backup/external_keys_p11slot1.bak</code>
----------------	---

<b>Output</b>	<code>2 external key(s) backed up</code>
---------------	--



## 6.4 BackupConfig

This command backs up the PKCS#11 slot configuration object.



Perform the `csadm MBKListKeys` command to determine which Master Backup Key (MBK) is currently in use in MBK slot 3 by the chSM. This MBK is used by the `p11tool2 BackupConfig` command to encrypt the backup file to be generated.

It is important to note down which MBK has been used because for a successful restoring of this backup file at a later date it is necessary that the same MBK is in MBK slot 3 or after an MBK rollover in an MBK slot  $\geq 3$ .

Otherwise, the backup file is inaccessible. This might be the result of the execution of a `csadm MBKImportKey` command.

It is not possible to retrieve the MBK by which a backup file has been generated from this backup file.

<b>Syntax</b>	<code>p11tool2 [Slot=&lt;slot_id&gt;] [Force=&lt;force&gt;] LoginSO=&lt;so_pin&gt; BackupConfig=&lt;filename&gt;</code>
---------------	---

Parameter	Description
<slot_id>	ID of the slot as number Default: 0
<force>	Boolean flag (0/1 or n/y) to overwrite file if already exists. Default: 0 (Cancel command if file already exists)
<so_pin>	SO PIN or string 'ask' if hidden PIN entry should be used.
<filename>	Name of the configuration backup file to be created

<b>Example</b>	<code>p11tool2 Slot=1 LoginSO=ask BackupConfig=C:/backup/config.bak</code>
----------------	--

<b>Output</b>	Slot configuration object backed up
---------------	-------------------------------------

## 6.5 RestoreInternalKeys

This command restores all keys from the given key backup file to the internal key store.

<b>Syntax</b>	p11tool2 [Slot=<slot_id>] <login_key_manager> RestoreInternalKeys=<filename>
---------------	---

Parameter	Description
<slot_id>	ID of the slot as number Default: 0
<login_key_manager>	Login as key manager (via Login). Note: By default the key manager and the key user have the same permission mask. In that case the normal user can also be logged in (via LoginUser).
<filename>	Name of a previously generated key backup file

<b>Example</b>	p11tool2 Slot=1 Login=keyM,ask Login=keyM2,ask RestoreInternalKeys=C:/backup/internal_keys.bak
----------------	---

<b>Output</b>	16 internal keys restored to internal key store
---------------	---

## 6.6 RestoreExternalKeys

This command restores all keys from the given key backup file to the external key store.

<b>Syntax</b>	p11tool2 [Slot=<slot_id>] <login_key_manager> RestoreExternalKeys=<filename>
---------------	---

Parameter	Description
<slot_id>	ID of the slot as number Default: 0
<login_key_manager>	Login as key manager (via Login). NOTE: By default the key manager and the key user have the same permission mask. In that case the normal user can also be logged in (via LoginUser).
<filename>	Name of a previously generated key backup file

<b>Example</b>	p11tool2 Slot=1 Login=keyM,ask RestoreExternalKeys=C:/backup/ external_keys.bak
----------------	--

<b>Output</b>	2 external keys restored to external key store
---------------	--

## 6.7 RestoreConfig

This command restores the slot configuration object from the given configuration backup file.

<b>Syntax</b>	p11tool2 [Slot=<slot_id>] LoginSO=<so_pin> RestoreConfig=<filename>
---------------	--

Parameter	Description
<slot_id>	ID of the slot as number Default: 0
<so_pin>	SO PIN or string 'ask' if hidden PIN entry should be used.
<filename>	Name of a previously generated configuration backup file

<b>Example</b>	p11tool2 Slot=1 LoginSO=ask RestoreConfig=C:/backup/config.bak
----------------	--

<b>Output</b>	slot configuration object restored
---------------	------------------------------------

## 6.8 DeleteSO

This command deletes the SO (security officer).

<b>Syntax</b>	p11tool2 [Slot=<slot_id>] Login=<admin_name>,<admin_auth_token> DeleteSO
---------------	---

Parameter	Description
<slot_id>	ID of the slot as number Default: 0
<admin_name>	Name of a CHSM administrator with permission mask 0x20000000

