Whats New in MyID® Version 12.3

Integration Toolkit

The MyID Toolkit consists of a package of APIs, documentation and sample code designed to extend the capabilities of MyID. Further details are on the Intercede Customer Portal.

Authentication Codes

- A MyID Operator can request that a temporary authentication code is sent by email to an end user to authenticate to the MyID Authentication Server, adding a helpdesk solution for when alternative authentication methods cannot be used. This helps organisations that have integrated MyID Authentication Server as an identity provider.
- A MyID Operator can also view an authentication code, so it can be read out over the telephone or provided through an alternative channel.
- Viewing authentication codes is also available for credential lifecycle cases such as collecting or activating credentials and unlocking device PINs.
- The complexity of authentication codes can be configured (for example excluding hard to access characters and defining the length of the code).
- Lifetime of authentication codes can be configured ensuring that they will expire if not used within the identified time.
- All features are also available through the MyID Core API (REST based APIs that are part of the Integration Toolkit).

Assign/Unassign Devices

- Smart cards and USB tokens can be pre-assigned to a credential request, before the device personalization takes place.
- For example, where an assignment has already taken place in a Physical Access Control or card printing system.
- The device can be assigned by inserting it to a reader or USB port, or by searching for the device from the MyID database.
- All features are also available through the MyID Core API (REST based APIs that are part of the Integration Toolkit) Integration Toolkit).

Certificate Renewal for Additional Identities

- Additional identity certificates (for example, administrator accounts for privileged access) that are issued in addition to the primary identity can now be automatically renewed as expiry approaches.
- When expiry approaches, the account owner will receive an email notification with instructions on how to collect the renewed certificates.
- The same certificate policy can now be used for both primary and additional identity certificates issued by MyID.

PIV – Office of Personnel Management

- Updated MyID Integration with Office of Personnel Management (OPM) for Background Investigations.
- MyID gathers required data during user enrolment including 10-Slap fingerprint capture and EFT generation.
- The process allows for automated submission to OPM once initial enrolment has taken place and allows adjudication decisions to be recorded in MyID, forming part of the PIV enrolment audit trail.
- The process can be managed through the MyID Core API in addition to Operator Client.
- The 10-Slap fingerprint enrolment process now supports capture of fingerprint rolls.

PIV - HID pivClass

- Updated MyID integration with HID pivClass to submit PIV card and user status information to physical access control systems (PACS).
- This integrates credential lifecycle management with physical access control, for example enabling or revoking physical and logical access from one user interface.
- PACS access areas can also be set from the MyID Operator Client user interface or MyID Core API.

Software Bill of Materials

- In accordance with US Executive Order 14028: Improving the Nation's Cybersecurity, a software bill of materials is now available for MyID PIV.
- This helps US Federal Agencies quickly assess impacts of cybersecurity vulnerabilities within their critical infrastructure.

Please contact Intercede to access this information.

Integration Updates

- Digicert One PKI
- Thales ID Prime MD930nc / MD940 B smartcards
- Aware Preface (PIV Facial biometric enrolment) with Canon EOS Rebel T8i/850D/KISS X10i
- Secugen Pro 10 & Pro 20 fingerprint readers
- Windows 11