# KEY CUSTODIAN MANUAL

Software Version 2.1.3

The specifications and information regarding the product in this manual are subject to change without prior notice. All statements, information, and recommendations in this manual are believed to be accurate but are presented without warranty of any kind, expressed or implied. Users must take full responsibility for their use of any products.

The software license and limited warranty for the accompanying product are set forth in the information packet that shipped with the product or was included in the contract between the parties and are incorporated herein by this reference. If you are unable to locate the software license or limited warranty, contact your Verisec representative for a copy.

Chiave Key Custodian Manual

# TABLE OF CONTENTS

ABBREVIATIONS ........ 5

TYPOGRAPHICAL CONVENTIONS ........ 6

INTRODUCTION ........ 7

Support ........ 7

BEFORE YOU BEGIN ........ 8

INTRODUCTION ........ 9

At a Glance ........ 9
Password ........ 9
Key Management Overview ........ 10
Key Types ........ 11
Keys ........ 13
Key variants ........ 13
Systems ........ 15
System groups ........ 16
Users ........ 16
User groups ........ 18
General on Import/Export restrictions ........ 19
Import/Export formats ........ 20
Component set ........ 20
JKS ........ 20
PKCS#12 ........ 20
XML ........ 21
Screen ........ 21
PREP ........ 22
TMS ........ 23
Atos ........ 23
Import/export format restrictions ........ 24
Dual control ........ 26

CONFIGURING KEY MANAGEMENT ........ 28

Configuring key types ........ 28
Configuring key variants ........ 33
Configuring system groups ........ 34

Configuring systems ........ 36

WORKING WITH KEYS ........ 38

My Keys ........ 38
Generating a new key ........ 39
Exporting a key ........ 42
Component set ........ 43
Password-protected file ........ 44
Encrypted under a transport key ........ 45
Importing a key ........ 45
Component set ........ 47
Password-protected file ........ 48
Encrypted under a transport key ........ 48
Retiring a key ........ 49
Deleting a key ........ 50

WORKING WITH TEMPLATES ........ 52

About templates ........ 52
Configuring templates ........ 53
Applying templates ........ 57

REPORTS ........ 59

APPENDIX A – KEY FORMAT SAMPLES ........ 60

# ABBREVIATIONS

| | |
|---|---|
| 2FA | Two-factor authentication |
| CKEK | Card Key Encryption Key |
| DST | Daylight Saving Time |
| FDQN | Fully Qualified Domain Name |
| HOTP | Event-Based OATH Tokens |
| ICT | Information and Communication Technology |
| LAN | Local Area Network |
| LMK | Local Master Key |
| NIC | Network Interface Card |
| NTP | Network Time Protocol |
| OATH | Open Authentication |
| OTP | One-Time Password |
| PKCS | Public Key Cryptography Standard |
| PSKC | Portable Symmetric Key Container |
| SNMP | Simple Network Management Protocol |
| TOTP | Time-Based OATH Tokens |

# Typographical Conventions

| | |
|---|---|
| **Text entered in bold** | Refers to menu options in Chiave (left hand pane). |
| **NOTE!** | Refers to sections that contain background information or information pertinent to other sections. |
| ***Warning!*** | Refers to cases where we point out issues that you need to take extra care about. |
| **Information Box** | Refers to information we would like to highlight. |
| `Constant width` | Refers to text entered by the admin verbatim. |

# INTRODUCTION

Thank you for purchasing Chiave Key Management appliance.

The intended reader of this manual is a Key Custodian with the need to define a model of key usage and/or to perform operational key tasks such as key generation, import, export, retirement or deletion.

In essence, Chiave Key Management is a web-based appliance which provides centralized storage and generation of cryptographic keys and a secure way to import and export them in a variety of formats. In addition, it contains a model of usage intended for each physical or logical system that employs the keys, making it easier to keep track of them once they are put to operational use.

Apart from relying on encryption and strong authentication to prevent unauthorized access, an important aspect of key management with Chiave is the notion of dual control. Sensitive operations cannot be performed on the appliance unless controlled by two users or more, depending on the type of action. Given that many of the previously paper-based processes are now automated, all this significantly reduces the possibility of human error.

## Support

For Chiave support, please contact us using one of the following options:

- UK phone (toll-free): 0800 917 8815
- Global Support number: +46 8 696 9999
- e-mail support@verisec.com
- http://www.verisec.com/en/support

# BEFORE YOU BEGIN

Before you start reading the manual, it is advisable you go through the checklist below to make sure you can login to a Chiave Key Management application within your organisation:

□ Obtain the URL required to access the Key Management application on one of the Chiave appliances in your organisation. In general, this URL will be in the form of https://XXXXXX:8443/ChiaveKeyManagement where XXXXXX is the FQDN or IP address of the key management interface of the Chiave appliance you will be accessing

□ Obtain a username and password from the administrator who has set up your account.

□ Collect an OTP token from the person responsible for giving out tokens within your organisation.

□ Collect an OSC smartcard from the person responsible for giving out smartcards within your organisation.

Having ensured the above, you can log in to the Key Management application. Contact an administrator in case there are any problems with accessing the application.

CHAPTER 1

# INTRODUCTION

This chapter describes the layout of the Key Management application and the main concepts that the processes of key management revolve around.

The chapter is divided as follows:

| | |
|---|---|
| At a glance (1) | Describes the layout of the application |
| Key Management Overview (2) | Describes the basic concepts of key management with Chiave. |
| Dual control (3) | Describes the notion of dual control and how it applies to different types of operations |

## At a Glance

Chiave Key Management is a web-based application for managing key instances. Since using Chiave appliance entails working with sensitive information, there are certain limitations on how it can be accessed.

For security reasons, the application should be used from a single browser tab.

Each user session on Chiave key management application is limited to the period of fifteen minutes after any interaction with the application – for instance, logging in, switching to another page in the application, etc. The timer, visible in the top-right corner of the screen, is reset each time any action is performed. After the set period has elapsed, the user will be logged out automatically.

***Warning! Despite the security measures built in the application, it is nevertheless of the utmost importance that you log out explicitly each time before leaving the computer.***

### Password

To change your password:

**Go to Password**

**a.** Enter the old password.

**b.** Enter the one you wish to replace it with. Note that the new password will need to comply with Chiave's password policy if one has been configured.

**c.** Re-enter the new password.

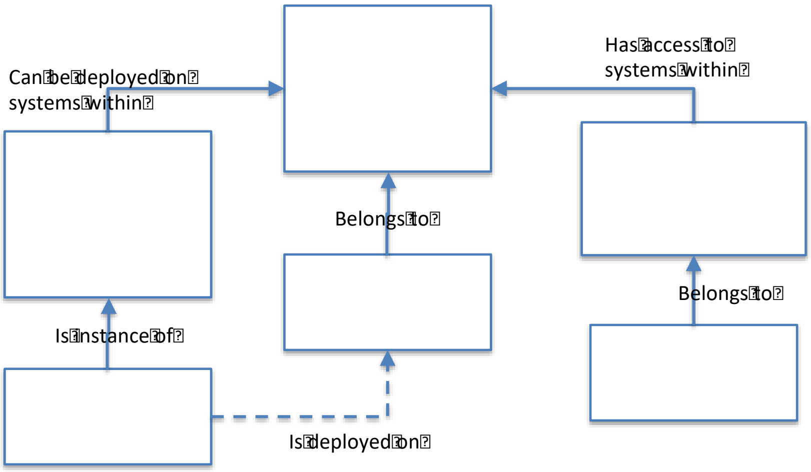
**d.** Click **Apply**.

**NOTE!** A Key Custodian's password can also be changed by an administrator. Should this be the case, when you next log in you will be prompted to set a different one before accessing the rest of the application.

# Key Management Overview

Key management in Chiave revolves around three types of entities: key types, systems and system groups, users and user groups. In very broad terms one can say that key types describe keys that can be used on systems within a system group which, in turn, can be accessed by Key Custodians associated with user groups.

**NOTE!** Each type of entities that constitute the structure of key management corresponds to a separate tab in the application. However, access to them is divided among different users. Key types, system groups and systems are visible only to Key Custodians with the privilege Manage Model. User groups and users, on the other hand, are managed through the Administration application.


Can be deployed on systems within
Has access to systems within
Belongs to
Belongs to
Is instance of
Is deployed on

## Key Types

A key type in Chiave encapsulates information about keys that can be deployed on systems. Over and above the obvious properties such as the cryptographic algorithm and key length, a key type contains information about the intended lifetime of key instances, acceptable transport formats and key usage.
Key types are associated with system groups i.e. sets of related systems (for example, servers, HSMs, or other consumers of cryptographic keys) that are somehow related and which use the same type of keys.

Key types may be regarded as “cookie templates” for producing key instances. In essence, they remove complexity from the day-to-day work of staff responsible for managing key instances by moving as many decisions as possible regarding key management to an enterprise modelling stage upfront.

For instance, a number of these decisions are related to the way keys are imported into and exported from Chiave. Parameters related to import and export are combined into Transport Profiles specific to each key type, which are later used when importing or exporting individual keys.

Key types in Chiave have the following attributes:

| | |
|---|---|
| **Name** | A reference that will help you identify the key type. We recommend you use descriptive names that contain one or more elements of algorithm, length, purpose and possibly an abbreviation of the systems it is intended for. |
| **Algorithm** | Specifies the key algorithm of the key. Currently Chiave supports double- and triple-length DES keys, AES 128, 192 and 256, as well as RSA 1024, 2048 and 4096 keys. |
| **Require dual control for generating** | When this key type is generated on Chiave, the operation can be configured to require dual control (i.e. the participation of two Key Custodians) for additional security. |
| **Require dual control for export/import in KEK format** | When this key type is imported or exported from Chiave encrypted under a transport key, these operations can be configured to require dual control (i.e. the participation of two Key Custodians) for additional security. |
| **Do not delete before** | Occasionally legal or operational requirements prohibit the destruction of key material for a period of |

| | |
|---|---|
| | time after it has been retired. This attribute allows Chiave to enforce this policy across all instances of a particular key type. Setting the value to 0 removes any restrictions on destruction, i.e. a key can be deleted as soon as it is retired from the last system it was used on. |
| **Default validity period** | Describes the intended period of key usage. If the key is generated on Chiave the period is timed from the moment of first export. For keys that are imported it is timed from the moment of import. The calculated expiry date is thereafter used as a basis of notification of key expiry. |
| **Default notification period** | Describes how many days ahead of a key instance expiry will Chiave notify responsible Key Custodians. |
| **Obsolete** | Removing a key type requires all instances of the particular type to be deleted, something that is not always practical. By marking a key type as obsolete one indicates that no new key instances of this key type can be created. |
| **Modes of use**<br>**Key usages** | TR-31 specific attributes aimed to provide further meta information about the intended usage for keys of this key type. While TR-31 is not supported by Chiave for the time being we recommend you enter relevant information in these fields to simplify the process of adopting TR-31 in the future. |
| **Comment** | Free form text describing the key type. |
| **Profiles** | A profile is a combination of parameters used when a key is imported to or exported from Chiave. Each key type may have multiple import/export profiles.<br>Configuring a profile in advance obviates the need to select the export/import parameters at each individual export and import, thus saving time and removing unnecessary complexity from day-to-day key management. |

**NOTE!** Key types are managed by Key Custodians with the privilege Manage Model.

## Keys

Key instances in Chiave have the following attributes:

| | |
|---|---|
| **Name** | A reference that will help you identify the key. We recommend you use descriptive names that contain one or more elements of its type, purpose and possibly an abbreviation of the systems it is intended for. |
| **Key identifier** | (Optional) An additional reference used to uniquely identify a key. |
| **Type** | Specifies the key type of the key. Currently Chiave supports double- and triple-length DES keys, AES 128, 192 and 256, as well as RSA 1024, 2048 and 4096 keys. |
| **Creation date** | Date when the key instance was generated |
| **Expiry date** | Describes the intended period of key usage. If the key is generated on Chiave the period is timed from the moment of first export. For keys that are imported it is timed from the moment of import |
| **Notification before expiry (days)** | Describes how many days ahead of the key instance expiry will Chiave notify responsible Key Custodians. |
| **Creation type** | Specifies whether the key instance was generated on Chiave or imported from an external system |
| **KCV** | Key checksum value of the key instance |
| **Do not delete before** | The date after which the key may be deleted once it has been retired. |
| **Comment** | Free-form text describing the key instance. |

## Key variants

One or more key variants can be used in cases where one key is used to encrypt others. Variants are hexadecimal strings that are combined with the actual key material according to the specific import/export algorithm (for example, IBM_CCA, simple XOR or other variant-based algorithms). By specifying key variants in advance one reduces the probability of error at the time of import/export.

Variants can be used in conjunction with any KEK format except for Atos. Furthermore, for the formats PREP and TMS it is mandatory to use a variant.

