Smart ID Blueprints

Supported Use Cases

⚠ **C0 Public Document**
Nexus property.

Identification of the document		
No pages: 37	**State:** published	**Reference:** Product Management
Creation date: 10/21/2025	**Last updated:** 7/1/2026	**Version:** 1.2

Version history			
Version	**Author**	**Date**	**What changes were made, where**
1.0	Stefanie Lenhard	2025-10-21	First draft
1.1	Stefanie Lenhard	2026-02-04	• Added two use case descriptions “Enroll FIDO2 token in Entra” and “Delete FIDO2 token from Entra”. • Added database attributes • Added the description of the use cases “Synchronize active/inactive LDAP users”
1.2	Stefanie Lenhard	2026-07-01	• Added Mobile ID use cases • Added LDAP search option for user creation and configuration visibility of user creation options • Smaller improvements
		Click or tap to enter a date.	
		Click or tap to enter a date.	
		Click or tap to enter a date.	

This document and the software described in it are copyrighted

© 2026 Technology Nexus Secured Business Solutions AB. All rights reserved.

All other trademarks and service marks are the property of their respective owners.
Information in this document is subject to change without prior notice.

Table of Contents

Smart ID Blueprints 5
1.1 Purpose of document 5
1.2 Scope 5
1.3 Abbreviations and definitions 5
2 Users 5
3 Cards 6
3.1 Physical smart card 6
3.2 Temporary card 6
3.3 Virtual smart card 6
4 Use case overview 6
4.1 Use case conventions 6
4.2 Options 7
5 Operators use cases 8
5.1 User Management 8
5.1.1 User attributes 8
5.1.2 Create user 10
5.1.3 Synchronize active LDAP users 11
5.1.4 Synchronize inactive LDAP users 11
5.1.5 Deactivate user 11
5.1.6 Reactivate user 12
5.1.7 Lock user 13
5.1.8 Edit user 14
5.1.9 Delete user 15
5.1.10 Reset password 15
5.1.11 Edit roles 16
5.1.12 Reset password for multiple users 16
5.1.13 Edit roles for multiple users 17
5.1.14 Delete multiple users 17
5.1.15 Expiry checks 18
5.2 Certificate Management 18
5.2.1 Certificate attributes 18

⚠ **C0 Public Document**
Nexus property.

5.2.2 Issue user certificate in PKCS#12 format 20
5.2.3 Display password 21
5.2.4 Revoke certificate 21
5.3 Card Management 22
5.3.1 Card attributes 22
5.3.2 Request card 25
5.3.3 Issue card 25
5.3.4 Recover certificates on user card 26
5.3.5 Renew card 27
5.3.6 Edit card 28
5.3.7 Deactivate card 28
5.3.8 Reactivate card 28
5.3.9 Lock card 29
5.3.10 Unblock card remote 29
5.3.11 Request multiple cards (Batch orders) 30
5.3.12 Issue multiple cards (Batch orders) 30
5.4 Temporary card management 31
5.4.1 Temporary card attributes 31
5.4.2 Request temporary card 31
5.4.3 Issue multiple temporary cards 32
5.4.4 Assign temporary card 32
5.4.5 Extend temporary card 34
5.4.6 Withdraw temporary card 34
5.4.7 Lock temporary card 35
5.5 Virtual smart card management 35
5.5.1 Virtual smart card attributes 35
5.5.2 Deactivate virtual smart card 35
5.5.3 Reactivate virtual smart card 36
5.5.4 Delete virtual smart card 36
5.6 Passkey management 37
5.6.1 Passkey attributes 37
5.6.2 Enroll FIDO2 token in Entra 37
5.6.3 Delete FIDO2 token from Entra 38

⚠ **C0 Public Document**
Nexus property.

5.7 Mobile ID management 38
5.7.1 Mobile ID attributes 38
5.7.2 Supply Mobile ID for user 38
5.7.3 Deactivate Mobile ID 39
5.7.4 Reactivate Mobile ID 40
5.7.5 Lock Mobile ID 40
6 Self-Service use cases 42
6.1 User management 42
6.1.1 Change password 42
6.1.2 Edit photo 42
6.2 Card Management 43
6.2.1 Unblock/Change PIN 43
6.2.2 PIN Unblock offline 43
6.2.3 Renew card 44
6.3 Virtual smart card management 45
6.3.1 Get virtual smart card 45
6.3.2 Change PIN for a virtual smart card 46
6.3.3 Lock virtual smart card 47
6.4 Mobile ID management 47
6.4.1 Get Mobile ID 47
6.4.2 Lock Mobile ID 48
7 Roles vs use cases in Smart ID Blueprints 49

⚠ **C0 Public Document**
Nexus property.

Smart ID Blueprints

The Smart ID Blueprints provides preconfigured processes to issue, manage, and use trusted user identities.

These identities can be provided as physical smart cards, virtual smart cards, or passkeys. Workforce identities are typically corporate ID cards or virtual smart cards deployed on employees' phones and laptops. They can be used for both physical and digital access, reducing the need for multiple passwords, cards, or tokens.

1.1 Purpose of document

This document describes all Digital ID use cases included in the Smart ID Blueprints.
Its purpose is to provide a clear and consistent understanding of the available user interactions and system behavior for all relevant stakeholders.

1.2 Scope

The document focuses on the functional use cases of the Digital ID system, including:

- User lifecycle management (creation, importing, deactivation, etc.)
- Card lifecycle management (request, deactivate, assign temporary card, etc.)
- Self-Service actions available to end users

1.3 Abbreviations and definitions

Definition	Comment
IDM	Identity Manager
CM	Certificate Manager
VSC	Virtual Smart Card
PKI	Public Key Infrastructure

2 Users

There can be multiple types of users in an organization, such as employees, contractors, visitors, trainees and pupils. The users are the consumers of the credentials and use them every day, for example to login to their computer using Smart Card, authenticate themselves to access intranet or using the qualified certificate to sign a document.

⚠ **C0 Public Document**
Nexus property.

3 Cards

3.1 Physical smart card

Smart cards are a secure form of identity credential used within Identity systems to enhance authentication and access control. Each smart card issued to a user typically contains digital certificates supporting authentication, digital signature, and encryption use cases. The lifecycle of a smart card - from issuing and activation to renewal or revocation - can be managed either by an operator or directly by the user through the self-service portal.

3.2 Temporary card

A time-limited card used to grant temporary access while a permanent card is being produced or replaced. It can also be issued to guests, contractors, or other temporary visitors who need short-term access.

3.3 Virtual smart card

The Virtual Smart Card (VSC) provides the same digital capabilities as a physical smart card, such as multifactor authentication (MFA) to digital resources, Windows logon, digital signing, and certificate-based authentication. Unlike physical smart cards, the VSC cannot be used for visual identification or physical access.

VSCs are provisioned and managed through the Nexus Smart ID Desktop App, which enables secure issuance and lifecycle management of virtual credentials. The related use cases are described under Card Management.

4 Use case overview

4.1 Use case conventions

Each use case in this document follows a consistent structure to ensure clarity and comparability.

Actors: the main role(s) interacting with the system (e.g., Operator, Approver or Self-Service User)

Process kinematic: Step-by-step description of the process.

Options: Configurable parameters or behaviors within the use case, e.g. enabling/disabling approvals.

⚠ **C0 Public Document**
Nexus property.

4.2 Options

Within the provided Smart ID Blueprints, options exist to meet customer requirements.

For example, an approval process can be enabled or disabled for any process that modifies the lifecycle of a user, a certificate, or a card. These options are set globally and therefore apply to all related processes and are managed through scripts.

These are the option scripts available:

Script Name	Description
UsersScriptOptions	Script to set options in user processes
UsersCertScriptOptions	Script to set user certificate options
CardsScriptOptions	Script to set options in cards processes
TempCardsScriptOptions	Script to set options in temporary cards processes
VirtualSmartCardScriptOptions	Script to set options for processes around virtual smart card
MobileIDScriptOptions	Script to set options for processes around mobile ID profiles

In the following is an example how to manage the option to have an approval step for the deactivation of a user.

