intercede

MyID

What's New in MyID® Version 12.9

Mobile Identity Documents

MyID now supports provisioning and lifecycle management of Mobile Identity Documents – verifiable, privacy enhanced credentials stored in a mobile wallet. These documents are based on technical standards ISO/IEC 18013-5 (Mobile Drivers Licence) but can be used for a broader range of use cases including proof of qualifications, authority, access rights or other scenarios where information about a person needs to be presented for verification.

Building on MyID's capabilities as a highly adaptable identity and credential management platform, you can now

- Provide a comprehensive solution that can be tailored to meet unique use cases for identity attribute enrolment & associated business processes including information from integrated systems
- Define the electronic attributes required in a document that are available for external verification
- Define a graphical layout for the document, including information, photos and PDF417 barcodes
- Manage requests for identity document issuance through user interfaces and APIs
- Facilitate self-service collection of documents on iOS and Android using the MyID Wallet app
- A person can present a document for verification by displaying a QR code on their device
- Support verification using 3rd party document readers (secure transfer of information of BLE)
- Build your own wallet apps using the MyID Mobile SDKs for iOS and Android
- Audit and inventory reporting of issued mobile identity documents
- Reprovision documents where information updates are required
- Disable, enable and cancel mobile identity documents
- Provide APIs for Verifiers to check status and further information about issued documents

Enhanced Contactless Card Management

Lifecycle management of devices with a Mifare contactless interface has been updated to

- Allow pre-registration of devices (either by importing information or presenting the device)
- Allow checks to take place at issuance to read the contactless device ID
- Block issuance when the device ID is not pre-registered in the system
- Provide inventory and assignment reports
- Lifecycle management – assign, disable, enable, replace, renew, cancel
- Send notifications when lifecycle management events occur (email or to REST API)
- Add support for additional contactless card types

Enhanced Search Results

Report results and data tables in operator client now have additional capabilities to help sort, refine and organise the data displayed. This adds the ability to

- Sort on single or multiple columns
- Group results by a column value, including multi-level grouping
- Move and resize columns
- Display and hide columns
- Change the row spacing

What's New in MyID® Version 12.9

User Account Attribute Change Log

Keeping an accurate and consistent audit record of events, including updates to enrolled user information is essential for identity and access management in high security environments. MyID CMS now provides a change log of updates to user accounts, in addition to the detailed information already captured in audit records. This includes changes to user information and role/scope assignments highlighting changes to user privileges managed by MyID. This information is displayed in the Operator Client and can also be retrieved using the MyID Core API.

Barcode Support

- 1d Barcode support has been updated to generate the barcode images on the MyID server, improving performance and enabling use on mobile badge layouts
- 2d Barcodes can now be added to mobile badge layouts

Integration Updates

Microsoft .Net 8 – MyID has been updated to use the latest long-term support (LTS) version of Microsoft .Net core

Entrust Security Manager v10 – MyID integration with Entrust SM v10 is now available when using the Administration Toolkit for C, as well as the Entrust CA Gateway.

Extending Authentication Capabilities

The MyID product portfolio now includes a fully integrated solution to issue and manage both Multi Factor Authentication credentials and high security PKI and FIDO credentials from a single pane of glass.

MyID MFA (Multi Factor Authentication) incorporates

- Passwordless and Deviceless logins with pattern-based authentication and secure One Time Passcodes.
- Multiple passwordless MFA login options to remove the risk of phishing, dictionary, or brute force attacks.
- Self-service portal where end-users can manage their own devices and reset their AD passwords.

MyID MFA can be integrated with MyID CMS enabling

- A single solution for requesting and managing MFA credentials alongside PKI and FIDO
- Aligned MFA and PKI/FIDO policies and management processes (e.g. requests, approvals, cancellation)
- Combined reporting across all credential types
- Drive all credential management processes from your own systems using the MyID Core API

MyID MFA can also be run as a standalone capability, in addition to integration with CMS.

For further information, please contact us to discuss your requirements.

Web: www.intercede.com
Email: info@intercede.com
or call: +44 (0) 1455 558111
+1 888 646 6943