Key variants in Chiave have the following attributes:

| | |
|---|---|
| **Name** | A reference that uniquely identifies the variant. |
| **Size** | May be either 16, 24 or 32 bytes. Variants that do not conform to one of these three lengths cannot be used. |
| **Value** | A variant may be of any value, as long as its size matches one of the three listed above. |

**NOTE!** Key variants are managed by Key Custodians with the privilege Manage Model.

Certain well-known key variants are available by default, with no need to add them explicitly. Their names and values are listed below:

| Name | Value |
|---|---|
| Atalla 01 | 08000000000000000800000000000000 |
| Atalla 02 | 10000000000000001000000000000000 |
| Atalla 03 | 18000000000000001800000000000000 |
| Atalla 04 | 20000000000000002000000000000000 |
| Atalla 05 | 28000000000000002800000000000000 |
| Atalla 06 | 30000000000000003000000000000000 |
| Atalla 07 | 38000000000000003800000000000000 |
| Atalla 08 | 40000000000000004000000000000000 |
| Safenet 01 | 01010101010101010101010101010101 |
| Safenet 02 | 02020202020202020202020202020202 |
| Safenet 03 | 03030303030303030303030303030303 |
| Safenet 04 | 04040404040404040404040404040404 |
| Safenet 05 | 05050505050505050505050505050505 |
| Safenet 06 | 06060606060606060606060606060606 |
| Safenet 07 | 07070707070707070707070707070707 |
| Safenet 08 | 08080808080808080808080808080808 |

**NOTE!** Default key variants cannot be deleted from Chiave.

Ways of combining a key with a variant are referred to as transformation algorithms. Chiave currently supports IBM, Thales and simple XOR. However, there are certain restrictions in using the transformation. The possible combinations with key type, mode and padding are listed in the table below.

| Transformation | (Key to encrypt) KEK | Mode/padding |
|---|---|---|
| XOR | All, refer to section Import/export format restrictions for more detail.Import/export format restrictionsImport/export format restrictionsImport/export format restrictionsImport/export format restrictionsImport/export format restrictionsImport/export format restrictionsImport/export format restrictionsImport/export format restrictions | All |
| IBM | (2 TDES) 2 TDES | ECB NoPadding |
| Thales | (2 TDES) 2 TDES<br>(2 TDES) 3 TDES<br>(3 TDES) 3 TDES | ECB NoPadding |

## Systems

Chiave does not make any operational use of cryptographic keys – it can generate, import and export cryptographic keys in a variety of formats but the keys are put to operational use on other physical or logical systems such as HSMs, web-servers, disk-encryption devices or similar. The concept of a system in Chiave therefore describes a point of operational key usage by encapsulating its location, type and similar.

Systems in Chiave have the following attributes:

| | |
|---|---|
| **Name** | A reference that will help you identify the system. We recommend you use descriptive names that contain one or more elements of hardware or server type, location, or purpose. |
| **System group** | The system group this system belongs to. As mentioned above every system must be connected to one, and only one system group. When you want to create a new system, assure therefore that its system group is created first. |
| **Organisation** | Optional information about the organisation the |

| | |
|---|---|
| | system belongs to/is located at. |
| **Location** | Optional information about the systems location and any relevant physical access information. |
| **Comment** | Free form text describing the system. |

**NOTE!** Systems are managed by Key Custodians with the privilege Manage Model.

## System groups

Operational points are rarely unique. In most cases one has a number of systems that can be treated in a uniform way. A system group in Chiave depicts this relationship – every system has to belong to a system group and a system group may have zero or more systems that belong to it. Moreover, all systems in a system group are constrained to use the same set of key types. This relationship reduces the probability of operational errors by avoiding situations where an inadequate key instance is generated and exported to a system.

System groups in Chiave have the following attributes:

| | |
|---|---|
| **Name** | A reference that will help you identify the system group. System groups comprise of one or more systems so a good name will contain some form of reference to the common denominator of the systems belonging to the group. |
| **Email(s)** | One or more notification e-mail addresses that will be used to send messages on events related to systems within the group. |
| **Key types** | A selection of key types that can be used by systems belonging to this group. |
| **Members of the group** | A selection of systems belonging to this group. |
| **Comment** | Free form text describing the system group. |

**NOTE!** System groups are managed by Key Custodians with the privilege Manage Model.

## Users

Chiave allows users to assume one of two pre-defined roles: Administrator and Key Custodian. Administrators are users that can manage the appliance from an operational perspective (for example, manage network connections, time or similar) as well as define other users. They cannot, however, work with key instances – an administrator cannot generate new key instances or, for that matter, import, export, retire or delete key material. Administrators have access only to the Admin application on the appliance and require a valid password and an OTP generated by their respective tokens.

Key Custodians, on the other hand, have only access to the Key Management application and work with systems, system groups, key types and key instances. In their work they are guided by the defined models, i.e. Key Custodians can only work with key instances targeted to/sourced from systems they have been given access to and then only with types of keys as previously defined. Over and above a password and a token, for day-to-day work with Chiave a Key Custodian also needs a personal Chiave smartcard. Each Key Custodian can have one and only one smartcard at any time and it is used for secure import and export of key components into and from Chiave.

Users in Chiave have the following attributes:

| | |
|---|---|
| **Username** | A reference that uniquely identifies the user to Chiave. Usernames cannot be changed at a later date. |
| **Role** | One of Administrator or Key Custodian. A user’s role cannot be changed at a later date. |
| **Name** | Given name of the user. |
| **Surname** | Family name of the user. |
| **Password** | The user’s password that must be used when accessing Chiave. |
| **Token serial** | The serial number of the token allocated to the user. |
| **Card serial** | (Optional, only if role is Key Custodian) The serial number of the Chiave smartcard associated with the Key Custodian. |
| **User groups** | A list of one or more user groups the user belongs to. Every user must belong to at least one user group. |
| **Email** | The e-mail address of the user. |
| **Telephone number** | The telephone number of the user. |
| **Organization** | The organization or organizational part the user belongs to. |
| **Certificate** | The user’s X.509 v3 certificate in Basd64 encoding. |

| | |
|---|---|
| | Whilst not currently used, this will allow encryption of information from Chiave to the user. |
| **Comment** | Free form text describing the user. |

**NOTE!** Users are managed through the Administration application.

## User groups

Similar to System groups, User groups are used to aggregate user management. In other words, operational privileges of Key Custodians over System groups are managed through User groups.

Members of a User group can have one or more of the following privileges over systems in a System group:

| | |
|---|---|
| **Manage Model** | Allows the Key Custodian to shape the intended model of key usage on Chiave, i.e. to manage key types, key variants, system groups and systems and to create templates. |
| **Request Import** | Allows the Key Custodian to initiate import into Chiave of key material generated on external systems. Through the import Chiave maintains a link between the key material and the system that uses it. |
| **Execute Import** | Allows the Key Custodian to complete import into Chiave of key material generated on external systems. |
| **Request Export** | Allows the Key Custodian to initiate export of key material from Chiave targeted at an external system. Through this action key material previously imported onto or generated on Chiave can be transported onto the system that will make operational use of it. |
| **Execute Export** | Allows the Key Custodian to complete export of key material from Chiave targeted at an external system. |
| **Generate keys** | Allows the Key Custodian to initiate or complete generating key material aimed at a system within the System group. Note that key material actually has to be exported in a separate step. |
| **Retire Keys** | Allows a Key Custodian to inform Chiave that a key is no longer in operational use on a particular system. |
| **Delete Keys** | Allows a Key Custodian to permanently delete key |

| | |
|---|---|
| | material once it has been retired from all systems that had operationally made use of it. |

**NOTE**! Unlike Generate, Request/Execute Import, Request/Execute Export and Retire, which are system-specific, Delete is a global privilege and extends to all system groups over which a user's user group or groups have that privilege. Manage Model is a global privilege as well.

Should a user belong to more than one User group, with the membership in the respective User groups granting different privileges over the same System group, the user is considered to have both sets of privileges over the relevant System group.

User groups in Chiave have the following attributes:

| | |
|---|---|
| **Name** | A reference that will help you identify the user group. User groups encapsulate privileges to one or more system groups so a good name will contain some form of reference to the system groups, as well as the Key Custodians' role within that system group. |
| **Privileges matrix** | A specification of the privileges mentioned above (Generate, Request Import, Execute Import, Request Export, Execute Export, Retire) on a per group basis, as well as whether Key Custodians that are members of the group have the global Delete and/or Manage Model key privileges. |
| **Members** | A list of Key Custodians that are members of the user group. |
| **Comment** | Free form text describing the user group. |

**NOTE!** User groups are managed through the Administration application.

## General on Import/Export restrictions

As we have previously noted, keys and their variants can be used to encrypt other keys when they need to be imported or exported. However, not every key type can be applied to every other. In broad terms, key types of greater cryptographic strength cannot be encrypted by weaker ones. In turn, key types used to encrypt a key can restrict the format in which it can be transported.

The following list presents symmetric keys in order of cryptographic strength, from weakest to strongest:

1) 2TDES
2) AES-128
3) 3TDES
4) AES-192
5) AES-256

# Import/Export formats

This section describes key import/export formats supported by Chiave.

## Component set

| | |
|---|---|
| **Description** | Key component handling as described in ANSI X9.24-1:2009, Appendix C.5 |
| **Applicable to** | Double-length DES<br>Triple-length DES<br>AES 128, 192, 256 |
| **Remarks** | Each component within a component set can be handled by one, and only one Key Custodian. Consequently the number of Key Custodians required to import or export a key in component equals to the number of key components. |

## JKS

| | |
|---|---|
| **Description** | Sun Java Keystore file format |
| **Applicable to** | All key types |
| **Remarks** | At least two key custodians must participate in the import or export process. After the import or export has been initiated, one enters the password for the keystore file and the other supplies/acquires the file itself. |

## PKCS#12

| | |
|---|---|
| **Description** | A format commonly used for storing key pairs with their certificate chain in a password-protected file. |

| | |
|---|---|
| **Applicable to** | RSA1024, 2048, 4096 |
| **Remarks** | At least two Key Custodians must participate in the import or export process. After the import or export has been initiated, one enters the password for the keystore file and the other supplies/acquires the file itself. |

## XML

| | |
|---|---|
| **Description** | Generic XML format. |
| **Applicable to** | If encrypting key is double-length DES:<br>Double-length DES keys.<br>If encrypting key is triple-length DES:<br>Double- and triple-length DES keys and AES-128 keys.<br>If encrypting key is AES-128:<br>Double-length DES and AES-128 keys.<br>If encrypting key is AES-192:<br>Double- and triple-length DES, AES-128 and AES-192 keys.<br>If encrypting key is AES-256:<br>Double- and triple-length DES, AES-128, AES-192 and AES-256 keys. |
| **Remarks** | Depending on the key type settings, two Key Custodians may have to participate in the import or export process: one Key Custodian initiates the action, the other completes it.<br>If the key which is being imported has a Key Identifier, that parameter is included in the XML file as a separate tag. |

## Screen

| | |
|---|---|
| **Description** | The transported key is entered manually into Chiave (import) or displayed on the screen (export) in a hexadecimal format. |
| **Applicable to** | If encrypting key is double-length DES: |

| | |
|---|---|
| | Double-length DES keys.<br>If encrypting key is triple-length DES:<br>Double- and triple-length DES keys and AES-128 keys.<br>If encrypting key is AES-128:<br>Double-length DES and AES-128 keys.<br>If encrypting key is AES-192:<br>Double- and triple-length DES, AES-128 and AES-192 keys.<br>If encrypting key is AES-256:<br>Double- and triple-length DES, AES-128, AES-192 and AES-256 keys. |
| **Remarks** | Depending on the key type settings, two Key Custodians may have to participate in the import or export process: one Key Custodian initiates the action, the other completes it. |

## PREP

| | |
|---|---|
| **Description** | IBM_CCA variant based format for SecureCom Prep system (see below). |
| **Applicable to** | Double-length DES keys encrypted by double-length DES |
| **Remarks** | Two Key Custodians must participate in the import or export process. One initiates the action, the other completes it. |

This is the format of the file; the file format is position-based according to the following table:

| Character length | Type | Contents |
|---|---|---|
| 8 | CHAR | Key type, left-oriented and padded with blanks. |
| 48 | CHAR | Name of the key in the entry, left-oriented and padded with blanks. |
| 8 | NUM | Date of entry creation. |
| 48 | CHAR | Encrypted key value, left-oriented and padded with blanks. |

|  |  |  |
|---|---|---|
| 16 | HEX | Check value for key. |
| 48 | CHAR | Name of transport key. |
| 48 | CHAR | Variant, left-oriented and padded with blanks. |

## TMS

|  |  |
|---|---|
| **Description** | IBM_CCA variant based format for SecureCom TMS system |
| **Applicable to** | Double-length DES keys encrypted by double-length DES |
| **Remarks** | Two Key Custodians must participate in the import or export process. One initiates the action, the other completes it. |