1. Log in to Identity Manager Admin.
2. In Identity Manager Admin, go to **Home > Scripts.**
3. Select the script **UsersScriptOptions**
4. In the section **Approvals** in the script, go to the **UsersDeactivationApproval** variable. By default, it is set to **false,** that is, there is no approval step when a user is created.

Example:

```
/*
Defines if user deactivation require approval.
Possible options:
 * true - Approval steps are enabled.
 * false - Approval steps are disabled.
*/
UsersDeactivationApproval = false
```


⚠ C0 Public Document
Nexus property.

5. If you want to have an approval step when deactivating a user, set **UsersDeactivationApproval** to **true**.
6. Click **Save** in the upper left corner to save the updated script

5 Operators use cases

The following cases are supported within the Smart ID Identity Manager Operator Web Application. These tasks are typically performed by an Operator or other administrative roles with similar permissions.

End users perform corresponding actions for themselves through the Self-Service Use Cases, which are described in the chapter Self-Service use cases.

5.1 User Management

The Smart ID Blueprints delivers a set of best practice use cases for how to create, deactivate or lock a user, and more, during the full life cycle.

In many environments, user data is maintained in an Active Directory (AD) or a Human Resource (HR) system. The Smart ID Identity Manager can automatically import this data through an **LDAP synchronization process**, which is part of the Smart ID Blueprints.

5.1.1 User attributes

The standard user attributes defined in the Smart ID Blueprints are:

Field name	Type	Mandatory	Example	Visible in interface
Created	Date with time	Yes	Set the creation date	No
Email	Text	Yes	Set the date when the record changes	Yes
First name	Text	Yes	John	Yes
Last name	Text	Yes	Smith	Yes
Updated	Date with time	Yes	Set the date when the record changes	No
User status	Text	Yes	Active / Inactive	Yes
Template	Text	Yes	Object Template e.g. User, Card	No

⚠ C0 Public Document
Nexus property.

Title	Text	No	Doctor	No
User number	Text	Yes	Calculated automatically by IDM	Yes
Organizational unit (OU)	Text	Yes	Nexus	Yes
Organization (O)	Text	Yes	INGroupe	Yes
Country	Text	No	France	No
Photo	Binary Data	No	User Photo	Yes
Signature	Binary Data	No	User Signature	No
Username	Text	No	john.smith	No
CN	Text	Yes	John Smith	Yes
User principal name	Text	Yes	john.smith@company.com	Yes
Source	Text	Yes	Ldap	Yes
Password	Password	Yes	User password for Smart ID Self-Service	No
Password reference	Encrypted field	Yes	Reference key used to retrieve the actual password	No
Valid from	Date	No	Meta field	No
Valid to	Date	No	Meta field	No
Comment	Text	No	Meta field	No
Reason	Text	No	Meta field	No
ObjectGUID	Text	No	Globally unique identifier of the object	No
PIN	Encrypted field	No	Pin field	No
Organization ID	Text	No	Meta field	No
Identifier	Text	No	ID card, passport	Yes
Entra UserID	Text	No	Entra ID for a registered Entra user	Yes

⚠ **C0 Public Document**
Nexus property.

5.1.2 Create user

Actors: Operator

Process kinematic: The Smart ID Blueprints provides a process to create a user manually,by csv import or LDAP search.

The process can be launched from the user **Quick Search** menu and is composed of the following steps:

Step 1:
The input source is selected by the responsible manager or registration office from the following options:

- Manual: User data is entered manually.
- CSV: A CSV file containing multiple users is imported. The required CSV format is defined by the Smart ID Identity Manager, and the necessary fields are displayed within the form.
- LDAP: User data is retrieved from an LDAP directory. A user can be searched for and selected from the available LDAP entries.

Step 2:
If an approval step is configured (see Options), an approver must validate the request.

Step 4:
If needed, IDM generates a password in its internal database and prints the password letter or sends it by mail.

Options included in this process

These options can be customized:

- Add an approval step
- Activate uniqueness check based on email
- Define maximum size of photo
- Define user status after creating, “Active” or “Inactive”
- Password management:
  - Send password by email
  - Print a password letter
  - Do not share the password
- Define the available user creation methods. Set a method to true to make it visible and selectable in IDM Operator:
  - Manual
  - CSV
  - LDAP

⚠ C0 Public Document
Nexus property.

5.1.3 Synchronize active LDAP users

Actor: Scheduled job (automatic)

Process kinematic: The synchronization of active LDAP users can be controlled via the Identity manager component “Scheduled Job”. With Smart ID Blueprints, we provide two preconfigured scheduled jobs that automatically synchronize active and inactive users via the LDAP interface.

Step 1:
Log in to Identity Manager Admin with your administrator account.

Step 2:
Select **Synchronize active LDAP users**

Step 3:
To adjust the scheduler, type the appropriate cron expression in the **Expression to schedule the job.**

Step 4:
Click **Save**

5.1.4 Synchronize inactive LDAP users

Actor: Scheduled job (automatic)

Process kinematic: The synchronization of inactive LDAP users can be controlled via the Identity manager component “Scheduled Job”.

Step 1:
Log in to Identity Manager Admin with your administrator account.

Step 2:
Select **Synchronize inactive LDAP users**

Step 3:
To adjust the scheduler, type the appropriate cron expression in the **Expression to schedule the job.**

Step 4:
Click **Save**

5.1.5 Deactivate user

Actor: Operator

Process kinematic: This process can be automatically called during LDAP sync when a user has been deactivated. The process can also be executed by operators on the web interface.

Step 1:
The process can be launched from the users search view or from the detailed view of a user.

⚠ **C0 Public Document**
Nexus property.

After execution the web page displays some user attributes:

- First name
- Last name
- Email
- Organization
- Organizational Unit
- Photo

The operator selects the reason for deactivation. The list of reasons must be defined by the customer for example:

- Parental leave
- Temporarily deactivated
- Other

Step 2:
If an approval step is configured (see Options), an approver must validate the request.

Step 3:
The user is deactivated; all credentials are deactivated and related certificates linked with the user will be set as “Certificate hold” or revoked if the PKI and/or connector doesn’t support this status.

When a user is in “Inactive” status, the available workflows are:

- Reactive user
- Lock user
- Reset password

Options included in this process

These options can be customized:

- Add an approval step

5.1.6 Reactivate user

Actors: Operator

Process kinematic: This process can be automatically called during LDAP sync when a user has been reactivated. The process can also be executed by operators on the web interface.

Step 1:
The process can be launched from the users search view or from the detailed view of a user.

After execution the web page displays some user attributes:

- First name

⚠ C0 Public Document
Nexus property.

- Last name
- Email
- Organization
- Organizational Unit
- Photo

The operator selects the reason for reactivation. The list of reasons must be defined by the customer, for example:

- Back after parental leave
- Other

Step 2:
If an approval step is configured (see Options), an approver must validate the request.

Step 3:
The user is reactivated, all credentials are reactivated, and the related certificates are switched to valid status.

Options included in this process

These options can be customized:

- Add an approval step

5.1.7 Lock user

Actors: Operator

Process kinematic: This process can be automatically called during LDAP sync when a user has been locked. The process can also be executed by operators on the web interface. The difference to the **Deactivate user** process is that the user and their credentials cannot be reactivated. The credentials are definitively revoked.

Step 1:
The process can be launched from the users search view or from the detailed view of a user.

After execution the web page displays some user attributes:

- First name
- Last name
- Email
- Organization
- Organizational Unit
- Photo

The operator selects the reason for locking. The list of reasons must be defined by the customer.

⚠ **C0 Public Document**
Nexus property.

Step 2:
If an approval step is configured (see Options), an approver must validate the request.

Step 3:
The user is locked, all credentials are locked, and the related certificates are switched to revoked.

When a user is in “locked” status, the only available process is

- Delete user

Options included in this process

These options can be customized:

- Add an approval step

5.1.8 Edit user

Actors: Operator

Process kinematic: This process can be automatically called during LDAP sync when the user has changed. The process can also be executed by operators on the web interface.

