intercede

What's New in MyID CMS 2026.1.0

Release Highlights for the MyID Credential Management System

This release is a significant milestone for the MyID® credential management system. It introduces:

A NEW VERSIONING APPROACH

MyID is moving to a new versioning scheme based on the calendar year and the iteration of the release. This gives customers greater clarity about the age of a release and a predictable frequency for upgrade planning.

The change has also given us the opportunity to simplify the product. It is now easier to manage from the web administration interface, duplicated functionality has been removed, and automation capabilities have been extended through the MyID Core API.

NEW FEATURES AND ENHANCEMENTS

PQC Software Certificate Support

As part of our research and development investment into post-quantum cryptography (PQC), MyID CMS 2026.1 brings support for software certificates using the new NIST-standardised post-quantum algorithms.

- Supports ML-DSA (Module-Lattice-Based Digital Signature Algorithm) and ML-KEM (Module-Lattice-Based Key-Encapsulation Mechanism).
- Issued through the EJBCA certificate authority (CA).
- This is the first in a series of features that will extend post-quantum credential issuance across the MyID suite.

Administrator-led FIDO Passkey Issuance

An administrator can now register a FIDO passkey on a security device, a process that is normally self-service. This supports the following:

- A randomised PIN can be set on the device during issuance and provided to the user separately, so they receive a fully prepared device.
- The device can be configured to require the user to change the PIN at first authentication.
- A shortened lifetime can be set for the FIDO Passkey, when used with Entra ID making it ideal for temporary credentials issued by a trusted administrator
- An administrator can prepare the credential for a new starter ahead of them joining, making onboarding a more efficient process

Biometric-only FIDO Passkey Device Authentication

MyID now supports collection of a FIDO passkey that requires fingerprint authentication, on biometric-enabled security keys.

- Collection works either as a self-service process or as a face-to-face, administrator-led process.
- The device PIN is set to a randomised value but is not distributed, so the only way to authenticate with the device is by fingerprint.
- No fingerprints can be added to the device without the PIN being entered.
- This helps prevent device sharing and ensures the intended user is present when authentication takes place.

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

intercede

What's New in MyID CMS 2026.1.0

Improvements for Multi-tenant Operation

A single MyID deployment can now manage a mixture of connected identity systems with tighter, per-tenant control.

- Supports a mixture of LDAP and REST-connected identity management systems integrated within one MyID deployment, including multiple instances of the same type (for example, many Entra ID tenants).
- Additional limits control access to each connected identity and access management (IDAM) system, alongside the existing MyID role-based access control methods.
- Aimed at deployments managing multiple separate business units within an organisation, or those offering credential management as a service, where each connected site has its own IDAM system, and MyID operators for local credential management.

Entra ID Integration Updates

You can now set MyID permissions using Entra ID security groups, enabling policy control in Entra to flow through to MyID CMS.

- Control which credential profiles may be issued to a given user. For example, a member of a privileged access Entra ID security group could be allowed to receive a credential profile with additional administrator certificates.
- Control operational permissions within MyID CMS. Members of a Credential Managers Entra ID security group would gain access to additional features for user enrolment and managing credential issuance.
- Security group membership synchronises between Entra ID and MyID CMS, either on demand or as part of a scheduled sync.
- Works with both static and dynamically defined Entra ID security groups, allowing Entra ID attribute-driven permissions in MyID CMS.

Third-party Key Recovery with a Pre-defined Secret

When requesting recovery of archived encryption certificates and keys for delivery to a third party, such as an auditor or investigator, a pre-agreed secret can now be set as part of the request.

- The secret, such as a device PIN, is applied automatically to the card, or as a password on the software PFX file that delivers the certificate.
- The value of the PIN or password is never exposed during collection.
- This limits knowledge of the sensitive information needed to access the certificates to those who generate the request.

INTEGRATION UPDATES

- Improved support for YubiKeys that have been factory reset outside MyID, enabling the keys to be reused.
- Support for Windows Server 2025.
- Support for SQL Server 2025.

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