This is the format of the file; the file format is position-based according to the following table:

| Character length | Type | Contents |
|---|---|---|
| 28 | NUM | 30 |
| 8 | NUM | Date of entry creation. |
| 225 | CHAR | Name of the key in the entry, left-oriented and padded with blanks. |
| 12 | CHAR | Key type. |
| 4 | CHAR | D11 |
| 64 | CHAR | Encrypted key value, left-oriented and padded with blanks. |
| 48 | CHAR | Variant, left-oriented and padded with blanks. |
| 2 | CHAR | Check value for key method S8. |
| 16 | HEX | Check value for key. |
| 510 | CHAR | Name of transport key. |

## Atos

|  |  |
|---|---|
| **Description** | Format suitable for import/export into Atos BankSys systems. |
| **Applicable to** | If encrypting key is double-length DES: |

| | |
|---|---|
| | Double-length DES keys<br>If encrypting key is triple-length DES:<br>Double- and triple-length DES keys and AES-128 keys.<br>If encrypting key is AES-128:<br>Double-length DES and AES-128 keys.<br>If encrypting key is AES-192:<br>Double-length DES and AES-128 keys.<br>If encrypting key is AES-256:<br>Double-length DES, AES-128 and AES-256 keys. |
| **Remarks** | Two Key Custodians must participate in the import or export process: one Key Custodian initiates the action the other completes it. |

This is the format of the file:

```
[GeneralParameters]
GenerationDateTime=DD/MM/YYYY HH:mm:ss
[EncryptedKey]
KEY_TYPE=DES | AES
KEY_TAG=
KEY_NAME=
ENC_MODE=ECB
TRANSPORT_KEYTYPE=DES | AES
TRANSPORT_KEY_INSTANCE=
CV_METHOD=NORM
CV=
ENC_KEY=
```

## Import/export format restrictions

The following table shows which import/export formats are available for each of the key algorithms supported:

| Key algorithm | Can be transported using the following formats: |
|---|---|
| 2TDES | JKS, CS, PREP, TMS, ATOS, XML, Screen |
| 3TDES | JKS, CS, ATOS, XML, Screen |
| AES128 | JKS, CS, ATOS, XML, Screen |

| | |
|---|---|
| AES192 | JSK, CS, XML, Screen |
| AES256 | JKS, CS, ATOS , XML, Screen |
| RSA1024 | JKS, PKCS#12 |
| RSA2048 | JKS, PKCS#12 |
| RSA4096 | JKS, PKCS#12 |

The following tables display the restrictions on transport keys and formats:

| Atos | KEK | | | | | |
|---|---|---|---|---|---|---|
| | | 2TDES | AES128 | 3TDES | AES192 | AES256 |
| Key to Encrypt | 2TDES | ✓ | ✓ | ✓ | ✓ | ✓ |
| | AES128 | ✗ | ✓ | ✓ | ✓ | ✓ |
| | 3TDES | ✗ | ✗ | ✓ | ✗ | ✗ |
| | AES192 | ✗ | ✗ | ✗ | ✗ | ✗ |
| | AES256 | ✗ | ✗ | ✗ | ✗ | ✓ |

| XML or Screen without padding | KEK | | | | | |
|---|---|---|---|---|---|---|
| | | 2TDES | AES128 | 3TDES | AES192 | AES256 |
| Key to Encrypt | 2TDES | ✓ | ✓ | ✓ | ✓ | ✓ |
| | AES128 | ✗ | ✓ | ✓ | ✓ | ✓ |
| | 3TDES | ✗ | ✗ | ✓ | ✗ | ✗ |
| | AES192 | ✗ | ✗ | ✗ | ✗ | ✗ |
| | AES256 | ✗ | ✗ | ✗ | ✗ | ✓ |

| XML or Screen with PKCS#5 padding | KEK | | | | | |
|---|---|---|---|---|---|---|
| | | 2TDES | AES128 | 3TDES | AES192 | AES256 |
| Key to Encrypt | 2TDES | ✓ | ✓ | ✓ | ✓ | ✓ |
| | AES128 | ✗ | ✓ | ✓ | ✓ | ✓ |
| | 3TDES | ✗ | ✗ | ✓ | ✓ | ✓ |
| | AES192 | ✗ | ✗ | ✗ | ✓ | ✓ |
| | AES256 | ✗ | ✗ | ✗ | ✗ | ✓ |

# Dual control

Most operations performed on Chiave Key Management application need the participation of two or more users to complete. After one user initiates the action, another Key Custodian with the same privileges can complete it. Both the initiator of the action and other users have the option of cancelling it.

Whenever a Key Custodian has initiated a dually controlled action, information about it will be displayed on the Info Screen, visible to all users with privileges to manage that particular key type. An e-mail notification with a brief description of the action initiated is also sent to all other Key Custodians able to complete that action. For instance, if the action initiated is a key export, the message will contain the name and checksum value of the key and the name of the system to which it is exported, as in the following example:

> Message subject: Key export initiated
>
> Message body: Key ‘AES128_key’ (KCV=C4BA2261) export initiated on system ‘banca_intesa_bgd’

Actions that are dually controlled include importing, exporting, retiring and deleting a key instance, while generating a key instance can optionally be configured to require dual control at the level of a key type. When a template is applied, if the tasks it contains entail any dually controlled actions, the execution of the template is dually controlled as well. Operations related to model management do not require the participation of more than one user, and neither does generating reports.

Keys can be imported and exported from Chiave in various formats. Transporting a key in a component set requires the use of Chiave OSC smartcards and the participation of as many users as there are components. One component set can be comprised of from two to ten components, each contained on a separate Smartcard.

When key instances are imported or exported in the form of a password-protected file, the process requires the participation of at least two users. After the import or export has been initiated, one user enters the password for the keystore file, and another supplies/acquires the file itself. If the user who initiates the export has both Request Export and Execute Export privileges, in addition to initiating the export they may have access either to the password or the file, but not both.

The import or export of key instances encrypted under a transport key can be dually controlled, depending on the way the key type is configured.

CHAPTER 2

# CONFIGURING KEY MANAGEMENT

After the necessary user groups have been defined on the Admin application, Key Custodians can configure key types, system groups which employ those key types and systems that belong to these groups. An administrator can then assign operational privileges over the system groups to Key Custodians.

**NOTE!** Entities described in this chapter and the corresponding tabs in the Key Management application are visible and available for configuration only to users with the privilege Manage Model.

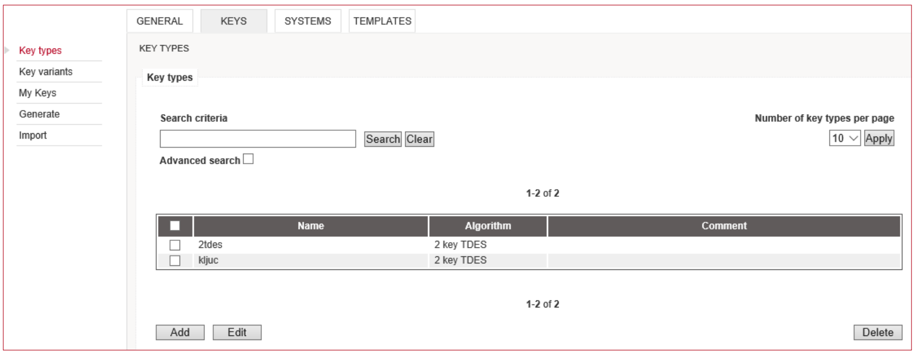
This chapter is divided as follows:

| | |
|---|---|
| Configuring Key Types (1) | Describes how key types are managed in Chiave. |
| Configuring System Groups (2) | Describes how system groups are managed in Chiave. |
| Configuring Systems (3) | Describes how systems are managed in Chiave. |

## Configuring key types

The modelling panels in Chiave are logically aligned with the model described above – one should first define key types used in an enterprise, then the systems that use those key types. The tabs in the application are presented in that order. To configure new or modify existing key types, click on the **Keys** tab, section Key types.

The number of key types shown per page is selectable in the top right corner, and you can search for key types by entering a search string in the **Search criteria** field and clicking on **Search**. This will trigger a basic search based on the key type name only. Select the **Advanced search** checkbox to present more search criteria (for the time being, the key type algorithm).



| □ | Name | Algorithm | Comment |
|---|---|---|---|
| □ | 2tdes | 2 key TDES | |
| □ | kljuc | 2 key TDES | |

To add a new key type:

### 1. Go to Keys > Key types

**a.** Click **Add.**

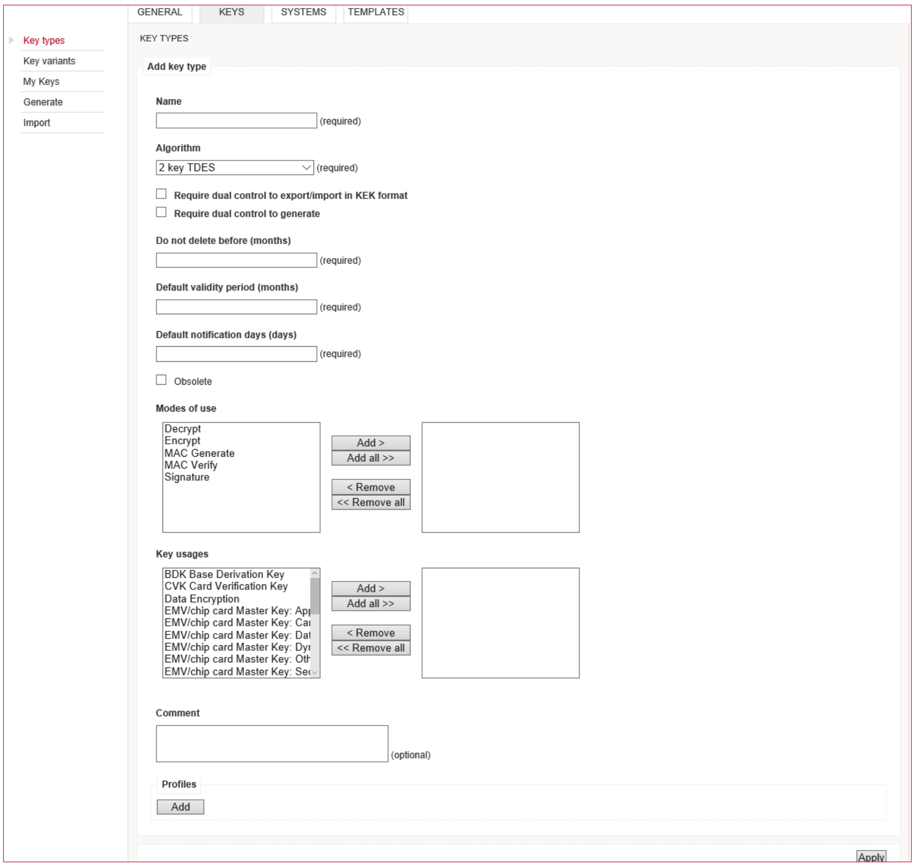
**b.** Enter a name for the key type.

**NOTE!** We recommend you use descriptive names that contain one or more elements of algorithm, length, purpose and possibly an abbreviation of the systems it is intended for.

**c.** Tick the checkbox **Require dual control for generating** if you want this operation to require the participation of two Key Custodians.

**d.** Select the algorithm for the key type. The options currently supported are double- and triple-length DES, AES 128, 192 and 256, and RSA based keys with lengths of 1024, 2048 and 4096.

**e.** Tick the **Require dual control for export/import** checkbox if you want these operations to require dual control when the keys are imported/exported. If the box is left unchecked, import or export under a transport key (though not in other formats) can be performed by a single Key Custodian if they have the appropriate privileges.



KEY TYPES

Add key type

Name
(required)

Algorithm
2 key TDES (required)

□ Require dual control to export/import in KEK format

□ Require dual control to generate

Do not delete before (months)
(required)

Default validity period (months)
(required)

Default notification days (days)
(required)

□ Obsolete

Modes of use
Decrypt
Encrypt
MAC Generate
MAC Verify
Signature

Key usages
BDK Base Derivation Key
CVK Card Verification Key
Data Encryption
EMV/chip card Master Key: Ap
EMV/chip card Master Key: Ca
EMV/chip card Master Key: Dat
EMV/chip card Master Key: Dy
EMV/chip card Master Key: Oth
EMV/chip card Master Key: Se

Comment
(optional)

Profiles

f. Enter a time span after which a key instance of this type may be deleted once it has been retired.

g. Enter a period of time after which a key instance of this type will expire.

h. Enter the number of days ahead of a key instance expiry when Chiave will notify the responsible key custodians.

i. Select the formats that are allowed when importing externally generated key instances of this key type into Chiave.

j. Select the formats that are allowed when exporting key instances of this type from Chiave.

k. (Optional) Select the intended modes of use and key usages for the key type.

l. (Optional) Enter an additional free-form comment about the key type.

m. Click **Add** to define an import/export profile. If any other elements need to be configured before a profile is created, you can save the key type as it is and define one or more profiles later.