Step 1:
The process can be launched from the users search view or from the detailed view of a user.

After execution the web page displays some user attributes:

- First name
- Last name
- Email
- Organization
- Organizational Unit
- Photo
- Title
- Identifier

Step 2:
If an approval step is configured (see Options), an approver must validate the request.

Step 3:
The operator enters attributes values and validates.

Options included in this process

These options can be customized:

- Add an approval step

⚠ **C0 Public Document**
Nexus property.

- Uniqueness check based on the email address

5.1.9 Delete user

Actors: Operator

Process kinematic: This process can be automatically called during LDAP sync when the user has been deleted. The process can also be executed by operators on the web interface.

Step 1:
The process can be launched from the users search view or from the detailed view of a user.

5.1.10 Reset password

Actors: Operator

Process kinematic: The Smart ID Blueprints provides a process to reset a user's password.

Step 1:
The process can be launched from the users search view or from the detailed view of a user.

After execution the web page displays some user attributes:

- First name
- Last name
- Email
- Organization
- Organizational Unit

The operator selects a password delivery method:

- Print password letter
- Send password by mail

IDM generates a password corresponding to the internal policy and assigns it to the user. Depending on the choice, a password letter is printed, or the password is sent by mail.

Options included in this process

These options can be customized:

- Configure password policy
  - Password length
  - List of characters used in password

⚠ **C0 Public Document**
Nexus property.

5.1.11 Edit roles

Actors: Operator

Process kinematic: The Smart ID Blueprints provides a process to edit roles of a user manually.

The Smart ID Blueprints provides a preconfigured role list (described in Roles vs use cases in Default Configuration)

Step 1:
The process can be launched from the users search view or from the detailed view of a user. A web page displays the roles currently assigned to the user.

Step 2:
The operator adds or removes the roles from the user profile.

Step 3:
If an approval step is configured (see Options), an approver must validate the request.

Options included in this process

These options can be customized:

- Add an approval step

5.1.12 Reset password for multiple users

Actors: Operator

Process kinematic: The Smart ID Blueprints provides a process to reset password for multiple users.

Step 1:
The process can be launched from the user batch order view.

Operator searches for users in the dedicated search screen. The search attributes are:

- User status
- First name
- Last name
- Email
- Organization
- Organizational Unit

Step 2:
The operator selects the user to reset the password (checkbox user by user or one page in one click) and starts the reset password process.

Step 3:
IDM lists the users affected by the password reset.

⚠ C0 Public Document
Nexus property.

Step 4:
Upon successful completion, a new password is generated for each user, and an email notification is sent out to the listed users.

5.1.13 Edit roles for multiple users

Actors: Operator

Process kinematic: The Smart ID Blueprints provides a process to edit roles for multiple users.

Step 1:

The process can be launched from the user batch order view.

Operator searches for users in the dedicated search screen. The search attributes are:

- User status
- First name
- Last name
- Email
- Organization
- Organizational Unit

Step 2:
The operator selects the users to assign new roles (checkbox user by user or one page in one click).

Step 3:
IDM lists the users, and the operator selects the roles to be assigned.

5.1.14 Delete multiple users

Actors: Operator

Process kinematic: The Smart ID Blueprints provides a process to delete multiple users which is disabled by default. This process can be automatically called during LDAP sync when the user has been deleted. The process can also be executed by the operator on the web interface.

Step 1:
The process can be launched from the user batch order view.

Operator searches for users in the dedicated search screen. The search attributes are:

- User status
- First name
- Last name
- Email
- Organization
- Organizational Unit

⚠ **C0 Public Document**
Nexus property.

Step 2:
The operator selects the user to be removed.

Step 3:
IDM displays the list of users to be removed.

5.1.15 Expiry checks

The Smart ID Blueprints includes processes that remind users when their credentials are about to expire or have already expired. Reminders can be configured for the following types:

- Expiring user certificates
- Expiring cards
- Expiring temporary cards
- Expiring virtual smart cards
- Expired cards
- Expired user certificates

Options included in this process

These options can be customized:

- Option to send reminder emails
  - Email will be sent out every day
- Option to set up how often to send emails regarding expired or expiring cards

5.2 Certificate Management

The Smart ID Blueprints provides a set of best practice use cases for issuing a P12 certificate directly to a user, displaying the P12 certificate password and revoking the certificate.

5.2.1 Certificate attributes

The standard certificate attributes defined in the Smart ID Blueprints are:

Field name	Type	Mandatory	Example	Visible in interface
Created	Date with time	Yes	Set the creation date	No
Issuer	Text	Yes	CN=ING Functional user CA, O=Nexus, C=FR	Yes

⚠ C0 Public Document
Nexus property.

KeyArchival	Number	No		No
Comment	Text	No	Meta field	No
Reason	Text	No	Meta field	No
Status	Text	Yes	Valid	Yes
Template	Text	Yes	User P12 Certificate	Yes
Renewal started	True/False	No	Renewal reminder sent	No
Valid from	Date	Yes	03/05/2026	Yes
Valid to	Date	Yes	04/05/2026	Yes
Email	Text	Yes	Copy from the user record	Yes
Data	Binary Data	Yes	Certificate data/file	No
CN	Text	Yes	Copy from the user record	Yes
User principal name	Text	Yes	Copy from the user record	Yes
Subject	Text	No	Set by IDM	No
P12 PasswordHash	Password	Yes	Set by IDM	No
P12 Password	Encrypted field	Yes	Set by IDM	No
Organization (O)	Text	No	Copy from the user record	Yes
Organization (OU)	Text	No	Copy from the user record	Yes
Serial number	Text	Yes	Chip serial number (ICCSN)	No
Certificate S/N	Text	Yes	7609480fd736272a9669d61a3eeb0b71	Yes
DNS	Text	No	Set by IDM	No
Country (C)	Text	No	France	No
State (S)	Text	No	Paris Region	No
Locality (L)	Text	No	Paris	No
URI	Text	No	Set by IDM	No
Key size	Text	No	2048	Yes

⚠ **C0 Public Document**
Nexus property.

Key type	Text	No	RSA	Yes
Key usage	Text	No	dataEncipherment, keyEncipherment, nonRepudiation, digitalSignature	Yes
Extended key usage	Text	No	Code Signing, Client Authentication, Secure E-mail	Yes
Hash algorithm	Text	No	SHA256	Yes
CDP	Text	No	Set by IDM	Yes
AIA OCSP	Text	No	Set by IDM	Yes
Subject DN	Text	No	EMAILADDRESS=john.smith@ingroupe.com, T=Registration Officer, PSEUDONYM=CP_UserP12, GIVENNAME=John, SURNAME=Smith, CN=John Smith, OU=Registration Office, O=Registration Office, C=FR	Yes
Issuer DN	Text	No	Set by IDM	No
IP	Text	No	Set by IDM	No
GUID	Text	No	Set by IDM	No
RID	Text	No	Set by IDM	No
P12 certificate data	Encrypted field	Yes	Certificate data/field	No
ImportedCardICCSN	Text	No	Set by IDM	No

5.2.2 Issue user certificate in PKCS#12 format

Name: Issue P12 certificate

Actors: Operator

Process kinematic: The Smart ID Blueprints provides a process to issue a certificate for an existing user.

Step 1:
The process can be launched from the users search view or from the detailed view of a user. The operator selects the process “Issue P12 certificate”.

Step 2:
The operator needs to select the certificate template.

⚠ **C0 Public Document**
Nexus property.

Step 3:
The certificate is issued for the selected template. A web page allows you to download the P12 file and the pem (public part) of the generated certificate. The password is displayed on the same page.

Step 4:

The certificate is sent by email to the end user.

Options included in this process

These options can be customized:

- Notification settings:
  - Possibility to send P12 password by email after certificate has been issued

5.2.3 Display password

Name: Display password

Actors: Operator

Process kinematic: The Smart ID Blueprints provides a process to display the password stored for a P12 certificate already issued for a user.

