intercede

MyID

# v12.2 NOW AVAILABLE

## Authentication Codes for general purpose authentication

The MyID authentication server allows users to authenticate with a time limited code, sent to them by Email or SMS.

Process is entirely self-service.

- Build authentication codes into your own processes as an alternative or fallback option when smart card authentication is not possible (e.g. lost or missing devices).
- Note that authentication server can be used for integration into other systems, not just for logon to MyID.

## Authentication Codes for credential management

A MyID operator can send authentication codes by email or SMS for credential collection, activation, or PIN reset.

The code is then used to prove the identity of the recipient, enabling them to carry out the requested operation (e.g. reset the card PIN).

Integrated systems can make same requests using the MyID Core API.

Short or long lifetime authentication codes can be configured.

- Helps secure self-service credential management with more flexible authentication options.
- Removes the need for permanent security questions to be stored by MyID (which may contain PII).
- Drive processes from your own systems using MyID Core API

## Software Certificate Management via MyID Core API

Create requests for software certificates, search and list and view details of the issued credentials. Cancel and trigger renewals of software certificates.

Available by MyID Operator Client and MyID Core API.

- Greater automation of software certificate (e.g. for identifying servers or network infrastructure) issuance and lifecycle management using MyID Core API to integrate with your existing systems
- Extends more features to MyID Operator Client

## Fingerprint Verified Enrolment Processes in MyID PIV

PIV Enrollment processes have been enhanced to require fingerprint verification for all enrolment sessions after initial fingerprint capture. This helps agencies ensure it is the same person at each visit, maintaining the chain of trust for the PIV Applicant.

Additionally, fingerprint authentication can take place at any time, allowing an audited record of this event taking place.

Trusted PIV Enrollment officers can bypass these fingerprint checks when required, based on their role assignment in MyID.

- Enforces fingerprint verification at each enrollment session
- Captures fingerprint verification evidence as part of the process to help with PIV Audits
- Allows an alternative enrollment process to be used where fingerprint verification cannot be achieved, which can be restricted to privileged operators

## Customizable Kiosk

MyID Self Service Kiosk can be customized to build in your own web pages and content, making the solution highly adaptable to your environment

Build in fingerprint enrolment or pages that interact with MyID Core APIs, in addition to your own web content.

## Integration Updates

Support for latest available smart cards and USB tokens including two new Idemia ID-One PIV cards.

- Idemia ID-One PIV 2.4.2 on Cosmo V8.2 NPIVP & CIV / SPE Configurations
- Thales IDPrime MD930 FIPS L3
- Thales eToken 5300 USB-C
- Thales Safenet Authentication Client 10.8 R6
- Improved recognition of Yubikey FIPS (firmware 5.4.2 onwards) and ability to require this device type to be used for specific credential profiles.

Ability to ensure certain credentials can only be collected onto a Yubikey FIPS device, helping enforce security policy requirements.