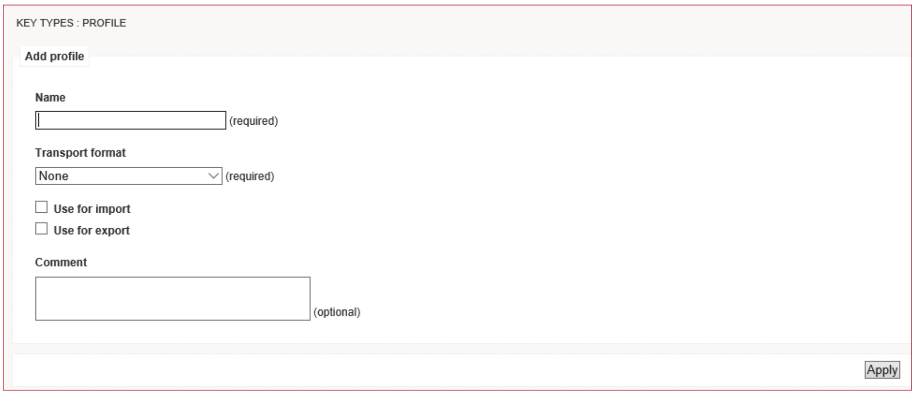
**Information Box**

If keys of this type are going to be transported encrypted under another key, the encrypting key type has to be defined prior to creating a profile. Variants used in key transformation may need to be configured separately as well, although a number of well-known variants are available by default.

To add or edit a transport profile within a key type:

**a.** Locate the section **Profiles**.

**b.** Click **Add**.



KEY TYPES : PROFILE

Add profile

Name

(required)

Transport format

None (required)

□ Use for import

□ Use for export

Comment

(optional)

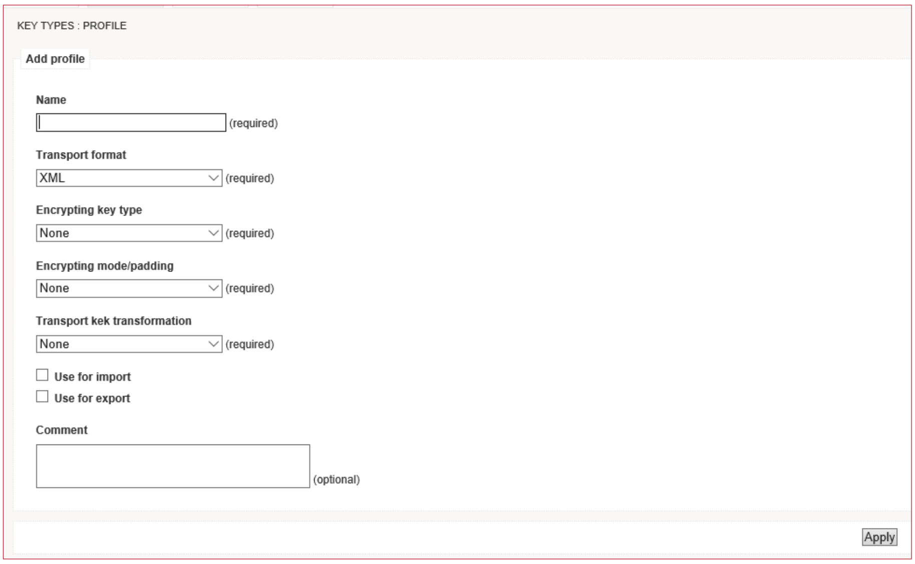
Apply

**c.** Enter a name for the profile. Profile name must be unique within a key type, but there is no such restriction across different key types.

**d.** Select a transport format. For more information on various formats, please refer to page 20 above.

**e.** If the format is Component set or one of the password-protected formats (JKS and PKCS#12), skip to step j. Otherwise proceed to step f. below.

**f.** (KEK formats only) If you have selected one of the formats that employ a key encrypting key, select a key type from the drop-down list.



KEY TYPES : PROFILE

Add profile

Name

(required)

Transport format

XML (required)

Encrypting key type

None (required)

Encrypting mode/padding

None (required)

Transport kek transformation

None (required)

□ Use for import

□ Use for export

Comment

(optional)

**g.** (KEK formats only) Select the encryption mode. Chiave supports CBC and ECB, where CBC can be used with or without PKCS#5 padding.

**h.** (KEK formats only) If the keys are going to be combined with a variant, select the transformation algorithm. The supported options are IBM, Thales and simple XOR. Whereas XOR is available for all formats, IBM can only be used when the key encrypting key belongs to the 2 TDES type. Thales can be used for 2TDES and 3TDES when key transformation is ECB NoPadding.

**Information Box**

Variants can be used in conjunction with any KEK format except for Atos. For the formats PREP and TMS, using a variant is mandatory.

**i.** (KEK formats only) Select a variant from the drop-down list. A number of commonly used variants is available by default; should you wish to use a variant other than these, please refer to the section Configuring key variants below.

**NOTE!** The variant needs to be of the same length as the key encrypting key. Therefore only the variants that meet this condition are available for selection within a profile. For example, if key type is AES 256, you can use variants whose length is 32 bytes.

**j.** Tick one or both checkboxes which indicate whether the profile will be used for export, import or both.

**k.** (Optional) Enter a free-form comment about the profile.

**l.** Click **Apply**.

To edit, delete or clone a profile, simply click the corresponding buttons on the page within the relevant key type.

If you want to modify the details of an existing key type, browse to the key type you want to modify and:

**a.** Click **Edit.**

**b.** Make the required changes.

**c.** Click **Apply.**

If you want to retire an existing key type, browse to the key type you want to retire:

**a.** Click **Edit.**

**b.** Tick the **Obsolete** checkbox**.**

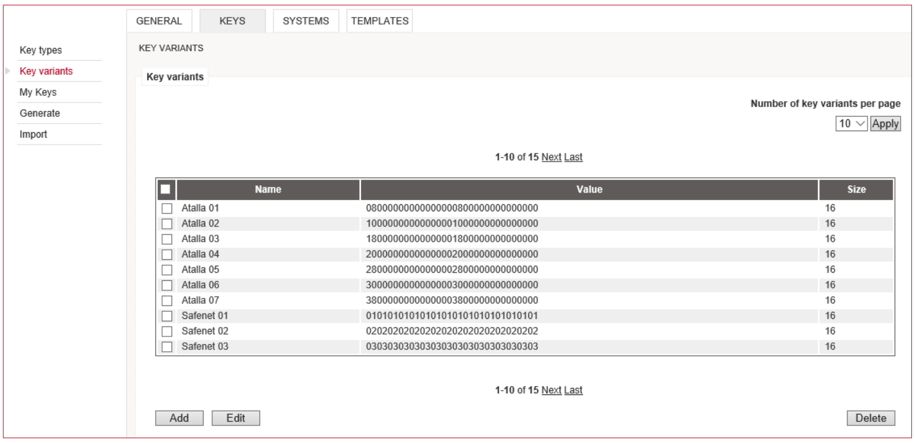
**c.** Click **Apply.**

**NOTE!** Before a key type is retired, keys that belong to it should first be removed from the system or systems. Note that retiring a key or marking a key type as obsolete are merely changes in Chiave's key management model, with no direct impact on the functioning of system or systems which employ the keys.

# Configuring key variants

Key variants are hexadecimal strings that can be combined with an encrypting key during key import or export. Since using variants reduces encrypting key reuse, the import/export process is rendered more secure. At the same time, specifying variants in advance removes the need to type them in manually at each key export/import and reduces the possibility of error.

To configure new or modify existing key variants, navigate to **Keys > Key variants**. The number of key variants shown per page is selectable in the top right corner.

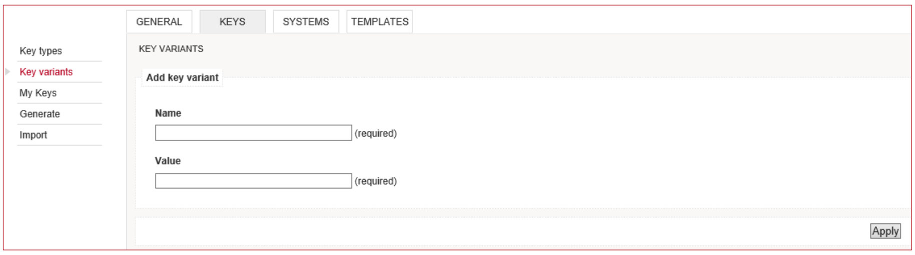


| □ | Name | Value | Size |
|---|---|---|---|
| □ | Atalla 01 | 08000000000000000800000000000000 | 16 |
| □ | Atalla 02 | 10000000000000001000000000000000 | 16 |
| □ | Atalla 03 | 18000000000000001800000000000000 | 16 |
| □ | Atalla 04 | 20000000000000002000000000000000 | 16 |
| □ | Atalla 05 | 28000000000000002800000000000000 | 16 |
| □ | Atalla 06 | 30000000000000003000000000000000 | 16 |
| □ | Atalla 07 | 38000000000000003800000000000000 | 16 |
| □ | Safenet 01 | 01010101010101010101010101010101 | 16 |
| □ | Safenet 02 | 02020202020202020202020202020202 | 16 |
| □ | Safenet 03 | 03030303030303030303030303030303 | 16 |

To add a new variant:

**Go to keys > Key variants**

a. Click **Add**.



Name
(required)

Value
(required)

b. Enter a suitable name for the variant.

c. Enter its value.

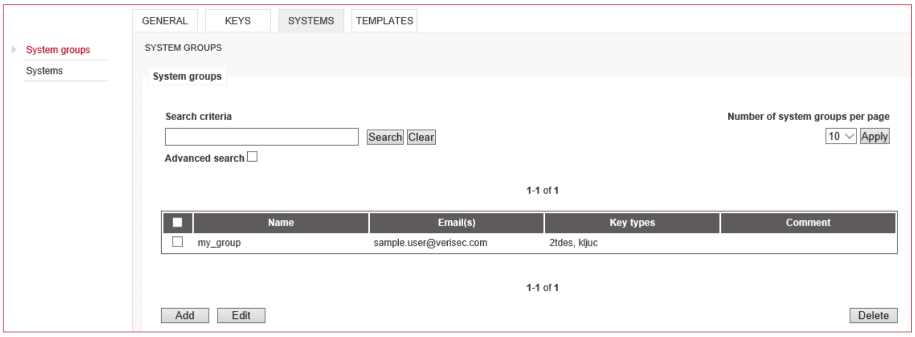
**NOTE!** The length of the variant may be either 16, 24 or 32 bytes. When creating an import/export profile, you'll be prompted to select from variants of the same length as the encrypting key.

d. Click **Apply**.

You can edit or delete existing variants by selecting them in the table and clicking the appropriate button. Note that a key variant cannot be deleted if it is used in an existing import/export transport profile. In addition, default variants cannot be removed from Chiave.

# Configuring system groups

To configure new or modify existing system groups, click on the **Systems** tab. The number of system groups shown per page is selectable in the top right corner. You can search for system groups by entering a search string in the **Search criteria** field and clicking on **Search**. This will trigger a basic search based on the group name only. Select the **Advanced search** checkbox to present more search criteria (for the time being, the key types used).

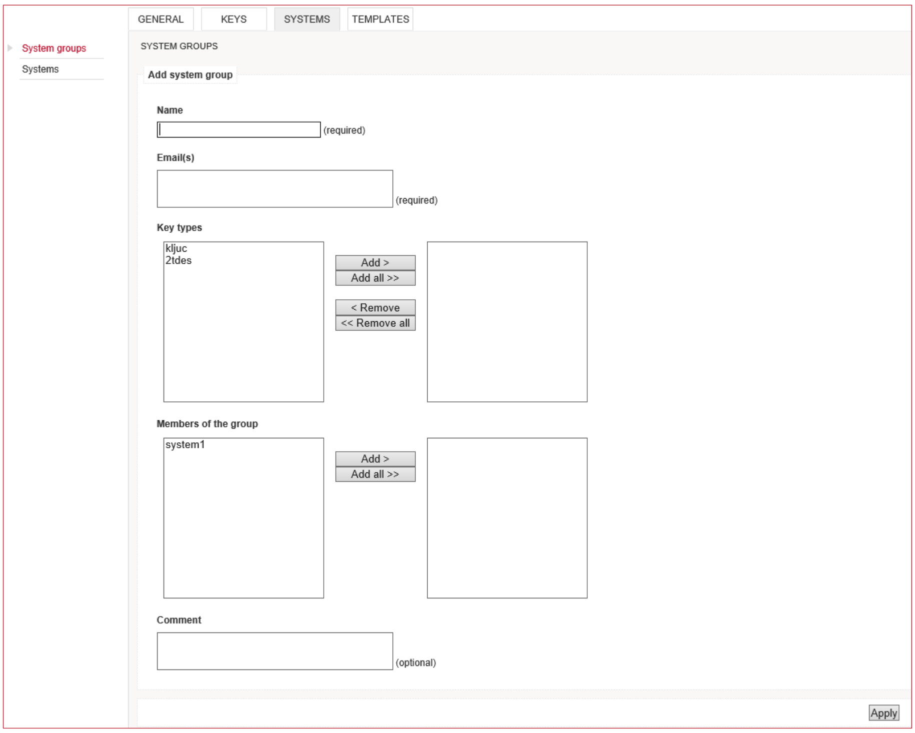


| ■ | Name | Email(s) | Key types | Comment |
|---|---|---|---|---|
| □ | my_group | sample.user@verisec.com | 2tdes, kljuc | |

To define a new system group:

## 1. Go to Systems > System groups

a. Click **Add.**



b. Enter a name for the system group.