Step 1:
The process can be launched from the certificate search or detailed view of a P12 certificate.

Options included in this process

These options can be customized:

- Notification settings:
  - Possibility to send P12 password by email after certificate has been issued

5.2.4 Revoke certificate

Name: Revoke certificate

Actors: Operator

Process kinematic: The Smart ID Blueprints provides a process to revoke a PKCS#12 certificate.

Step 1:
The process can be launched from the certificate search or detailed view of a P12 certificate.

Step 2:
All information contained in the certificate are displayed on the screen.

⚠ C0 Public Document
Nexus property.

Step 3:
The operator selects the reason why the certificate should be revoked amongst:

- Cessation of activity
- Change of affiliation
- Key compromised
- Privileged removal

Step 4:
Certificate is revoked

5.3 Card Management

The Smart ID Blueprints includes a set of best practice use cases for how to issue a card, change PIN for a card or lock a card. and more, during the full life cycle.

Cards and middleware

The cards used in the Smart ID Blueprints are Thales IDPrime MD 830. Other cards can also be evaluated and supported, provided that the vendor offers a middleware based on the PKCS#11 standard.

These cards will be accessed from the CMS web browser through two different applications deployed on Windows computers:

- **Nexus CardSDK,** for operators realizing printing and contact chip encoding (contactless encoding in options).
- **Nexus SmartID Desktop App**, for:
  - operator realizing contact chip encoding only (no printing, no contactless encoding), for example PIN unlock or certificate renewal
  - end user realizing contact chip encoding (change / unblock PIN, renew certificates).

On each card attached to a user, typically 3 certificates will be deployed:

- Authentication
- Signature
- Encryption
- (optional) recover previous encryption certificate

5.3.1 Card attributes

The standard card attributes defined in the Smart ID Blueprints are:

⚠ C0 Public Document
Nexus property.

Field name	Type	Mandatory	Example	Visible in interface
Number	Text	Yes	Internal ID generated by IDM	Yes
First name	Text	Yes	Copy from user	Yes
Last name	Text	Yes	Copy from user	Yes
Title	Text	Yes	Copy from user	Yes
Organizational unit (OU)	Text	Yes	Copy from user	Yes
Organization (O)	Text	Yes	Copy from user	Yes
Country	Text	No	Copy from user	No
Photo	Binary data	No	Copy from user	No
Signature	Binary data	No	Copy from user	No
Email	Text	Yes	Copy from user	Yes
CN	Text	Yes	Copy from user	Yes
User principal name	Text	Yes	Copy from user	Yes
Card image (Back)	Image	Yes	Card layout	No
Card image (Front)	Image	Yes	Card layout	No
User number	Text	No	Copy from user	No
Valid from	Date	Yes	03/05/26	Yes
Valid to	Date	Yes	03/05/27	Yes
Renewal started	True/False	Yes	Renewal reminder sent	No
PIN	Encrypted field	Yes	PIN code of the card	No
PUK	Encrypted field	Yes	PUK code of the card used to unblock card	No
Admin Key	Encrypted field	No	Set by IDM	No
ICCSN	Text	No	Set by IDM	No
External ID	Text	No	Set by IDM	No
Mifare	Text	No	Set by IDM	No
EM	Text	No	Set by IDM	No

⚠ **C0 Public Document**
Nexus property.

IDCUser ID	Text	No	Set by IDM	No
Profile ID	Text	No	Set by IDM	No
Created	Date with time	Yes	Set by IDM	No
Updated	Date with time	Yes	Set by IDM	No
Status	Text	Yes	Valid	Yes
Comment	Text	Yes	Set by IDM	No
Reason	Text	Yes	Set by IDM	No
Template	Text	Yes	Card	No
RequestEncryptionCertificate	True/False	Yes	Set by IDM	No
RequestAuthenticationCertificate	True/False	Yes	Set by IDM	No
RequestSignatureCertificate	True/False	Yes	Set by IDM	No
Order ID	Text	Yes	Set by IDM	No
Production type	Text	Yes	Set by IDM	No
Imported user email	Text	Yes	Set by IDM	No
Entra UserID	Text	No	john.smith@ingroupe.com	No
Entra MethodID	Text	No	Set by IDM	No
EntraCredentialResponse1	Text	Yes	Set by IDM	No
EntraCredentialResponse2	Text	Yes	Set by IDM	No
EntraCredentialResponse3	Text	Yes	Set by IDM	No
EntraCredentialResponse4	Text	Yes	Set by IDM	No
EntraCredentialResponse5	Text	Yes	Set by IDM	No
EntraCredentialResponse6	Text	Yes	Set by IDM	No
EntraCredentialResponse7	Text	Yes	Set by IDM	No
EntraCredentialResponseCount	Number	Yes	Set by IDM	No

⚠ **C0 Public Document**
Nexus property.

5.3.2 Request card

Actors: Operator, Approver

Process kinematic: The Smart ID Blueprints provides a process to request a card for an existing user in active status. This process is used when the operator requesting the card can't directly produce the card (another person is required), or when an approval is required. If no approval is wanted, and the operator has the right to issue the card, they can use directly the "Issue card" process.

Step 1:
The process can be launched from the users search or detailed view of a user. The operator has a view of all data information of the user.

Step 2:
The operator checks the data and clicks on "Next".

Step 3:
A message is displayed to the operator that the card has been requested and is waiting for approval.

Step 4:
Approver: from the "Search view" page related to "Requests", all the cards waiting for approval with status "requested" are displayed.

Step 5:
Approver: select the card request for the user and launch process "Card approval".

Step 6:
Approver: A form is displayed, with all data related to the user. Then, the operator can reject, accept or postpone the request.

Step 7:
Approver:

- If "approve" is selected, then the card is in state: "approved" and no longer displayed to the approbator. An email is sent to the requester. The operator can take back the process and launch card production ("Issue card")
- If "reject" is selected, then the approbator can choose a reason why the request is rejected (drop down list) and add a custom comment in a text zone. An automatic email is sent to the requester.
- If "postpone" is selected, then the approbation is still pending.

5.3.3 Issue card

Actor: Operator

Process kinematic: The Smart ID Blueprints provides a process to issue a card for an existing user.

Step 1:
The process can be launched from the users search view or from the detailed view of a user.

⚠ **C0 Public Document**
Nexus property.

Step 2:
Smart ID Desktop App or CardSDK is launched and the operator is asked to select their card reader. The certificates are issued, then the PIN & PUK code are generated, and the PIN is printed in a PIN letter. The Operator prints the PIN letter. The card state is “active”.

Options included in this process

These options can be customized:

- Card activation:
  - Possibility to not activate the certificates issued directly after the card encoding and add an activation workflow. (card state can be active/inactive)
- PIN/PUK management:
  - Possibility to send PIN/PUK by email or print PIN/PUK letter during card issuance
  - Possibility to choose PIN length (6 by default)
  - Possibility to choose PUK length (8 by default)
- Number of cards:
  - Possibility to limit the number of cards that a user can have at the same time (2 by default)
- Certificates:
  - Possibility to choose to deliver the following certificates during the process:
    - Authentication (Yes/no)
    - Signature (Yes/no)
    - Encryption (Yes/no)
- Card printing: IDM can print the card using CardSDK instead of Smart ID Desktop App on step 3. In this case the card printing Layout is defined in the beginning of the project.
- Recovery of encrypted certificates
  - Possibility to enable certificate retrieval during card issuance (a form displays the list of existing certificates that are recoverable)

5.3.4 Recover certificates on user card

Actors: Operator

Process kinematic: The Smart ID Blueprints provides a process to recover certificates on a user card.

Step 1:
The process can be launched from the users search view or from the detailed view of a user.

Step 2:
The operator must select which certificates need to be recovered (one or several depending on existing certificates).

⚠ C0 Public Document
Nexus property.

Step 3:
Smart ID Desktop App is launched; operator must accept to launch Smart ID Desktop App and click „open link“.

