Smart ID Blueprints

Start-up guide

⚠ **C0 Public Document**
Nexus property.

Identification of the document		
No pages: 7	**State:** puplished	**Reference:** Product Management
Creation date: 11/11/2025	**Last updated:** 1/29/2026	**Version:** 1.0

Version history

Version	Author	Date	What changes were made, where
1.0	Stefanie Lenhard	2025-11-11	First draft
		Click or tap to enter a date.	
		Click or tap to enter a date.	
		Click or tap to enter a date.	
		Click or tap to enter a date.	
		Click or tap to enter a date.	

Table of Contents

1 Introduction

This guide provides a step-by-step approach to upload and deploy the Smart ID Blueprints for Smart ID Identity Manager. By following these instructions, you will set up a ready-to-use foundation that includes essential configurations, roles, and options required for initial operation.

1.1 Prerequisites

Before you begin, ensure the following:

- **Smart ID Identity Manager** is installed and accessible.
- The configuration **SmartIDBlueprints.zip** is available.
- For **card production**, you will need a production component. You can use the following components for this:
    - Smart ID Desktop App or
    - Nexus Card SDK (at least 6.6.0.15)
        - Cards **Thales IDPrime MD 830**
    - Middleware e.g., Safe Net Authentication Client
- You have administrative access to **Identity Manager Admin** and **Identity Manager Operator**.
- The default roles csv file is available.
- Update your custom-beans.xml with the following entry:

```
<bean id="importIdentitiesFromCSVTaskErrorCatchingWrapper" class="de.nexus.projectutils.action.ExceptionCatchingWrapperParameterizedJavaDelegate" parent="parameterizedTask">

    <property name="javaDelegate" ref="importIdentitiesFromCSVTask"/>

    <property name="errorCode" value="ERROR_CSV_IMPORT"/>

  </bean>
```

Once everything is prepared, follow the steps below.

2 Step by Step Instruction

Step 1 - Upload Smart ID Blueprints

1. Log in to **Identity Manager Admin**
    - Username: admin
    - Password: admin (*We recommend changing the password immediately after logging in.)*

2. Navigate to **Configuration File** tab.
3. Click **Upload configuration**.
4. Click **Select file** and choose the SmartIDBlueprints.zip.
5. Click **Upload** to import the configuration.

Step 2 - Adjust Configuration Options via Scripts (Optional)

The Smart ID Blueprints include scripts that allow you to enable or disable specific behaviors to match customer requirements (e.g., whether user deactivation requires approval).

Available option scripts:

Script Name	Description
UsersScriptOptions	User-related process options
UsersCertScriptOptions	User certificate options
CardsScriptOptions	Card lifecycle options
TempCardsScriptOptions	Temporary card processes options
VirtualSmartCardScriptOptions	Virtual smart card options

Example: Enable approval for user deactivation

1. In **Identity Manager Admin**, go to **Home** → **Scripts**.
2. Open the script **UsersScriptOptions**.
3. Locate the section **Approvals** and find the variable **UsersDeactivationApproval**.

Default value:

```
/*
Defines if user deactivation requires approval.
Possible options:
 * true  - Approval step is enabled.
 * false - Approval step is disabled.
*/
UsersDeactivationApproval = false
```

5. Set **UsersDeactivationApproval = true** if you want to require approval.

6. Click **Save** in the upper left corner.

Step 3 - Configure Connection Details

Identity Manager requires connection details for several external components. These connections must be configured to ensure that processes can communicate with required backend systems.

1. Configure the required connections for the following components:
   - **Certificate Authorities (CA)**
     Configure the connection parameters to the Certificate Authority.
   - **Messaging Server**
     Define the connection details for the messaging server.
   - **Datapools**
     Configure the LDAP connection settings for the following datapools:
     - *Ldap active users*
     - *Ldap inactive users*
2. Verify that all required connection parameters (e.g., host, port, credentials, certificates) are correctly entered.
3. Save the configuration changes.

Step 4 - Configure System Properties

During process execution, the system may need to send email notifications (e.g., approval requests, status updates etc.). To enable this, configure SMTP settings so Identity Manager can communicate with your mail server.

1. Log in to **Identity Manager Operator**
   - Username: **admin**
   - Password: ******
2. Navigate to the **Admin** Section.
3. Under **Administration Area,** select **Configure System Properties.**
4. Open the **SMTP Settings** section.
5. Enter SMTP configuration details.
6. Save changes.

Step 5 - Upload default roles

Default roles define permissions and capabilities for different user types. After uploading, roles can be assigned to users, ensuring dedicated processes are visible only to authorized roles.

1. Log in to **Identity Manager Operator**.
2. On the right side of the start page, click **Upload Default Roles**.
3. Select and upload the file **Default_Roles.csv.**
4. After the upload, assign roles to users via the process **Edit Roles**.

Default roles overview:

Role	Description
Approver	Can approve user requests, e.g., deactivate user.
Self-Service User	Can sign in to Smart ID Self-Service.
Operator	Can manage user lifecycle, e.g., deactivate a user.
Virtual Smart Card Manager	Can lock a virtual smart card in Operator.
Virtual Smart Card Self-Service User	Can obtain a virtual smart card via self-service.
Passkey Manager	Can enroll a passkey for a specific Entra user (user must be registered in Entra)
Passkey User	Can obtain or receive a passkey.

Step 6 - Required Users

Important: Before executing any process, create at least two users with these roles:

- **Operator** – Manages user lifecycles and operational tasks.
- **Approver** – Approves requests (e.g., user deactivation). Approval processes will not function without this role.

Step 7 - Create Reasons

Reasons are mandatory for actions such as activating, deactivating, or locking a user or card. Create reasons before starting to use the Smart ID Blueprints.

1. Log in to **Identity Manager Operator**.
2. Click **Create reason** on the right side of the start page.
3. Select a reason type from the dropdown.
4. Enter a Reason name and optionally a description.
5. Click **Next** to save.

Step 8 - Create Identifier Types

When creating a user, you must set an identifier for personal identification (e.g., passport, driver license, national ID card).

1. In **Identity Manager Operator**, click **Create identifier** on the right side of the start page.
2. Enter a name and description for the identifier.
3. Click **Next** to save.

The system is now fully prepared with the initial configuration, roles, reasons, and identifiers — and is ready for use and further customization.

Recommended: Test key processes (e.g., user creation, approval process) to verify the correct setup.