intercede

MyID CMS

What's New in MyID CMS v12.14

Using MyID to register passkeys for Microsoft Entra ID

You can now use the advanced credential management features of MyID to provide passkeys on security keys and smart cards that are used directly for authentication to Entra.

The benefits this brings include:

- Using MyID data validation and permissions to control who can register passkeys through the CMS
- Consolidated lifecycle management for passkeys alongside other credential types such as certificates
- Align Passkey registration, reporting, and lifecycle processes across multiple Entra ID tenants
- Support for Entra cloud only and Hybrid Joined tenants
- Automatically create accounts in MyID during Passkey registration or link Entra ID accounts to existing MyID accounts
- Applying expiry dates to passkeys – automatically revoke the credential for fixed term workers, or for temporary passkey usage
- Support for passkeys as a derived credential – using an existing strong authentication credential such as a certificate to authenticate for the registration of a passkey

FIDO Enterprise Attestation

This feature allows enterprise organisations to have greater confidence in physical devices used for Passkey registration, by ensuring that the devices presented are trusted for use within your organisation. In conjunction with device vendors supporting this capability, MyID can ensure that Passkey registration through the CMS rejects untrusted devices that do not hold 'Enterprise Attestation' data for your organization.

Additionally, this feature enables better tracking of which physical device is used to hold the Passkey by storing a unique device identifier in the CMS for inventory control purposes, when this is supplied within the Enterprise Attestation data. In this case, MyID can also associate Passkey registrations with records of certificates issued to the device, enabling consolidated reporting and lifecycle management capabilities.

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

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

What's New in MyID CMS v12.14

Enhanced Certificate Recovery processes

Managed processes for recovering archived S/MIME certificates, where the certificate private keys are held in a Key Escrow store, have been updated in this release. The updated features are available in both the MyID Operator Client user interface and MyID Core APIs and allow administrators or connected systems to request recovery of a selection of certificates to an issued device, or to be recovered as part of issuance of a new device. Where allowed by certificate policies, the certificates and keys can also be downloaded as software pfx files.

This feature supports recovery onto a range of physical devices including smart cards and security keys, Windows Hello for Business and Virtual Smart Cards.

The solution works with any supported certificate authority and can also be integrated with the Intercede Secure Vault, which provides a key escrow database that is not locked into your certificate authority infrastructure and allows organisations greater control and ownership of private keys that protect sensitive information.

Improved flexibility for Self Service App deployments

Complex environments that use multiple MyID deployments to service different types of credentials can now take advantage of more flexibility when deploying the self-service applications for MyID. By allowing the server path to be provided programmatically, within administrator-controlled parameters, then self-service can be launched from email notifications, web page links or customers own scripted solutions when required and directed to connect to the appropriate MyID server.

This feature is available on both the Windows and Mac OS versions of MyID Self Service.

Collection of derived credentials to smartcards, security keys, Windows Hello and Virtual Smart Cards has been streamlined, by building in authorisation information to the MyID Self Service Portal web page, which performs authentication and validation of derived credential requests. This avoids an additional user step to enter authentication codes at collection.

Integration updates

- Yubikey 5 and Yubikey FIPS Security Keys (firmware 5.7.4)
- Idemia FIDO & CIV Security Keys
- Idemia CIV Smartcards
- Thales ID Prime MD3940C Smartcards
- Egofy v4 Smartcards

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