Step 4:
Smart ID Desktop App is launched; the operator is asked to select his card reader.

Step 5:
The PIN code of the smartcard is requested.

Step 6:
The encryption certificates are recovered and stored on the card. The card is in „active“ state.

5.3.5 Renew card

Actors: Operator

Process kinematic: The process “Renew” is used by the operator to issue new certificates on a card when the previous ones are about to expire or a renewal is required for other reasons.

Step 1:
The process can be launched from the card search or detailed view of a user card. The operator has a view of all card information. The operator checks the data and clicks on “Next”.

Step 2:
Smart ID Desktop App is launched; operator must accept to launch Smart ID App and click “open Link”.

Step 3:
The old certificates are erased from the card. The new certificates are issued, based on the same policy as the one used for “Issue card”. The PIN & PUK code remain the same.

The card is in “active” state

Options included in this process

These options can be customized:

- Certificates:
  - Possibility to choose to deliver the following certificates during the process:
    - Authentication (Yes/no)
    - Signature (Yes/no)
    - Encryption (Yes/no)
- Recovery of encrypted certificates
  - Possibility to enable certificate retrieval during card issuance (a form displays the list of existing certificates that are recoverable)

⚠ **C0 Public Document**
Nexus property.

5.3.6 Edit card

Actors: Operator

Process kinematic: Smart ID Blueprints provides a process to edit specific card information by an operator.

Step 1:

The process can be launched from the card search or detailed view of a user card.

Step 2:
The operator checks the data, modifies data if needed, and clicks on “Next” to save the changes. The data is saved.

5.3.7 Deactivate card

Actors: Operator

Process kinematic: Smart ID Blueprints provides a process to deactivate a card for a specific user. This card can be later reactivated. The certificates are put “Certificate hold” if the PKI supports this status. If the PKI doesn’t support ‘Certificate hold’, then we recommend using the “lock card” process.

Step 1:
The process can be launched from the card search or detailed view of a user card. The operator has a view of all data of the card and related to the user. The operator checks the data and clicks on “Next”.

Step 2:
The certificates deployed on the card are put „Certificate hold“ if the PKI supports this status, otherwise revoked. The card state is “inactive”.

Options included in this process

These options can be customized:

- Approval:
  - Possibility to add an approval step

5.3.8 Reactivate card

Actors: Operator

Process kinematic: Smart ID Blueprints provides a process to reactivate a card for a specific user. The card has been previously deactivated and is in inactive state. The certificates are put back on “valid” status. If the PKI doesn’t support “Certificate hold” status, then we recommend using “Renew” process to issue new certificates on this card.

⚠ C0 Public Document
Nexus property.

Step 1:
The process can be launched from the card search or detailed view of a user card. The operator has a view of all data of the card and related to the user. The operator checks the data and clicks on “Next”.

Step 2:
The certificates are put back on „valid“ state if the PKI supports this “Certificate hold” feature. The card state is “active”**.**

Options included in this process

These options can be customized:

- Approbation:
  - Possibility to add an approval step

5.3.9 Lock card

Actors: Operator

Process kinematic: Smart ID Blueprints provides a process to lock a card of a specific user and revoke all related certificates. A locked card cannot be reactivated.

Step 1:
The process can be launched from the card search or detailed view of a user card. The operator has a view of all data of the card and related to the user. The operator checks the data and clicks on “Next”.

Step 2:
The certificates are “revoked”. The card state is “locked”**.** No further operations can be done on this card.

Options included in this process

These options can be customized:

- Approval:
  - Possibility to add an approval step

5.3.10 Unblock card remote

Actors: Operator

Process kinematic: Smart ID Blueprints provides a process to unblock a card remotely. This allows a user to change the PIN code of a card. This workflow is used when the card has been blocked (3 wrong PIN code) or when the user forgot the PIN code. This is based on a challenge/response mechanism.

⚠ **C0 Public Document**
Nexus property.

Step 1:
The user contacts the operator and gives him the challenge code (for example generated in Windows logon screen or directly from the middleware).

Step 2:
From the page corresponding to the card, the operator selects the process “Unblock Card Remote”. The operator must enter the Challenge code given by the user. **Note:** The operator must validate that the user is the owner of the card by an external mechanism.

Step 3:
A response code is calculated and displayed to the operator who communicates this code in return to the user.

Step 4:
The user types the response code and is asked to enter a new PIN code. The PIN code is changed.

5.3.11 Request multiple cards (Batch orders)

Actors: Operator

Process kinematic: Smart ID Blueprints provides a process to request cards for multiple users. The card can then be issued through either single or mass production. (“Issue card” or “Issue multiple cards”).

Step 1:
From the register “Batch orders”, the operator selects the process “Request multiple cards”, and searches amongst the active users.

Step 2:
The operator selects the users by ticking them in the displayed list and launches the process “Request multiple cards”

Step 3:
A form is displayed, and the operator can check the selected users, order the list and click on “Next” to validate the card requests.

Step 4: The cards are now ordered and waiting for issuance either through “Issue card” or “Issue multiple cards” process. The card state is “approved”.

5.3.12 Issue multiple cards (Batch orders)

Actors: Operator

Process kinematic: Smart ID Blueprints provides a process to issue cards for multiple users. A request must be made before cards can be issued.

⚠ **C0 Public Document**
Nexus property.

Step 1:
From the register ‘Batch orders’**,** the operator selects the process ‘Issue multiple cards’, and searches amongst the approved card requests the cards that should be issued.

Step 2:
The operator selects the requests by ticking them in the displayed list and launching the process “Issue multiple cards”.

Step 3:
A form is displayed, and the operator can check the selected requests, order the list and click on “Next” to begin card issuance process.

Step 4:
Smart ID Desktop App or CardSDK is launched. The certificates are issued, then the PIN & PUK code is generated and sent by email. The card state is “active”.
The process continues from step 4 to 6 until the whole list of requests is finished.

Options included in this process:

Options are the same as in the “Issue Card” process.

5.4 Temporary card management

The Smart ID Blueprints includes a set of best practice use cases for how to request and issue a temporary card, assign temporary cards, and more, during the full life cycle.

Cards and middleware

5.4.1 Temporary card attributes

The temporary card attributes are the same as those described in the Card Management section.

5.4.2 Request temporary card

Actors: Operator

Process kinematic: Smart ID Blueprints provides a process to request the production of several temporary cards. The request must always be made before the cards are produced.

Step 1:
From the start page of IDM Operator, the operator selects the process “Request temporary cards”.

Step 2:
The operator selects the number of temporary cards to be produced.

⚠ **C0 Public Document**
Nexus property.

Step 3:
After approval, the card requests are created and ready to be issued/produced.

5.4.3 Issue multiple temporary cards

Actors: Operator

Process kinematic: Smart ID Blueprints provides a process to produce/issue several temporary cards.

Step 1:
From the page ‘Batch order’**,** the operator selects the workflow ‘Issue multiple temporary cards’, and search amongst the approved temporary card requests.

Step 2:
A form is displayed, and the operator can check the selected cards, order the list and click on “Next” to begin card issuance process.

Step 3:
Smart ID Desktop App or CardSDK is launched; In case of Smart ID Desktop App the user must confirm the launch and click **“Open link”**.

Step 4:
Smart ID Desktop App or CardSDK is launched is launched; the operator is asked to select his card reader.

Step 5:
The certificates are issued, then the PIN & PUK code is generated and sent by email. The card state is “unassigned”.

Step 6:
The process continues from Step 3 to 5 until the whole list of cards is finished.

Options included in this process

These options can be customized:

- PIN/PUK management:
  - Possibility to choose PIN length (6 by default)
  - Possibility to choose PUK length (8 by default)

5.4.4 Assign temporary card

Actors: Operator

Process kinematic: Smart ID Blueprints provides a process to assign a temporary card to a user.

⚠ **C0 Public Document**
Nexus property.

Step 1:
The process can be launched from the temporary card search or detailed view of a temporary card.