**NOTE!** We recommend you use descriptive names that contain some form of reference to the common denominator of the systems belonging to the group.

c. Enter at least one e-mail address that will receive messages on events related to systems within the group.

d. Select key types that can be used by systems in this group.

e. Select one or more systems that will belong to this group.

f. (Optional) You may add a free-form comment about the group.

g. Click **Apply** to save the changes you made.

If you want to modify details for an existing system group browse to the group you want to modify and:

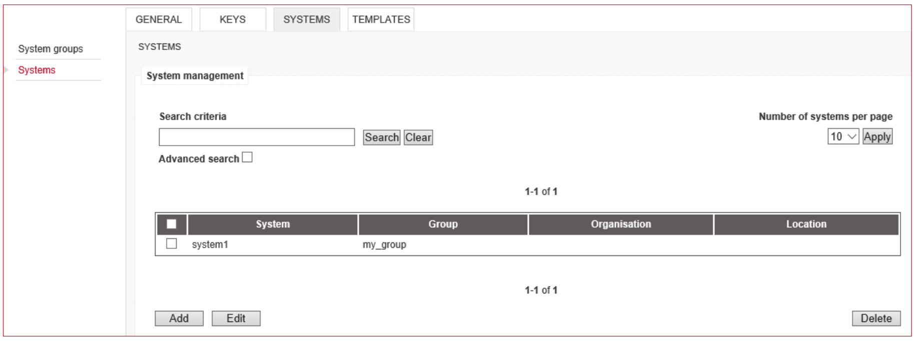
a. Click **Edit.**

b. Make required changes.

c. Click **Apply.**

# Configuring systems

To configure new or modify existing systems, click on the **Systems** tab. The number of systems shown per page is selectable in the top right corner. You can search for systems by entering a search string in the **Search criteria** field and clicking on **Search**. This will trigger a basic search based on the system name only. Select the **Advanced search** checkbox to present more search criteria (for the time being, the group to which a system belongs).



Search criteria

Advanced search □

Number of systems per page 10

1-1 of 1

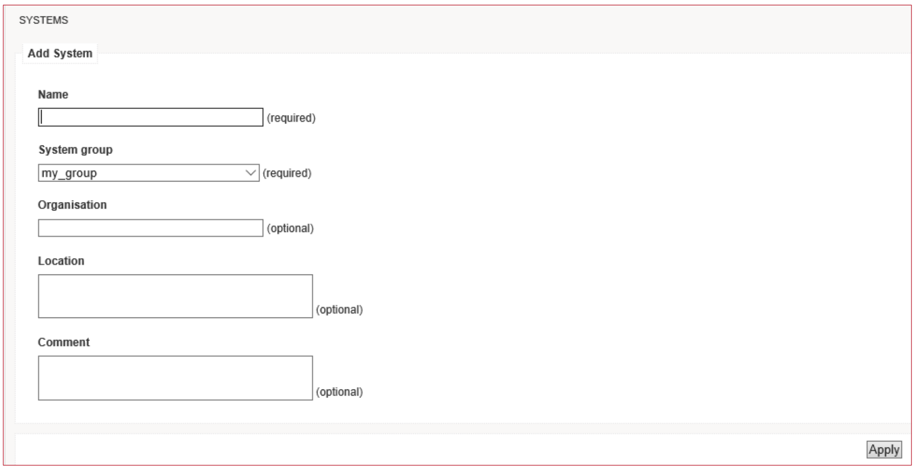
| □ | System | Group | Organisation | Location |
|---|---|---|---|---|
| □ | system1 | my_group | | |

1-1 of 1

To define a new system:

**Go to Systems > Systems**

a. Click **Add.**



SYSTEMS

Add System

Name

(required)

System group

my_group (required)

Organisation

(optional)

Location

(optional)

Comment

(optional)

**b.** Enter a name for the system.

**NOTE!** We recommend you use descriptive names that contain one or more elements of hardware or server type, location, or purpose.

**c.** Select the system group that the system will belong to. Note that a system cannot be defined unless it belongs to one and only one system group.

**d.** (Optional) Enter additional information about the organization that system belongs to or is located at.

**e.** (Optional) Enter additional information about the system's location and any relevant physical access information.

**f.** (Optional) Enter a free-form comment about the system.

**g.** Click **Apply** to save the changes you made.

If you want to modify the details of an existing system, browse to the system you want to modify and:

**a.** Click **Edit.**

**b.** Make the required changes.

**c.** Click **Apply.**

CHAPTER 3

# WORKING WITH KEYS

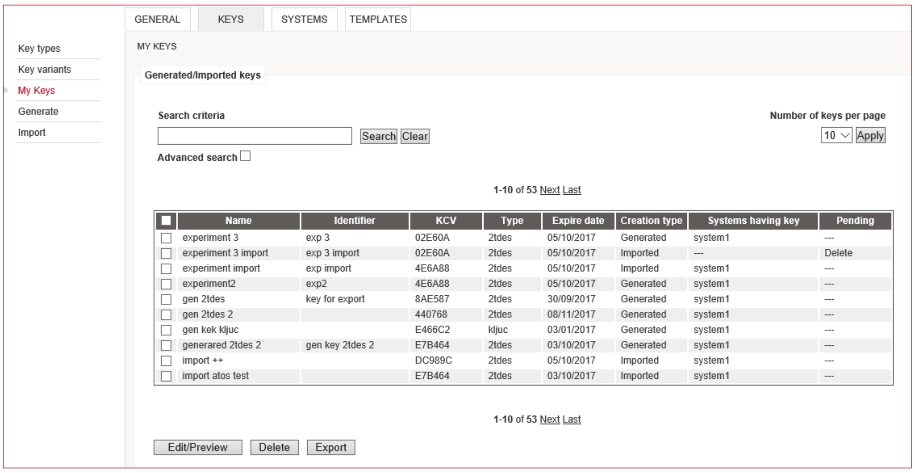
This chapter describes the specific steps of each operation that can be performed on key instances.

The chapter is divided as follows:

| | |
|---|---|
| My Keys (1) | Describes how a user can view and search existing key instances |
| Generating a new key (2) | Describes how key instances are generated on Chiave |
| Exporting a key (3) | Describes how key instances are exported from Chiave to an external system |
| Importing a key (4) | Describes how key instances are generated on external systems are imported into Chiave |
| Retiring a key (5) | Describes how a key is retired from a system |
| Deleting a key (6) | Describes how a key is permanently deleted |

## My Keys

The starting point for managing key instances is the page **My Keys**, which displays basic information about the keys that can be managed through the application. The number of key instances shown per page is selectable in the top right corner. You can search for keys by entering a search string in the **Search criteria** field and clicking on **Search**. This will trigger a basic search based on the key name only. Select the **Advanced search** checkbox to present more search criteria (identifier, key type, creation type, system or pending action).



| □ | Name | Identifier | KCV | Type | Expire date | Creation type | Systems having key | Pending |
|---|---|---|---|---|---|---|---|---|
| □ | experiment 3 | exp 3 | 02E60A | 2tdes | 05/10/2017 | Generated | system1 | --- |
| □ | experiment 3 import | exp 3 import | 02E60A | 2tdes | 05/10/2017 | Imported | --- | Delete |
| □ | experiment import | exp import | 4E6A88 | 2tdes | 05/10/2017 | Imported | system1 | --- |
| □ | experiment2 | exp2 | 4E6A88 | 2tdes | 05/10/2017 | Generated | system1 | --- |
| □ | gen 2tdes | key for export | 8AE587 | 2tdes | 30/09/2017 | Generated | system1 | --- |
| □ | gen 2tdes 2 |  | 440768 | 2tdes | 08/11/2017 | Generated | system1 | --- |
| □ | gen kek kljuc |  | E466C2 | kljuc | 03/01/2017 | Generated | system1 | --- |
| □ | generared 2tdes 2 | gen key 2tdes 2 | E7B464 | 2tdes | 03/10/2017 | Generated | system1 | --- |
| □ | import ++ |  | DC989C | 2tdes | 05/10/2017 | Imported | system1 | --- |
| □ | import atos test |  | E7B464 | 2tdes | 03/10/2017 | Imported | system1 | --- |

To view details about any of the key instances, select the key in the table and click **Edit/Preview**.

# Generating a new key

Generating key material on Chiave comprises of two steps. When initiating the action, the user is responsible for setting all the necessary parameters, while in the second step user is required simply to complete the key generation. Generating keys of a particular key type may be configured as a dually controlled action requiring the participation of two Key Custodians.

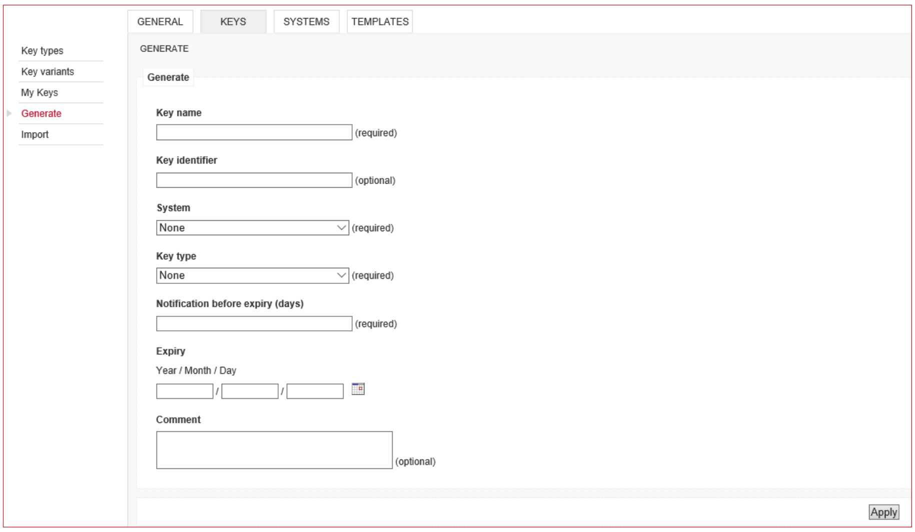
To initiate generating a new key instance:

**Go to Keys > Generate**

**a.** Enter a suitable name for the key.

**NOTE!** We recommend you use descriptive names that contain one or more elements of its type, purpose and possibly an abbreviation of the system it is intended for.

**b.** (Optional) Enter a key identifier as an additional reference to uniquely identify the key.



Generate

Key name
(required)

Key identifier
(optional)

System
None (required)

Key type
None (required)

Notification before expiry (days)
(required)

Expiry
Year / Month / Day
/ /

Comment
(optional)

**c.** Select a system from the drop-down list. Note that a key instance has to be exported to the system that will make operational use of it as a separate step.

**d.** Select a key type from the drop-down list. Note that the selection of the system determines which key types are available.

**e.** The choice of key type determines the default number of days ahead of the key instance expiry when Chiave will notify responsible Key Custodians via e-mail. You may enter a different notification period.

**f.** The choice of key type determines the default validity period of the key. You may select a different date of expiry.

**g.** (Optional) Enter a free-form comment about the key instance.

**h.** Click **Apply** to save changes.

An e-mail notification is sent to all users able to complete the action. A notification about the pending generation also appears on the Info Screen with a shortcut to the page with key details

To complete generating a key:

**Go to Keys > My Keys**

**a.** Select the key instance in the table. It will be marked as involved in a pending generate action.

**b.** Click **Edit/Preview**.

**c.** Locate the link for completing the generation and click **Complete**.

Key generation can also be cancelled by any of the users with the same privileges, including the user who has initiated the action. To cancel generating a key:

**Go to Keys > My Keys**

- **a.** Select the key from the table.
- **b.** Click **Edit/Preview.**
- **c.** Locate the relevant link and click **Cancel**.

When generating a key pair, follow the same procedure as described above. Key pairs generated on Chiave automatically get a self-signed certificate. If you acquire a certificate from a Certification Authority at a later date, the certificate received from the CA will replace the self-signed one after it has been processed.

In order to obtain a certificate you need to send the CSR (Certificate Signing Request) to a Certification Authority and then processes the reply in Chiave. To perform the certification of a key pair a Key Custodian needs to have the Generate privilege for the relevant key type.

To initiate certifying a key pair:

**Go to Keys > My Keys**

- **a.** Select the key from the table.
- **b.** Click **Edit/Preview.**
- **c.** In the following screen, locate the label **Initiate certifying** and click **Initiate.**
- **d.** Enter the distinguished name in the required format.
- **e.** Click **Apply**.
- **f.** In the presented file dialogue select a location to save the CSR file.
- **g.** Send the CSR to a CA.

After you receive the reply, repeat steps a-c and then:

- **a.** Locate the label **Pending certification actions** and click **Process**.
- **b.** In the section **Certification response**, click **Browse**... and upload the file containing the response.
- **c.** In the section **Trusted certificate**, click **Browse**... and upload the file containing the CA’s certificate.
- **d.** Click **Process**.

