Siemens Authentication Process

Overview – MyID and Siemens ID
Table of Contents

- Introduction
  Page 3-5

- Authentication for Siemens externals without SCD-Entry
  Page 6-9

- Authentication for Siemens internal with existing SCD entry
  Page 10-13

- Authentication for Known Business Partners with existing SCD entry
  Page 14-15
Introduction
Because MyID and Siemens ID federate in both directions each of the systems can focus on serving their user group more focused. MyID is focused on the employee authentication (including contractors) while Siemens ID on customers, suppliers and partners. Thru federations the access to any application can be provided at any direction. The application owner however is expected to define the primary use group for which the application is positioned to decide which service is more reasonable to integrate with.

**Example 1:** an application is built to offer configuration serve customers for ordering a Siemens digital product while Siemens employees have to authenticate to administer this solution. Siemens ID would be the better choice to integrate.

**Example 2:** a Siemens internal application require some external identities of suppliers to login. Here MyID is likely to be a better choice to integrate with.
Identity Management

<table>
<thead>
<tr>
<th>Validity</th>
<th>Bound to the contract validity. If the contract ends the identity and account is removed thru off-boarding</th>
<th>Never expires</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password reset and change</td>
<td>AD services, Help Desk, MyPassword Service, Password reset on the login page.</td>
<td>Thru the user using PingID enrollment and PingID reset.</td>
</tr>
<tr>
<td>Password life-cycle</td>
<td>Rotation enforced according to Siemens policies</td>
<td>Never expires. Further features like anomaly detection and breached password detection applied. MFA can optionally be used.</td>
</tr>
<tr>
<td>Ownership</td>
<td>Siemens and affiliates based on the employment or business partner contact agreement.</td>
<td>Customer, partner, supplier.</td>
</tr>
<tr>
<td>MFA Management</td>
<td>Thru the user using PingID enrollment and PingID reset. Thru the User Self Service performed thru the user.</td>
<td>Thru the User Self Service performed thru the user.</td>
</tr>
<tr>
<td>Identity attributes change (Name etc.)</td>
<td>Only thru HR processes or by sponsors in case of contractors.</td>
<td>Thru the User Self Service performed thru the user.</td>
</tr>
<tr>
<td>Identity Assurance Level</td>
<td>IAL 1-3 (dependent on identity origin)</td>
<td>IAL 1-3 (dependent on identity origin) IAL 1-2 for external identities.</td>
</tr>
<tr>
<td>Creation</td>
<td>Relies on Active Directory data (ADDSI3). Accounts are created and activated thru myIT processes (Windows Account) based on the SCD data.</td>
<td>Supports multiple methods: 1. Sign-Up (Self Registration) 2. Creation thru API 3. Siemens ID Identity Manager (Invitation process) 4. Creation thru tools like DirX/SAM including roles / groups provisioning</td>
</tr>
<tr>
<td>Available user attributes</td>
<td>The list of available attributes is described here.</td>
<td>Unified user profile is described here.</td>
</tr>
<tr>
<td>Available authentication methods</td>
<td>Windows Authentication (incl. AMA), User Name and Windows Password, PKI, SoftPKI, PingID (Push App and SMS), User Name and password, Siemens ID Push and OTP App, Google Authenticator, SMS</td>
<td></td>
</tr>
<tr>
<td>Authentication Assurance Level</td>
<td>AAL 1-3</td>
<td>AAL 1-2</td>
</tr>
<tr>
<td>ACF Security Level</td>
<td>ACF3</td>
<td>ACF2</td>
</tr>
</tbody>
</table>

Identity management is a process of creating, changing and deactivating of identities.

On the left you can see the differences between both systems or find the table on the Wiki page here.
Authentication for Siemens externals without SCD-Entry
What is Siemens ID?
Siemens ID enables secure access of Siemens employees, customers and partners to different Siemens application and services. With Siemens ID, you can use one digital identity to access different/most services provided to Siemens.

What do I need to do to sign-up (self-register) for a new digital identity in Siemens ID?
A working email address is required for the creation of a new digital identity in Siemens ID. You must also provide your family name, your given name and a password which complies with the Siemens ID password policy. Your new digital identity in Siemens ID will only be activated after you validated your email by clicking on the link in the confirmation email we send you.
Where can sign-up (self-register) for a new digital identity in Siemens ID?

You can use the ‘Sign-up tab’ of a connected Siemens application (if activated for this application) or use the ‘Sign-up tab’ in the login window of the ‘User Self Service Portal’ of Siemens ID: https://uss.login.siemens.com. Please be aware, that this will not automatically authorize you to use specific Siemens applications and services.
2. Step – Siemens ID Login

After signing up, you can login by using your provided email address and your password.
Authentication for Siemens internal with existing SCD entry
What is MyID?

- Proceeds authentication of users, placed in attached Active Directory (AD) Forests (As Oct. 2020: AD001 - SAG, AD005 - SHS, AD101 - SE) and provide their AD attributes to applications.
- Proceeds authentication of users, provided Siemens certificates (Kerberos, PKI and Soft PKI) and provide their AD attributes to applications.
- Forward the users authenticated by federated identity providers (IDP) and users attributes provided by those IDPs to applications.

Which authentication methods are possible with myID?

Depending on the security requirements of the accessed application multiple methods and their combinations are available:

- Windows Password
- Kerberos (including PKI authentication information on windows)
- PKI-SmartCard
- Soft-PKI (only for Siemens Employees and Business Partners)
- PingID App (Push and TOTP)
- SMS (as a part of the PingID module)
1. Step – Choose login method

Choose one of the displayed login methods.
2. Step – e.g. Login via Smart Card

When you choose Smart Card as login method, you need to enter your Smart Card PIN.
Authentication for Known Business Partners with existing SCD entry
Known Business Partners with an existing SCD entry can also use myID to authenticate themselves.

-> For more information about myID authentication see page 11.