Step 2:
The operator checks the data, searches for an “unassigned” temporary card and clicks on „Next“.

Step 3:
Smart ID Desktop App or CardSDK is launched, the operator is asked to select their card reader.

Step 4:
The certificates are issued, then the PIN code is generated, and the PIN is printed in a PIN letter. The Operator prints the PIN letter. The card state is “assigned”.

Options included in this process

These options can be customized:

- Define certificate duration on temporary cards
- PIN/PUK management:
  - Possibility to send PIN/PUK by email or print PIN/PUK letter during card issuance
  - Possibility to choose PIN length (6 by default)
- Number of cards:
  - Possibility to limit the number of temporary cards that a user can have at the same time (2 by default)
- Certificates:
  - Possibility to choose to deliver the following certificates during the process:
    - Authentication (Yes/No)
    - Signature (Yes/No)
    - Encryption (Yes/No)

⚠ **C0 Public Document**
Nexus property.

5.4.5 Extend temporary card

Actors: Operator

Process kinematic: Smart ID Blueprints provides a process to extend the validity of an assigned temporary card. For example, the user must keep the temporary card because the new card has not been produced.

Step 1:
The process can be launched from the temporary card search or detailed view of a temporary card.

Step2:
The operator checks the data and clicks on „Next“.

Step 3:
Smart ID Desktop App or CardSDK is launched, the operator is asked to select their card reader.

Step 4:
The new certificates are issued, then the PIN code is generated, and the PIN is printed in a PIN letter. The Operator prints the PIN letter. The card state is “assigned”.

Options included in this process

These options can be customized:

- Define certificate duration on temporary cards
- PIN/PUK management:
  - Possibility to send PIN/PUK by email or print PIN/PUK letter during card issuance
  - Possibility to choose PIN length (6 by default).

5.4.6 Withdraw temporary card

Actors: Operator

Process kinematic: Smart ID Blueprints provides a process to unassign a temporary card from a user. Once the workflow is finished the temporary certificates deployed on the card are revoked and the card can be assigned to another user.

Step 1:
The process can be launched from the temporary card search or detailed view of a temporary card.

Step2:
The operator checks the data and clicks on “Next”.

Step 3:
All filled user data, the assigned certificate, and PIN/PUK will be revoked and removed; The card state is “unassigned”.

⚠ **C0 Public Document**
Nexus property.

5.4.7 Lock temporary card

Actors: Operator

Process kinematic: Smart ID Blueprints provides a process to lock a temporary card. This process is useful when a temporary card can no longer be assigned to a user (card broken, stolen, lost ..).

Step 1:
The process can be launched from the temporary card search or detailed view of a temporary card.

Step2:
The operator checks the data and clicks on “Next”.

Step 3:
The card state is “locked”. Certificates are “revoked”.

5.5 Virtual smart card management

The Smart ID Blueprints includes a set of best practice use cases for how to get a virtual smart card (VSC), change PIN for a virtual smart card, and more, during the full life cycle.

A virtual smart card defines a profile containing personal information stored within the Smart ID Desktop App, which is installed on a notebook/PC. By using dedicated workflows via Smart ID Self Service, an end user can enroll different kinds of certificate types (authentication, signature or encryption) to the notebook/PC and use them to, for example, authenticate with different applications/services. Operators can deactivate, reactivate, and delete virtual smart cards.

Info: The process to get/request, change pin and lock a virtual smart is described in the self-service use cases Get virtual smart card.

5.5.1 Virtual smart card attributes

The virtual smart card attributes are the same as those described in the Card Management section.

5.5.2 Deactivate virtual smart card

Actors: Virtual smart card manager

Process kinematic: This process is used by an operator to deactivate a virtual smart card and related certificates for an existing user. The VSC can be reactivated later. The certificates are put “Certificate hold” if the PKI supports this status. If the PKI doesn’t support “Certificate hold”, we recommend using the “Lock virtual smart card” process.

⚠ C0 Public Document
Nexus property.

Step 1:
The process can be launched from the virtual smart card search or detailed view of a virtual smart card. The operator has a view of all data of the card and related to the user.

Step 2:
The operator checks the data and clicks on “Next”

Step 3:
The certificates deployed on the virtual smart card are put “Certificate hold”. The card state is “inactive” and the certificates are “Certificate hold”.

5.5.3 Reactivate virtual smart card

Actors: Virtual smart card manager

Process kinematic: Smart ID Blueprints provides a process to reactivate a virtual smart card. The card has been previously deactivated and is in state “inactive”. The certificates are put back on “valid” status. If the PKI doesn’t support “Certificate hold” status, then we recommend issuing a new virtual smart card with “Get virtual smart card” process to issue new certificates on this virtual smart card.

Step 1:
The process can be launched from the virtual smart card search or detailed view of a virtual smart card. The operator has a view of all data of the card and related to the user.

Step 2:
The operator checks the data and clicks on “Next”.

Step 3:
The certificates are put back in “valid” state and the card is “active” again.

5.5.4 Delete virtual smart card

Actors: Virtual smart card manager

Process kinematic: Smart ID Blueprints provides a process to delete a virtual smart card and revoke the related certificates.

Step 1:
The process can be launched from the virtual smart card search or detailed view of a virtual smart card. The operator has a view of all data of the card and related to the user.

Step 2:
The operator checks the data and clicks on “Next”.

Step 3:
The certificates are revoked. The virtual smart card is completely deleted (no more visible in the Web UI).

⚠ **C0 Public Document**
Nexus property.

5.6 Passkey management

The Smart ID Blueprints include two use cases: executing an on-behalf registration of a FIDO2 token with Entra and deleting a registered FIDO2 token from Entra. A prerequisite is that the IDM user is already registered in the Entra system.

FIDO2 security keys significantly enhance security by providing a phishing-resistant authentication method. However, registering a FIDO2 credential typically requires manual interaction and the physical presence of the future credential holder. In the standard workflow, the user must first authenticate to the target service and then enroll the FIDO2 token. As a result, the user temporarily maintains two authentication methods, one of which may still rely on username and password authentication.

For enterprise environments, a more suitable approach is to enable operators to register FIDO2 tokens on behalf of users and subsequently distribute the configured tokens to them. Microsoft Entra provides an interface that supports FIDO enrollment on behalf of another user.

5.6.1 Passkey attributes

The passkey attributes are the same as those described in the Card Management section.

5.6.2 Enroll FIDO2 token in Entra

Actors: Passkey Manager, Passkey User

Process kinematic: Smart ID Blueprints provides a process to enroll a passkey on behalf of a registered Entra user.

Step 1:
The process can be launched from the detailed view of a user with the assigned **Passkey user** role. The Passkey manager has a view of all data of the user.

Step 2:
The passkey manager checks the data and clicks on “Enroll FIDO2 token in Entra”. The **Passkey manager** role must be assigned to the manager.

Step 3:
A form with the detailed user information is displayed to the passkey manager and clicks “Next”.

Step 4:
Smart ID Desktop App is launched; the passkey manager must confirm the launch and click “Open link”.

Step 5:
The passkey manager is asked to choose where to save the passkey and clicks on “Security key”.

Step 6:
The passkey user must enter a security key PIN and touch the security key.

⚠ **C0 Public Document**
Nexus property.

Step 7:
The passkey manager clicks on “Ok”, to finish the enrollment.

5.6.3 Delete FIDO2 token from Entra

Actors: Passkey Manager

Process kinematic: Smart ID Blueprints provides a process to delete an enrolled passkey for a registered Entra user.

Step 1:
The process can be launched from the detailed view of an enrolled passkey.

Step 2:
The passkey manager checks the data and clicks on “Delete FIDO2 token from Entra”.

Step 3:
A form with the detailed passkey information is displayed to the passkey manager and clicks “Next”.

Step 4:
A form is displayed with the information that the passkey is deleted in Entra and IDM.

5.7 Mobile ID management

The Smart ID Blueprints includes a set of best practice use cases for provisioning and managing Mobile ID profiles for users throughout the entire lifecycle. The use cases cover scenarios such as issuing a Mobile ID profile, locking a profile, and more. They are described in detail and are divided according to the roles of operator and self-service user.