Once the certificate response has been processed, the certificate chain of the key pair can be viewed in the key details. Should you need to re-certify a key pair, either because the original certificate is about to expire, because you need a certificate from a different CA or for any other reason, locate the label **Initiate re-certifying** in the key details page and acquire the new certificate in the same manner.

**NOTE!** Certifying and recertifying a key pair requires that you have the Generate privilege.

# Exporting a key

Exporting a key from Chiave to an external system is a dually controlled action and will require the participation of one or more other Key Custodians to complete. The exception is exporting a key encrypted under a transport key, which does not have to be dually controlled, but may optionally be configured as such at the level of a key type.

To initialize a key export:

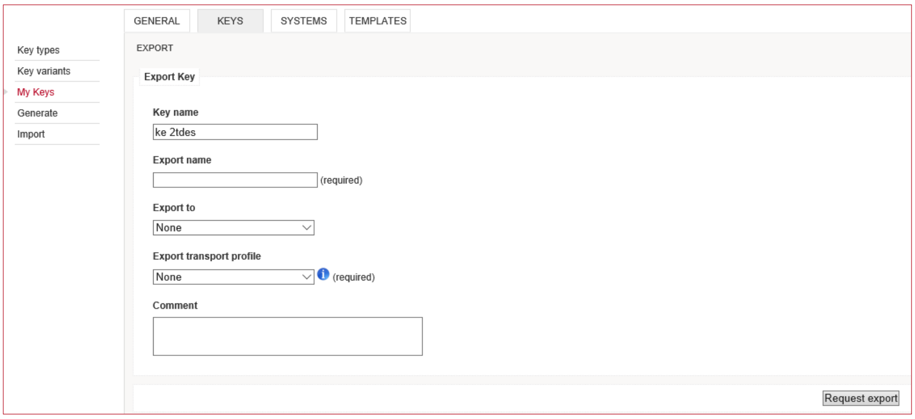
**Go to Keys > My Keys**

**a.** Select a key from the table.

**b.** Click **Export**.

**c.** Enter an export name that will serve as an identifier to differentiate between multiple exports of the same key instance.

**NOTE!** We recommend that you use names that contain the name of the key and the system to which the key is being exported.



Export Key

Key name: ke 2tdes

Export name: (required)

Export to: None

Export transport profile: None (required)

Comment:

**d.** Select a system from the drop-down list.

**e.** (Optional) Enter a free-form comment about the export.

**f.** Select an export transport profile from the drop-down list. For more information about the selected profile, hover the mouse over the Info icon next to the field.

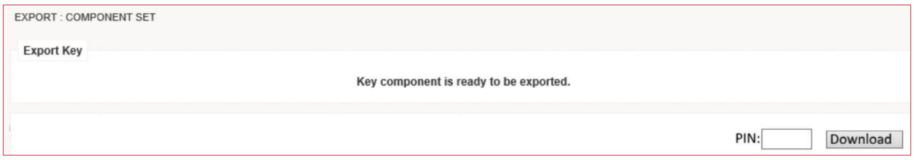
If the format used in the export is Component set, go to step g. Otherwise, simply click **Request export**.

**g.** Select the number of components (2-10).

**h.** Click **Next.**

**i.** Insert an OSC smartcard into the online card reader.

**j.** Enter online PIN of the card.



EXPORT : COMPONENT SET

Export Key

Key component is ready to be exported.

**NOTE!** A smartcard contains ten key component slots. Chiave ensures that any one smartcard cannot hold more than one component of any given key. During export or import, the first available card slot is automatically used to store the component. If there are no available card slots, an appropriate message is displayed on the screen.

**k.** Download the component onto the card.

**l.** Click **Confirm and continue.**

When an export is initiated, an e-mail notification is sent to all users able to complete the action. A notification about the pending export also appears on the Info Screen with a shortcut to the page with key details.

The way an export is completed is somewhat different for various formats. Depending on the export mechanism selected within the profile, proceed to one of the sections below: Component set, Password-protected file (the formats JKS or PCKS#12) or Encrypted under a transport key (PREP, TMS, Atos, XML or Screen).

## Component set

**Go to Keys > My Keys.**

**a.** Select the key from the table.

**b.** Click **Edit/Preview.**

c. In the **Initiated exports** table find the export and click **Complete**.

d. Insert an OSC smartcard into the online card reader.

e. Enter online PIN.

f. Download the component onto the card.

g. Click **Confirm and continue** if there are more components to be exported or **Finish** if you are completing the process.

h. If necessary, have other Key Custodians repeat the process until all components are exported.

## Password-protected file

For the time being, password-protected file formats supported by Chiave are JKS, which can be used for any key type, and PKCS#12, which is used for asymmetric keys.

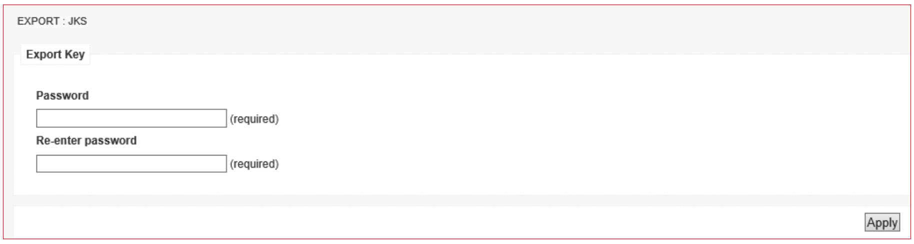
**1. Go to Keys > My Keys.**

a. Select the key from the table.

b. Click **Edit/Preview.**

c. In the **Initiated exports** table find the export and click **Complete**.

d. In the following screen enter the keystore password.



EXPORT : JKS

Export Key

Password

(required)

Re-enter password

(required)

e. Re-enter the same password.

f. Click **Apply.**

**2.** Have another Key Custodian log in and repeat steps a-c.

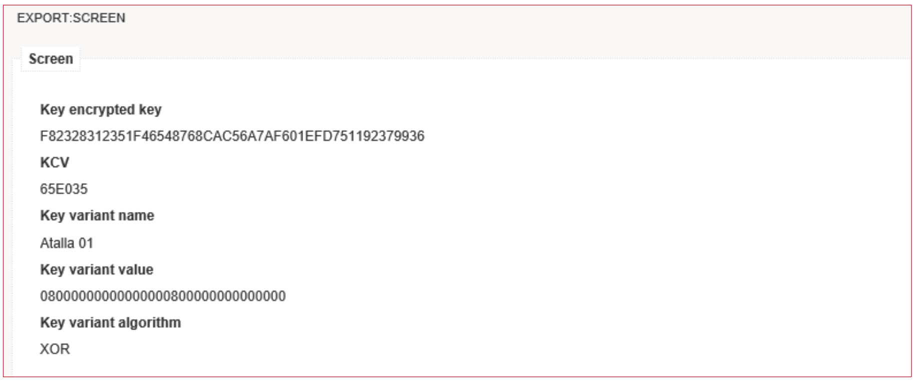
a. Click **Download**.

b. In the presented file dialogue select a location to save the file.

### Encrypted under a transport key

**Go to Keys > My Keys.**

- **a.** Select the key from the table.
- **b.** Click **Edit/Preview.**
- **c.** In the **Initiated exports** table find the export and click **Complete**.
- **d.** If the format is Screen, the key and its checksum value are now displayed.



EXPORT:SCREEN

Screen

**Key encrypted key**

F82328312351F46548768CAC56A7AF601EFD751192379936

**KCV**

65E035

**Key variant name**

Atalla 01

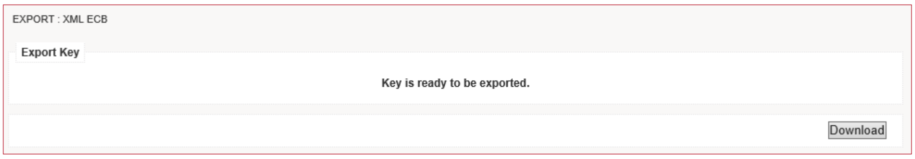
**Key variant value**

08000000000000000800000000000000

**Key variant algorithm**

XOR

For any other KEK format, click **Download** and in the presented file dialogue select the location to save the file.



EXPORT : XML ECB

Export Key

Key is ready to be exported.

An export action can be cancelled by any of the users with the same privileges, including the user who has initiated the action. To cancel an export:

**Go to Keys > My Keys.**

- **a.** Select a key from the table.
- **b.** Click **Edit/Preview.**
- **c.** In the **Initiated exports** table find the export and click **Cancel**.

# Importing a key

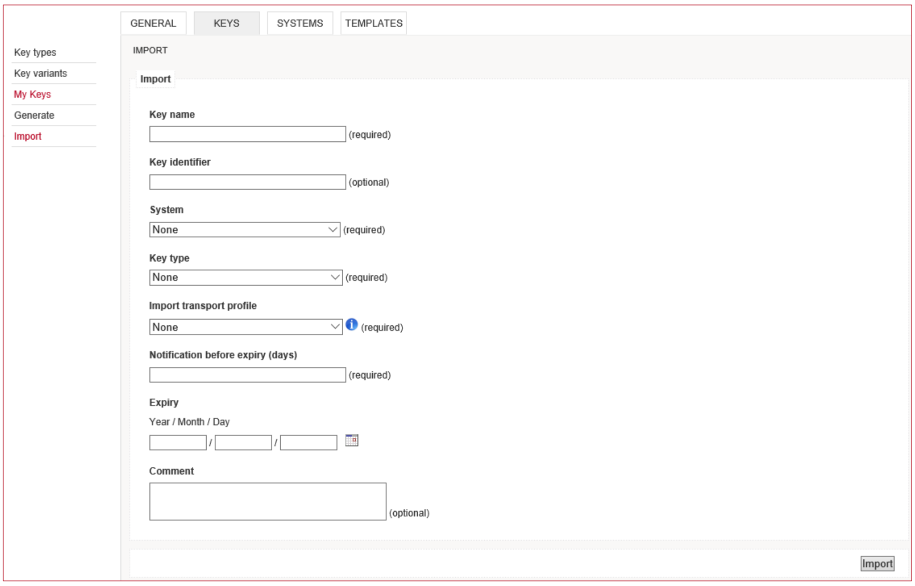
Importing a key from an external system into Chiave is a dually-controlled action and will require the participation of one or more other Key Custodians to complete. The exception is importing a key encrypted under a transport key, which may optionally be configured as dually controlled at the level of a key type.

To initialise importing a key:

**Go to Keys > Import**

**a.** Enter a name for the key.

**NOTE!** We recommend you use descriptive names that contain one or more elements of its type, purpose and possibly an abbreviation of the system associated with it.



Key name (required)

Key identifier (optional)

System None (required)

Key type None (required)

Import transport profile None (required)

Notification before expiry (days) (required)

Expiry Year / Month / Day

Comment (optional)

**b.** Select a system from the drop-down list.

**c.** Select the key type of the key instance from the drop-down list.

**d.** (Optional) Enter a key identifier as an additional reference to uniquely identify the key.

**e.** The choice of key type determines the default validity period of the key. You may select a different date of expiry.

**f.** (Optional) Enter a free-form comment about the key instance.

**g.** Select an import transport profile from the drop-down list. For more information about the selected profile, hover the mouse over the Info icon next to the field.

**h.** Click **Import**. If you have selected Component set as the import mechanism, go to step l.

**i.** Select the number of components (2-10).

j. Click **Next**.

k. Insert an OSC smartcard into the online card reader.

l. Enter online PIN.

m. Select the card slot holding the component.

n. Upload the component from the card.

o. Click **Confirm and continue.**

An e-mail notification is sent to all users able to complete the action. A notification about the pending import will appear on the Info Screen with a shortcut to the page with key details.

When completing a key import, the following steps are common for all import formats, while the remainder of the procedure differs with regards to the import mechanism selected.

**Go to Keys > My Keys**

a. Select the key which is to be imported.

b. Click **Edit/Preview.**

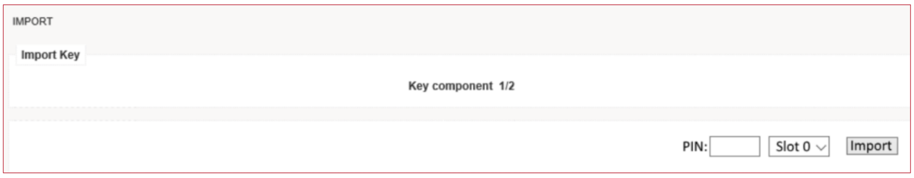
c. Locate the table **Initiated imports** and click **Complete**.

Depending on the import format of the selected profile, proceed to one of the following subsections: Component set, Password-protected file (JKS or PCKS#12) or Encrypted under a transport key (PREP, TMS, Atos, XML or Screen).

## Component set

a. Insert an OSC smartcard into the online card reader.

b. Enter online PIN.



c. Select the card slot holding the component.