Parameter	Description
<admin_auth_token>	<p>Authentication token of the cHSM administrator with &lt;admin_name&gt;:</p> <ul style="list-style-type: none"><li>▪ Case password-based authentication: Administrator password or string 'ask' if hidden password entry should be used.</li><li>▪ Case signature-based authentication: Key specifier where the private part of the administrator key should be loaded from:<ul style="list-style-type: none"><li>• Smartcard specifier, e.g., 'cs2:cjo:USB0'</li></ul></li></ul> <p>See <i>Authentication Mechanisms</i> in the <a href="#">u.trust Anchor FIPS 140-3 - Containerized Hardware Security Module (cHSM) - Administration Manual</a>.</p> <li>• keyfile[#password], e.g., 'my.key#pwd'</li> <p>If the keyfile is encrypted, hidden password entry is possible by entering string 'ask' as password.</p>
Example	<pre>p11tool2 Slot=1 Login=ADMIN,"C:\Program Files\Utimaco\SecurityServer\Administration\ADMIN.key" DeleteSO</pre>
Output	None on success, or error message

## 6.9 RecryptExternalKeys

This command is used when an MBK rollover is performed, see *Master Backup Key Rollover* [u.trust Anchor - cHSM - Administration Manual](#). The `p11tool2 RecryptExternalKeys` command creates a backup with the specified filename and recrypts all available external cryptographic keys within the slot with the current MBK.




The `p11tool2 RecryptExternalKeys` command only recrypts external cryptographic keys if the old MBK and the new MBK are AES MBKs.

The `p11tool2 RecryptExternalKeys` command must be performed for each PKCS#11 slot containing cryptographic keys.

The `p11tool2 RecryptExternalKeys` command is proprietary and only works with PKCS#11 library R3.

<b>Syntax</b>	<code>p11tool2 [Slot=&lt;slot_id&gt;] [Force=&lt;force&gt;] &lt;login_key_manager&gt; RecryptExternalKeys=&lt;filename&gt;</code>
---------------	---

Parameter	Description
<slot_id>	ID of the PKCS#11 slot as number <u>Default:</u> 0 The PKCS#11 slot number must not be confused with the MBK slot number.
<force>	Boolean flag (0/1 or n/y) to overwrite file if already exists. <u>Default:</u> 0 (Cancel command if file already exists)
<login_key_manager>	Login as key manager (via Login). <div> By default the key manager and the key user have the same permission mask. In that case the normal user can also be logged in (via LoginUser).</div>
<filename>	Name of the key backup file to be created

<b>Example</b>	Back up all keys being available in PKCS#11 slot 1 and recrypt them with the current MBK. The USR_0000 user is also a key manager. <code>p11tool2 Slot=1 Login=USR_0000,123456 RecryptExternalKeys=p11.pks.bak</code>
----------------	--

<b>Output</b>	Example: 5 external key(s) backed up 5 external key(s) recrypted Or error message
---------------	--

## 7 Contact Address for Support Queries

You can reach us from Monday to Friday, 09.00 a.m. to 05.00 p.m., Central European Time (CET).

Utimaco IS GmbH  
Germanusstr. 4  
52080 Aachen  
Germany

### RMA Query

If you need to send the device back to Utimaco IS GmbH, please open a new RMA case (Return Merchandise Authorization). We request that you use the following web address. RMA cases cannot be opened by email or phone.

<https://support.hsm.utimaco.com/support/rma/new>

### Other Support Queries

- Mail (preferred contact method)  
[support@utimaco.com](mailto:support@utimaco.com)  
Attach the diagnostic information to your email.
- Web portal  
<https://support.hsm.utimaco.com/support/cases/new/>  
The diagnostic information will be requested in our response if necessary.
- By phone  
AMERICAS +1-844-UTIMACO (+1 844-884-6226)  
EMEA +49 800-627-3081  
APAC +81 800-919-1301  
The diagnostic information will be requested in our response if necessary.

## 8 References

Title/Company	Document No.
u.trust Anchor FIPS 140-3 - csadm - Manual/Utlimaco IS GmbH.	2023-0037
u.trust Anchor FIPS 140-3 - Containerized Hardware Security Module (cHSM) - Administration Manual /Utlimaco IS GmbH.	2023-0028
u.trust Anchor FIPS 140-3 - cxitool Manual	2024-0012
CryptoServer - PKCS#11 P11CAT - Manual /Utlimaco IS GmbH.	M013-0001-en
PKCS#11 R3 - Developer Guide/Utlimaco IS GmbH.	2012-0007
"PKCS #11 Cryptographic Token Interface Current Mechanisms Specification Version 2.40," Committee Specification 01, September 16, 2014/OASIS Standard. Available: <a href="http://docs.oasis-open.org/pkcs11/pkcs11-curr/v2.40/cs01/pkcs11-curr-v2.40-cs01.html">http://docs.oasis-open.org/pkcs11/pkcs11-curr/v2.40/cs01/pkcs11-curr-v2.40-cs01.html</a>	