A mobile ID defines a profile containing personal information stored within the Smart ID Mobile App, which is installed on a user's mobile device. By using dedicated workflows in Smart ID Identity Manager, different types of certificates (authentication, signature or encryption) can be enrolled on mobile devices and used, for example, to authenticate in various applications and services.

5.7.1 Mobile ID attributes

The Mobile ID attributes are the same as those described in the Card Management section.

5.7.2 Supply Mobile ID for user

Actors: Mobile ID Manager

Process kinematic: Smart ID Blueprints provides a process to supply a Mobile ID for a user.

⚠ C0 Public Document
Nexus property.

Step 1:
The process can be launched from the detailed view of a user with the assigned role **Mobile ID Self-Service User**. The **Mobile ID Manager** has a view of all data of the user.
The **Mobile ID Manager** role must be assigned to the manager.

Step 2:
The **Mobile ID Manager** checks the data and clicks on “Supply Mobile ID for user”.

Step 3:
A form with relevant information is displayed to the manager and clicks “Next”.

Step 4:
With next, an email will be sent to the users email address. This email contains a QR code that the user must scan, using Smart ID App to set up their Mobile ID.

Step 5:
The user starts the Smart ID App, clicks on “scan” button. The camera view is going to be presented.

Step 6:
After the user has followed the instructions in the app, the Mobile ID profile is successfully created.

Options included in this process

These options can be customized:

- Certificates:
  - Possibility to choose to deliver the following certificates during the process:
    - Authentication (Yes/no)
    - Signature (Yes/no)
    - Encryption (Yes/no)
- Mobile ID Profile validity:
  - Possibility to define a lifetime for the Mobile ID profile (2 years by default)
- Recovery of encrypted certificates
  - **Enable** or **disable** the possibility to display a form to manually select encryption certificates for recovery. If this option is disabled it will recover automatically the latest three encryption certificate.
- Definition of whether the QR code should be displayed in the form or sent by email
- Email notification after the failed or successful creation of a Mobile ID profile
- Definition of properties which will be visible directly on the Mobile ID profile

5.7.3 Deactivate Mobile ID

Actors: Mobile ID Manager

⚠ **C0 Public Document**
Nexus property.

Process kinematic: This process is used by a Mobile ID Manager to deactivate a Mobile ID profile and the related certificates for an existing user. The Mobile ID profile and the certificate can be reactivated. The certificates are put on “Certificate hold” if the PKI supports this status. If the PKI doesn’t support “Certificate hold”, we recommend using the “Lock Mobile ID” process.

Step 1:
The process can be launched from the Mobile ID search or from the detailed view of a Mobile ID profile. The Mobile ID Manager has a view of all data of the profile related to the user.

Step 2:
The operator checks the data and clicks on “Next”.

Step 3:
The certificates deployed on the profile are put on “Certificate hold”. The profile state is “inactive”, and the certificates are on “Certificate hold”.

5.7.4 Reactivate Mobile ID

Actors: Mobile ID Manager

Process kinematic: Smart ID Blueprints provides a process to reactivate a Mobile ID profile. The profile has been previously deactivated and is in the state “inactive”. The certificates are put back on “valid” status. If the PKI doesn’t support “Certificate hold” status, then we recommend issuing a new Mobile ID profile with “Get Mobile ID profile” process to issue new certificates.

Step 1:
The process can be launched from the Mobile ID search or detailed view of a Mobile ID profile. The manager has a view of all data of the profile related to the user.

Step 2:
The operator checks the data and clicks on “Next”.

Step 3:
The certificates are back in “valid” state, and the Mobile ID profile is “active” again.

5.7.5 Lock Mobile ID

Actors: Mobile ID Manager

Process kinematic: The Smart ID Blueprints provides a process to lock a Mobile ID profile and revoke the associated certificates. The Mobile ID profile will be in state “Locked”; the related certificates will be in the state revoked.

Step 1:
The process can be launched from the Mobile ID search or detailed view of a Mobile ID profile. The

⚠ **C0 Public Document**
Nexus property.

manager has a view of all data of the profile related to the user. The manager checks the data and clicks on “Next”.

Step 2:
The certificates are “revoked”. The Mobile ID profile state is “locked”**.** No further operations can be done on this profile.

⚠ **C0 Public Document**
Nexus property.

6 Self-Service use cases

The following use cases are available in the self-service web app.

6.1 User management

6.1.1 Change password

Actors: Self-Service user

Process kinematic: The Smart ID Blueprints provides a process to change the user's login password.

Step 1:
The user connects to the Smart ID Self-service portal.

Step 2:
The user clicks on "Identities" menu and launches the "Change password" process.

Step 3:
A Webpage displays the password policy; the user enters and confirms the new password.

Options included in this process

These options can be customized:

- Configure password policy:
  - Password length
  - List of characters used in password

6.1.2 Edit photo

Actors: Self-Service user

Process kinematic: The Smart ID Blueprints provides a process to edit the user photo.

Step 1:

The user connects to the Smart ID Self-service portal.

Step 2:

The user clicks on "Identities" menu and launches the "Edit photo" process.

Step 3:

⚠ **C0 Public Document**
Nexus property.

A form is displayed to the user that explains the next steps. The user clicks on “Next”.

Options included in this process

These options can be customized:

- Define the maximum size of the photo

6.2 Card Management

6.2.1 Unblock/Change PIN

Actors: Self-Service User

Process kinematic: The Smart ID Blueprints provides a process to unblock/change PIN when the card has been blocked (3 wrong PIN entries).

NB: To allow this use case, the PUK must be available in the CMS, and the user has a means to authenticate to Smart ID Self-Service through another login method (SAML IdP, Mobile App…) The card must be in state “active”.

Step 1:
The user connects to the Smart ID Self-service portal through another login method than card.

Step 2:
The user clicks on “Cards” menu and launches the “Unblock PIN/Change PIN” process.

Step 3:
A form is displayed to the user that explains the next steps. The user clicks “Next”.

Step 4:
Smart ID Desktop App is launched; the user must confirm the launch and click **“Open link”**.

Step 5:
The user selects a card reader, and after the card is read, enters and confirms a new PIN code.

Step 6:
The new PIN code is set.

6.2.2 PIN Unblock offline

Actors: Self-Service User

Process kinematic: The Smart ID Blueprints provides a process to unblock the PIN offline. The process is based on a challenge response mechanism.

⚠ C0 Public Document
Nexus property.

NB: To allow this use case, the user has a means to authenticate to Smart ID Self-Service through another login method than the card (SAML IdP, Mobile App…). The card must be in state "active". The challenge code must be prompted to use through the.

Step 1:
The user connects to the Smart ID Self-service portal through another login method than card.

Step 2:
The user clicks on "Cards" menu and launches the "Unblock PIN offline" process.

Step 3:
The user is asked to enter the challenge code.

Step 4:
The CMS is calculating the response code that is displayed to the user.

Step 5:
The user can now change their PIN code.

Step 6:
The user enters the new PIN code twice.

6.2.3 Renew card

Actors: Operators

Process kinematic: The Smart ID Blueprints provides a process to renew card certificates.

NB: To allow this case to be used, the user has access to Smart ID Self-Service with their current card. The card must be in state "active" and certificates still valid. The same policy as the one used during card issuance will be used.

Step 1:
X days before certificate expiration, IDM sends an email to the card holder, warning that the certificates on the card will expire soon.

Step 2:
The user connects to the Smart ID Self-service portal.

Step 3:
The user clicks on "Dashboard" menu and launches the "Renew Card" process.

Step 4:
A form is displayed to the user that explains the next steps. The user clicks on "Next".

Step 4:
Smart ID Desktop App is launched; the user is asked to select the card reader and enters a new PIN code.

⚠ **C0 Public Document**
Nexus property.

Step 5:
The old certificates are erased from the card. The new certificates are issued, based on the same policy as the one used for “Issue card”. The PIN & PUK code remain the same.