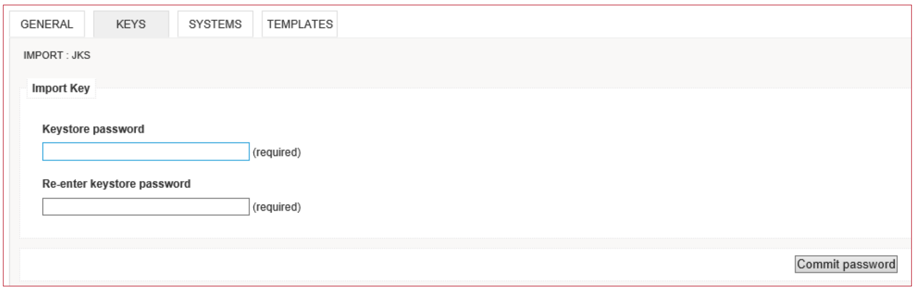
d. Click **Import.**

e. Click **Confirm and continue** if there are more components to be imported or **Finish** if you are completing the process.

## Password-protected file

For the time being, password-protected file formats supported by Chiave are JKS, which can be used for any key type, and PKCS#12, which is used for asymmetric keys.

To supply the password, after the steps listed above:



Keystore password (required)

Re-enter keystore password (required)

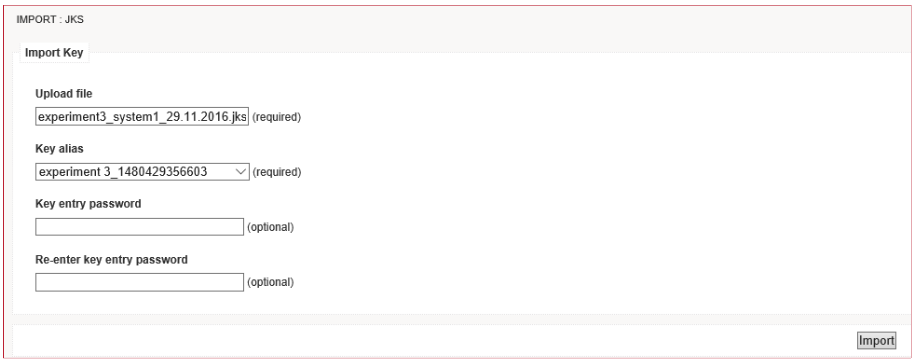
a. Enter the keystore password.

b. Re-enter the same password.

c. Click **Commit Password.**

To complete the import, have another Key Custodian log in and:

a. Click **Browse...** and select the file to be uploaded.



Upload file: experiment3_system1_29.11.2016.jks (required)

Key alias: experiment 3_1480429356603 (required)

Key entry password (optional)

Re-enter key entry password (optional)

b. Select the key alias from the drop-down list.

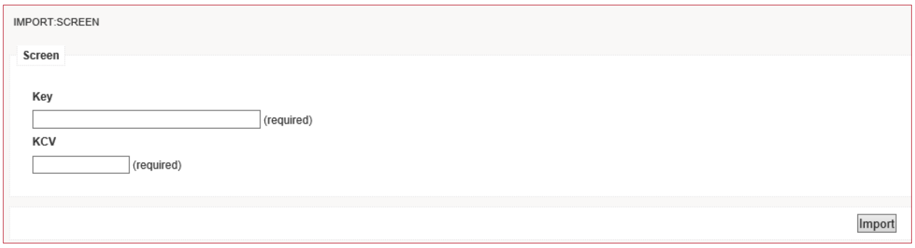
c. (Optional) If the key entry is protected with a password different than the keystore password, enter the key entry password.

d. (Optional) Re-enter the same key entry password.

e. Click **Import.**

## Encrypted under a transport key

If the import format is Screen:


IMPORT:SCREEN

Screen

Key

(required)

KCV

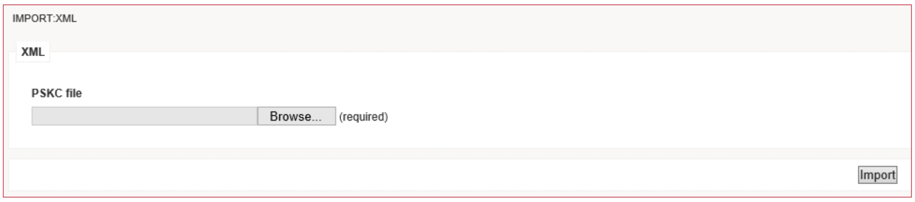
(required)

a. Enter the value of the key.

b. Enter the key checksum value.

c. Click **Import**.

If the import format is any other KEK format:


IMPORT:XML

XML

PSKC file

(required)

a. Click Browse... and select the file to be uploaded.

b. Click **Import**.

An import action can be cancelled by any of the users with the same privileges, including the user who has initiated the action. To cancel an import, go to **Keys > My keys**, follow the same steps as you would for completing it until you have located the **Initiated imports** table for this key instance and click **Cancel**.

**NOTE!** Whenever you initiate an import, the entry for that key instance in the table on the **My Keys** page will be marked as **Import*** to indicate that you may cancel this action, but not complete it.

# Retiring a key

Retiring a key instance is a dually-controlled action and will require the participation of another Key Custodian to complete.

**NOTE!** Before a key type is retired, keys that belong to it should first be removed from the system or systems. Note that retiring a key is merely a change in Chiave's key management model, with no direct impact on the functioning of system or systems which employ the keys.

To initialise retiring a key:

**Go to Keys > My Keys**

**a.** Select a key from the table.

**b.** Click **Edit/Preview.**

**c.** Locate the table **Systems having key** and click the **Initialize** button in the **Retire** column.

**d.** When prompted, confirm whether you really want to retire the key.

An e-mail notification is sent to all users able to complete the action. A notification about the pending delete action will appear on the Info Screen as well with a shortcut to the page with key details.

To complete retiring a key:

**Go to Keys > My Keys**

**a.** Select a key from the table.

**b.** Click **Edit/Preview.**

**c.** In the table **Systems having key**, click **Complete** in the **Retire** column.

**d.** When prompted, confirm whether you really want to retire the key.

A retire action can be cancelled by any of the users with the same privileges, including the user who has initiated the action. To cancel a retire action, go to **My keys** and follow the same steps as you would for completing it until you have located the column **Retire** in the table **Systems having key** and click **Cancel**.

# Deleting a key

Deleting a key instance is a dually controlled action and will require the participation of another Key Custodian to complete.

To initialise deleting a key:

**Go to Keys > My Keys**

**a.** Select a key from the table.

**b.** Click **Delete.**

**c.** When prompted, confirm whether you really want to delete the key.

An e-mail notification is sent to all users able to complete the action. A notification about the pending delete action will appear on the Info Screen as well with a shortcut to the page with key details.

To complete deleting a key, go to **Keys > My Keys** and repeat the same steps as the user who initiated the delete action.

**NOTE!** A key cannot be deleted if it is deployed on one or more systems, if an import or export process has been initiated or if the period of time before which its deletion is prohibited has not elapsed.

A delete action can be cancelled by any of the users with the same privileges, including the user who has initiated the action. To cancel a delete action:

**Go to Keys > My Keys.**

**a.** Select the key from the table.

**b.** Click **Edit/Preview.**

**c.** Locate the parameter **Pending delete** and click **Cancel**.

CHAPTER 4

# WORKING WITH TEMPLATES

In day-to-day use of Chiave key management appliance there will often arise a need to manage keys on a large scale, on a per-system basis. In such cases the same combinations of processes frequently occur together as well – for instance, generating a key and exporting it to an external system, or retiring a key and creating a suitable replacement. Therefore, commonly repeated processes on Chiave can be automated through the use of templates. Templates are defined at the level of a system group and applied to key instances in a specific system.

This chapter is divided as follows:

| | |
|---|---|
| About templates (1) | Describes the basic concepts of working with templates |
| Configuring templates (2) | Describes how new templates are defined or existing ones edited. |
| Applying templates (3) | Describes how templates are applied to specific key instances. |

## About templates

A template consists of tasks – atomic actions performed upon a key instance. Every task pertains to one of the following types:

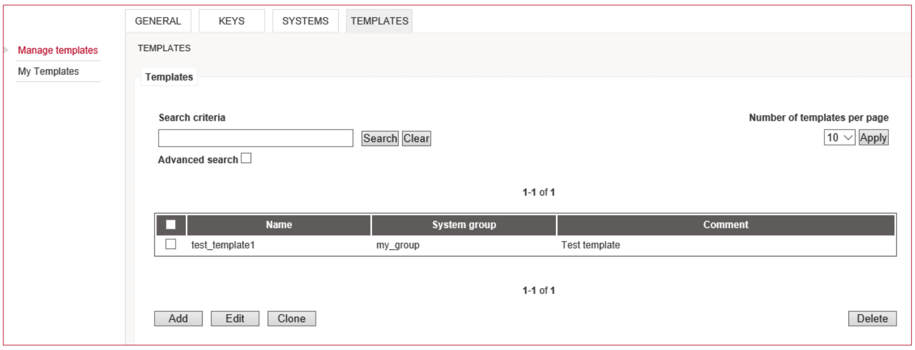
| | |
|---|---|
| **Select** | Selects one key instance of a specified key type. |
| **Generate** | Generates a new key instance with the following parameters predefined: key type, key name template, notification before expiry in days, validity period in months and comment. |
| **Clone** | Generates a new key instance based on an existing one, replicating the characteristics such as notification time, expiry date and comment. |
| **Retire** | Retires the key from the system on which it is deployed. |
| **Export** | Exports the key from Chiave to an external system. |

Templates are created by users with the privilege Manage Model. To access and apply a template, Key Custodians need to have the appropriate privileges to perform the operations which the template entails. Clone is treated as the equivalent of Generate in terms of privileges. Select does not require a privilege.

If a template includes one or more dually controlled operations, the execution of the template is dually controlled as well. To initiate the execution of a template, a Key Custodian needs to have the appropriate privilege for performing every task that the template contains. To complete it, however, it is enough to have a privilege for the operations which have not been completed. For example, if a template comprises of generating a key instance and exporting it, the Key Custodian initializing the template needs to have both Generate and Request Export privileges. Since key generation is completed in a single step, the execution of a template can be completed by a Key Custodian who only has Execute Export.

# Configuring templates

To view and search all existing templates, go to **Templates > Manage Templates**. The number of templates shown per page is selectable in the top right corner. You can search for templates by entering a search string in the **Search criteria** field and clicking on **Search**. This will trigger a basic search based on the template name only. Select the **Advanced search** checkbox to include searching according to the group the template is associated with.



| ■ | Name | System group | Comment |
|---|---|---|---|
| □ | test_template1 | my_group | Test template |

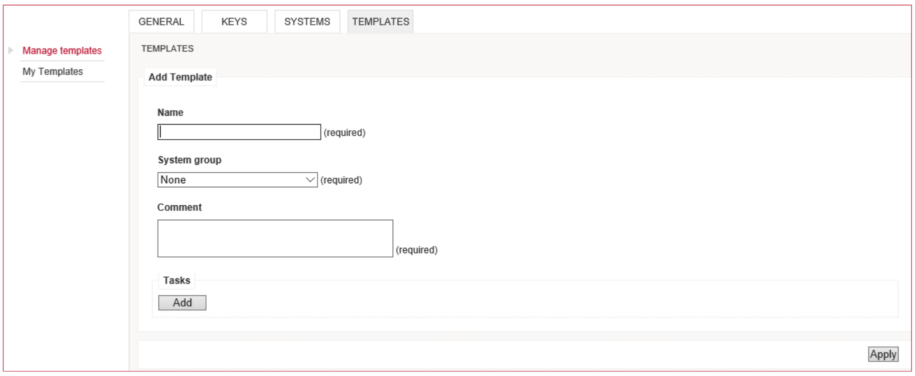
In order to create or edit a template:

**Go to Templates > Manage Templates**

**a.** Click **Add** to define a new template or **Edit** to make changes to an existing one.

**b.** Enter an appropriate name for the template.

**c.** Fill in a free-form comment about the intended usage of the template.



**d.** In the Task section, click **Add** to define a new task.

In the process of defining a task, the first three steps – selecting the type, entering the name and filling in the comment – are the same for all types of tasks, whereas the rest vary according to the type. To define a task:

**a.** Enter a suitable name for the task. It is recommended to choose a name which briefly describes its purpose.

**b.** Select the type of action that the task involves (Select, Generate, Clone, Retire or Export).

**c.** Depending on the type of task in question, proceed to step d. for Select, e. for Generate, f. for Clone, g. for Retire or h. for Export.

**d.** If the task type is **Select**:

i. Choose the key type from the drop-down menu.

ii. Enter a free-form comment about the task.

iii. Click **Apply**.

**e.** If the task type is **Generate**:

i. Choose the key type from the drop-down menu.

ii. Enter the key name template.

