What's New in MyID CMS v12.11

Mac Client

Self-service collection and management of Yubikeys and other smart cards with a PIV Applet is now available on Apple Mac computers that have M-Series processors. This allows collection of certificates, device personalization and lifecycle management features such as PIN resets, collecting certificate renewals and device update and reprovision.

This feature is also integrated with the MyID Self Service Request Portal web page, allowing authentication with Entra ID accounts to rapidly replace temporary credentials with hardware protected certificates for secure logon to a Mac.

Printed Identity Documents

MyID credential management has been extended to produce printed identity documents – often these may accompany stronger credentials for use cases where complementary information is needed or where a visual identification document is required to be produced to high standards, following an organisations policies and procedures with traceability back to the source for audit, compliance, and status information. For example, visitor passes or other printed document templates requiring personalized information captured during an enrolment process such as a photo or signature.

These documents are produced using a managed process and MyID can also send information to other business systems through notifications APIs or be used as a source of information for verification of the credential by other systems.

Inactive Account Monitoring

High security environments will often have policies that require dormant accounts to be quickly identified and access removed, to prevent the opportunity for compromise. In MyID v12.11 a user account last logon to the system is now tracked, and accounts that have not authenticated for a configurable period can have administrative access to the system disabled.

Depending on your policy, self-service credential management can remain accessible to avoid enacting full revocation and the corresponding overheads of re-issuing certificates or other credentials.

Inactive accounts can easily be identified through user interface and API reports, and trusted administrators can simply restore access to the account without having to issue new credentials.

Access can also be restricted on demand, through the operator client user interface, or driven by another system using the MyID core API.

Reassign Credential API

MyID CMS is often used to meet highly complex credential management requirements where one person has multiple identities within an organisation, or group of organisations. Different personas may be needed depending on their role, administrative access or level of secrecy required, each with different credentials across a range of form factors.

What's New in MyID CMS v12.11

To help facilitate these needs, an issued credential can now be reassigned between related user accounts. The reassignment helps bridge the gap between job transitions & temporary assignments and overcomes the need to issue completely new credentials where this is not essential to the security policy.

Mobile Device Management Enhancements

MyID supports integration with Microsoft InTune and VMWare Workspace One UEM to facilitate validation of devices being used to collect credentials. This capability has now been extended to allow multiple instances of each MDM to be connected to the MyID server adding more flexibility for complex IT infrastructures.

Mobile Identity Documents

Previous MyID releases added support for provisioning Mobile Identity Documents (based on the ISO/IEC 18013-5 standard) from MyID CMS to a wallet app on iOS and Android. These customizable documents can contain images and attribute information about a person that is verifiable, cryptographically secure, and incorporates privacy by design.

In MyID 12.11 this feature has been extended to provide a simplified web-based enrolment process, including the ability to register using a trusted credential from an identity provider that supports OpenID Connect, and collection of the documents launched from a QR Code scan.

Enterprises can also validate the mobile device to be used for collection against a mobile device management system, ensuring both the person and the device used to hold these documents are trusted.

Scan/search for certificates with UserSID values

Organisations that use certificates for Windows Authentication should be preparing for changes being enforced by Microsoft in February 2025 that requires strong binding of a certificate to Active Directory accounts (UserSID). MyID can already support certificate issuance to meet these requirements, in 12.11 we are also adding more capabilities to report certificates that do not yet have this information built in. Existing certificates known to MyID are scanned for the UserSID value, and the information is extracted to allow certificates without this information to be easily located. Certificate replacement processes can be triggered helping you target user accounts that have not yet been prepared for this change.

Integration Updates

- Primekey v8.2 Certificate Authority
- Entrust nShield 5c Hardware Security Module
- Yubikey 5 & Yubikey FIPS (firmware v5.7)
- Larger key size (RSA 3072, RSA 4096) support on selected devices
- Topaz Signature Capture tablet support (MyID PIV IDCMS only)
- Desko Penta 4x Identity Document Scanner (MyID PIV IDCMS with Acuant Support add-on)

More information about MyID CMS 12.11 can be found on the **Intercede Customer Portal.**

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