Options included in this process

These options can be customized:

- Certificates:
  - Possibility to choose to deliver the following certificates during the process:
    - Authentication (Yes/no)
    - Signature (Yes/no)
    - Encryption (Yes/no)
- Recovery of encrypted certificates
  - Possibility to enable certificate retrieval during card issuance (a form displays the list of existing certificates that are recoverable)

6.3 Virtual smart card management

6.3.1 Get virtual smart card

Actors: Virtual Smart Card Self-Service User

Process kinematic: The Smart ID Blueprints provides a process to request the issuing of a virtual smart card.

NB: The VSC can be either stored in the TPM, Microsoft Keystore or on a Yubikey.

Step 1:
The user connects to the Smart ID Self-service portal.

Step 2:
The user clicks on “Dashboard” menu and launches the “Get Virtual Smart Card” process.

Step 3:
A form is displayed to the user that explains the next steps. The user clicks on “Next”.

Step 4:
Smart ID Desktop App is launched; the user must confirm the launch and click “Open link”.

Step 5:
The user is asked to choose a PIN code*.

Step 6:
The PIN code is set, then the user is asked to enter again the PIN code before certificate issuing on the TPM/Yubikey.

⚠ **C0 Public Document**
Nexus property.

Step 7:
The certificate is issued.

**NB: for Yubikey, the PIN code is managed outside IDM, directly through Yubikey Middleware*

Options included in this process

These options can be customized:

- Certificates:
  - Possibility to choose to deliver the following certificates during the process:
    - Authentication (Yes/no)
    - Signature (Yes/no)
    - Encryption (Yes/no)
- Virtual Smart Card validity:
  - Possibility to define a lifetime for the VSC (2 years by default)
- PIN management:
  - Possibility to send PIN by email or print PIN letter during card issuance
  - Possibility to choose PIN length (6 by default)
- Definition of properties which will be visible directly on the virtual smart card

6.3.2 Change PIN for a virtual smart card

Actors: Virtual Smart Card Self-Service User

Process kinematic: The Smart ID Blueprints provides a process to change the PIN of a virtual smart card. The virtual smart card must be in “active” state.

NB: This case is only available for VSC stored on TPM.

Step 1:
The user connects to the Smart ID Self-service portal.

Step 2:
The user clicks on “Virtual Smart Card” menu and launches the “Change PIN” process

Step 3:
A form is displayed to the user that explains the next steps. The user clicks on “Next”.

Step 4:
Smart ID Desktop App is launched; the user must confirm the launch and click “Open link”.

Step 5:
The user is asked to enter a new PIN code and confirm it.

⚠ **C0 Public Document**
Nexus property.

Step 6:
The new PIN code is set up.

NB: for Yubikey, the PIN code is managed outside IDM, directly through the Yubikey Middleware

6.3.3 Lock virtual smart card

Actors: Virtual Smart Card Self-Service User

Process kinematic: The Smart ID Blueprints provides a process to lock a virtual smart card and revoke the associated certificates. The virtual smart card will be in state “Locked”, erased from the TPM (through Smart ID Desktop App) but still present in the Self-service portal in “locked” status.

Step 1:
The user connects to the Smart ID Self-service portal.

Step 2:
The user clicks on “Virtual Smart card” menu and launches the “Lock virtual smart card” process.

Step 3:
A form is displayed to the user that explains the next steps. The user clicks on “Next”.

Step 4:
Smart ID Desktop App is launched; the user must confirm the launch and click **“Open link”**.

Step 5:
Smart ID Desktop App is launched; the user is asked to allow virtual smart card to be deleted.

Step 6:
The virtual smart card is deleted from Smart ID Desktop App and associated certificates are revoked.

NB: Smart ID Desktop App allows to see all VSCs deployed on the computer.

6.4 Mobile ID management

6.4.1 Get Mobile ID

Actors: Mobile ID Self-Service User

Process kinematic: The Smart ID Blueprints provides a process to request the issuing of a Mobile ID profile with related certificates.

Step 1:
The user connects to the Smart ID Self-service portal.

⚠ **C0 Public Document**
Nexus property.

Step 2:
The user clicks on “Dashboard” menu and launches the “Get Mobile ID” process.

Step 3:
A form is displayed to the user that explains the next steps. The user scans the QR code with the help of the Smart ID App. After the user has followed the instructions in the app, the Mobile ID profile is successfully created.

Step 4:
Back in the IDM self-service portal, the user confirms the successful creation of the Mobile ID profile by clicking “Next”.

Step 5:
The Mobile ID profile and the related certificate are displayed in the Self-Service portal.

6.4.2 Lock Mobile ID

Actors: Mobile ID Self-Service User

Process kinematic: The Smart ID Blueprints provides a process to lock a Mobile ID profile and revoke the associated certificates. The profile will be in state “Locked”, the certificate will be in the final state “revoked”.

Step 1:
The user connects to the Smart ID Self-service portal.

Step 2:
The user clicks on “Mobile ID” menu and launches the “Lock Mobile ID” process.

Step 3:
A form is displayed to the user that explains the next steps. The user clicks on “Next”.

Step 6:
The Mobile ID profile is locked, and the related certificates are revoked.
Options included in this process

These options can be customized:

- Certificates:
  - Possibility to choose to deliver the following certificates during the process:
    - Authentication (Yes/no)
    - Signature (Yes/no)
    - Encryption (Yes/no)
- Mobile ID Profile validity:
  - Possibility to define a lifetime for the Mobile ID profile (2 years by default)
- Recovery of encrypted certificates

⚠ C0 Public Document
Nexus property.

- **Enable** or **disable** the possibility to display a form to manually select encryption certificates for recovery. If this option is disabled it will recover automatically the latest three encryption certificate.

- Definition of whether the QR code should be displayed in the form or sent by email
- Email notification after the failed or successful creation of a Mobile ID profile
- Definition of properties which will be visible directly on the Mobile ID profile

7 Roles vs use cases in Smart ID Blueprints

The table below provides an overview of the roles and their associated use cases.

Use case	Operator	Self-Service user
Upload default roles	☑	
Create default roles	☑	
Delete default roles	☑	
Edit identifier	☑	
Delete identifier	☑	
Create reason	☑	
Edit reason	☑	
Delete reason	☑	
Create user (Manually/CSV)	☑	
Deactivate user	☑	
Reactivate user	☑	
Lock user	☑	
Edit user	☑	
Delete user	☑	
Reset password	☑	

⚠ **C0 Public Document**
Nexus property.

Edit roles	☑	
Reset multiple passwords	☑	
Edit roles for multiple users	☑	
Delete multiple users	☑	
Change password		☑
Edit photo		☑
Forgot password		☑
Issue P12 certificate	☑	
Display password	☑	
Renew user certificate via PKCS#12	☑	
Revoke certificate	☑	
Request card	☑	
Issue card	☑	
Recover certificates on user card	☑	
Renew	☑	
Edit card	☑	
Deactivate card	☑	
Reactivate card	☑	
Lock card	☑	
Unblock card remote	☑	
Request multiple cards	☑	
Issue multiple cards	☑	

⚠ **C0 Public Document**
Nexus property.

Import cards by CSV	☑	
Import certificates by CSV	☑	
Unblock/Change PIN		☑
PIN Unblock offline		☑
Renew card		☑
Request temporary card	☑	
Assign temporary card	☑	
Withdraw temporary card	☑	
Abort temporary card	☑	
Extend temporary card	☑	
Lock temporary card	☑	
Issue multiple temporary cards	☑	
Get virtual smart card		☑
Change PIN for VSC		☑
Lock VSC	☑	☑
Deactivate VSC	☑	
Reactivate VSC	☑	
Delete VSC	☑	☑
Supply Mobile ID for user	☑	
Deactivate Mobile ID	☑	
Lock Mobile ID	☑	☑
Get Mobile ID		☑

⚠ **C0 Public Document**
Nexus property.

⚠ **C0 Public Document**
Nexus property.