**Information Box**

Key name templates contain tags that will be replaced with the appropriate values when the task is executed. Chiave supports the following tags:

- <key_type> tag will be replaced with the name of key type
- <system> tag will be replaced with name of system to which the template is applied
- <date date_format> will be replaced with the current date value in the specified date format (yyyy, yyyy-MM-dd, dd/MM/yyyy, etc.)
- <time time_format> tag will be replaced with the current time in

specified format (HH_MM_SS, HH, HH-MM, etc.)

   iii. (Optional) Enter the key identifier template. The same tags available for key name templates can be used for the key identifier.

   iv. Enter the key validity period in months. This field is automatically populated when the key type is selected, but the value can be modified.

   v. Enter the number of days ahead of the key instance expiry when Chiave will notify the responsible key custodians. This field is automatically populated when the key type is selected, but the value can be modified.

   vi. (Optional) Enter a free-form comment about the key instance.

   vii. Enter a free-form comment about the task.

   viii. Click **Apply**.

**f.** If the task type selected is **Clone**:

   i. Select the result of a previously executed Select or Generate task as the key to be cloned.

   ii. Enter the key name template.

   iii. (Optional) Enter the key identifier template.

   iv. Enter a free-form comment about the task.

   v. Click **Apply**.

**g.** If the task type selected is **Retire**:

   i. Select the result of a previously executed Select task as the key to be retired.

   ii. Enter a free-form comment about the task.

   iii. Click **Apply**.

**h.** If the task type selected is **Export**:

   i. Select the result of a previously executed Select, Generate or Clone task as the key to be exported.

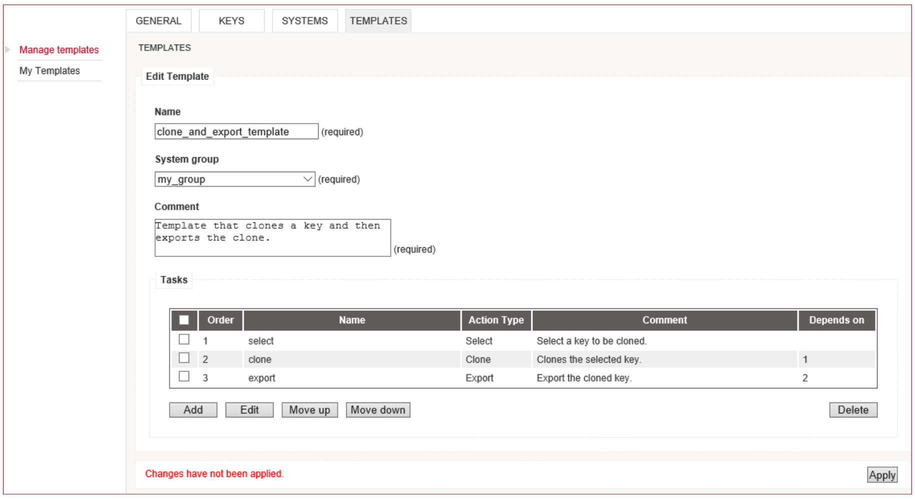
   ii. Select the export transport profile from the drop-down menu. For more information about the selected profile, hover the mouse over the Info icon next to the field.

iii. (KEK formats only) If required by the profile, select the key encryption key. Note that in this case the KEK type has to be defined in another Select task first.

iv. Enter a free-form comment about the task.

v. Click **Apply.**

After adding or editing each task you will be redirected to the page where you can view the template as a whole and make any modifications that may be needed.



Name: clone_and_export_template (required)

System group: my_group (required)

Comment: Template that clones a key and then exports the clone. (required)

| □ | Order | Name | Action Type | Comment | Depends on |
|---|---|---|---|---|---|
| □ | 1 | select | Select | Select a key to be cloned. | |
| □ | 2 | clone | Clone | Clones the selected key. | 1 |
| □ | 3 | export | Export | Export the cloned key. | 2 |

Changes have not been applied.

Once all the necessary tasks have been defined and arranged in the desired order, click **Apply** to save the template.

**NOTE!** When defining a template, make sure that the responsible Key Custodians have the appropriate privileges to apply it.

To delete an existing template:

**a.** Locate and select the template in the table.

**b.** Click on the **Delete** button.

**c.** When prompted, confirm whether you really want to delete the template.

To create a new template based on the settings of an existing one:

**a.** Locate and select the template in the table.

**b.** Click on the **Clone** button.

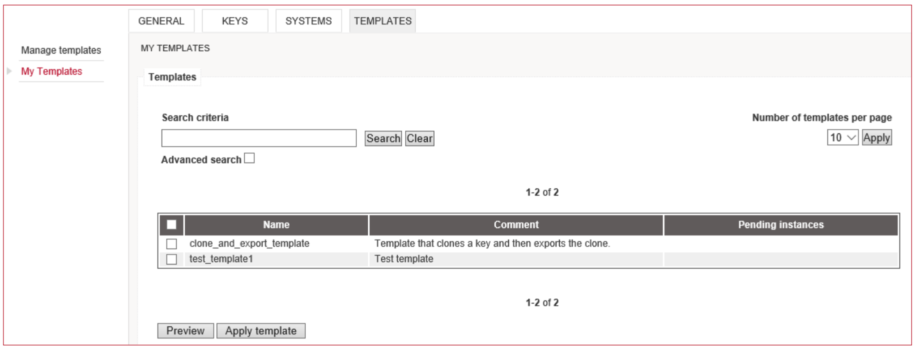
**c.** Make the necessary modifications. Note that the template name needs to be different from the one of the original template.

**d.** Click **Apply** to save the new template.

# Applying templates

To view and search all available templates, go to **Templates > My Templates**. For each template, its comment and any pending instances are displayed alongside the template name in the table. The number of templates shown per page is selectable in the top right corner. You can search for templates by entering a search string in the **Search criteria** field and clicking on **Search**. This will trigger a basic search based on the template name only. Select the **Advanced search** checkbox to include searching according to the system to which the template can be applied.

To preview the details of a template, the tasks it comprises and any pending instances, select a template in the table and click **Preview**.



| □ | Name | Comment | Pending instances |
|---|---|---|---|
| □ | clone_and_export_template | Template that clones a key and then exports the clone. | |
| □ | test_template1 | Test template | |

To apply a template:

**a.** Select the template in the table.

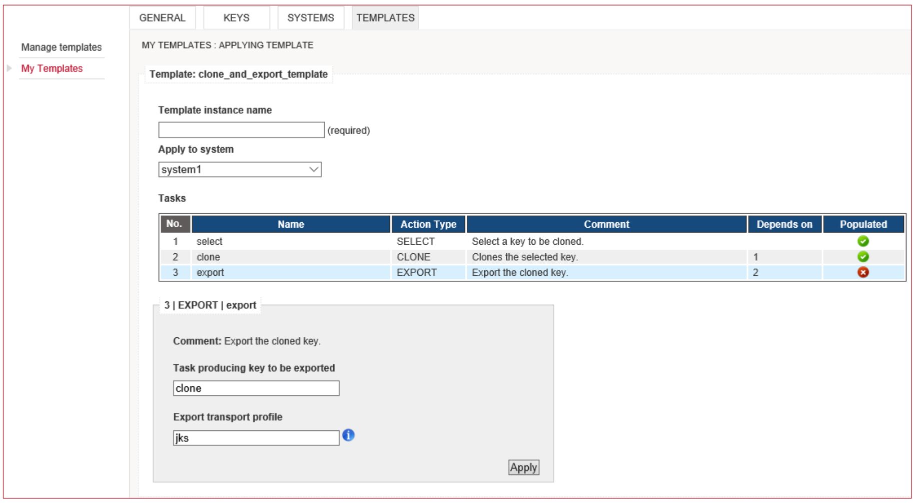
**b.** Click **Apply**.

**c.** (Optional) Enter a unique template instance name.

**Information Box**
If the template requires dual control, a pending template instance is created and the user needs to provide a unique name which will later be used by other Key Custodians to cancel or complete the template execution. If the template entails no dually controlled actions, it is applied immediately, without creating a pending template instance.

**d.** Select the system to which the template will be applied from the drop-down menu.

**e.** Populate the necessary parameters for each of the tasks within the template and click **Apply**. The task which is currently being applied is shown in the pane below the **Tasks** table. Once a task has been correctly populated, it is marked with a check mark in the table.



Template: clone_and_export_template

Template instance name: (required)

Apply to system: system1

Tasks

| No. | Name | Action Type | Comment | Depends on | Populated |
|---|---|---|---|---|---|
| 1 | select | SELECT | Select a key to be cloned. | | ✓ |
| 2 | clone | CLONE | Clones the selected key. | 1 | ✓ |
| 3 | export | EXPORT | Export the cloned key. | 2 | ✗ |

3 | EXPORT | export

**Comment:** Export the cloned key.

Task producing key to be exported: clone

Export transport profile: jks

**NOTE!** Most parameters of a task are pre-defined within the template and merely need to be confirmed at the point of their execution. The exceptions are Select, where a specific key has to be selected, and Generate, where the elements that can be modified include key name, key identifier, validity time and notification time.

**f.** After populating all the tasks, click **Apply template.**

**g.** When prompted, confirm whether you really want to apply the template.

To complete the execution of a dually controlled template:

**Go to Templates > My Templates**

**a.** Select the template in the table.

**b.** Click **Preview**.

**c.** Locate the table **Pending instances** and click **Complete**.

**d.** If the task to be completed is exporting a key in one of the password-protected file formats, one of the responsible Key Custodians will need to provide the password before the other can acquire the file.

**e.** When prompted, confirm whether you really want to complete the template instance.

A pending template instance can be cancelled at any time, either by the Key Custodian who initiated its execution or by others with an appropriate set of privileges. To cancel a pending template instance, follow the same steps as for completing it and click **Cancel** in the table **Pending instances**.

CHAPTER 5

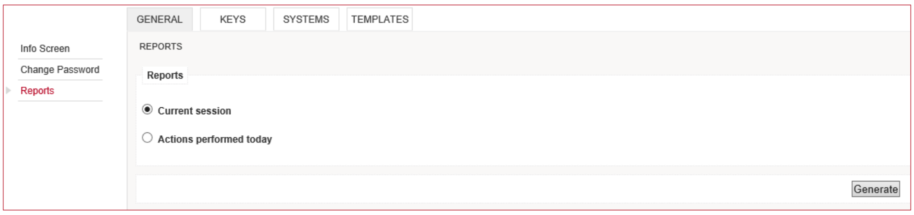
# REPORTS

Chiave Admin and Key Management applications have an engine for generating reports about the information stored in Chiave's database. Some reports are pre-installed on the appliance.

For reports that are not already bounded by a time frame or HTTP session ID, Chiave offers the possibility of including either all results that match the criteria of the report or only the events that occurred since the last report was generated.

To generate a report:

### Go to Reports



● Current session

○ Actions performed today

**a.** Select one of the reports and click **Generate**.

**b.** If a report of this kind has been generated before, select whether you wish to include all events that match the report criteria or only those that have occurred since the last report was generated.

**c.** In the presented file dialogue select a filename to save the report.

To acquire one or more new report definitions that are to replace the existing ones, contact a Chiave Administrator who can then receive new report definitions from Verisec support and upload them to the appliance.

# APPENDIX A – KEY FORMAT SAMPLES

1. The following is an example of Atos file format:

```
[GeneralParameters]
GenerationDateTime=10/08/2012 14:50:44
[EncryptedKey]
KEY_TYPE=DES
KEY_TAG=verisec_atos_key
KEY_NAME=1_2tdes
ENC_MODE=ECB
TRANSPORT_KEYTYPE=DES
TRANSPORT_KEY_INSTANCE=00
CV_METHOD=NORM
CV=0B08B0
ENC_KEY=510BEEAC3AD3FEC7E3F8643871500A0C
```

2. The following is an example of XML file format, with the mode IV-CBC without padding:

```
<?xml version="1.0" encoding="UTF-8"?>
<KeyContainer Version="1.0"
xmlns="urn:ietf:params:xml:ns:keyprov:pskc"
xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
xmlns:xenc11="http://www.w3.org/2009/xmlenc11#"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<EncryptionKey>
<ds:KeyName>Pre-shared key</ds:KeyName>
</EncryptionKey>
<KeyPackage>
<Key Id="1_2tdes" Algorithm="urn:verisec_key">
<Data>
<Secret>
<EncryptedValue>
<xenc:EncryptionMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#tripledes-cbc"/>
<xenc:CipherData>
<xenc:CipherValue>trb+deAATd4HMOHckNCObmu4pyvxubUyXl6e3kCWHMw
=</xenc:CipherValue>
</xenc:CipherData>
</EncryptedValue>
<ValueMAC>0B08B0F8</ValueMAC>
</Secret>
```

```
</Data>
<Extensions>
<VerisecKeyExtension>
<KeyType>2TDES</KeyType>
<MachineCreationDate>1344602819207</MachineCreationDate>
<CreationDate>10/08/2012 14:46:59</CreationDate>
<TransportKeyType>2TDES</TransportKeyType>
<Description/>
</VerisecKeyExtension>
</Extensions>
</Key>
</KeyPackage>
</KeyContainer>
```