



Phishing-Resistant Credentials, Simply Managed at Scale with MyID



Credential Lifecycle Management for Swissbit Devices

Features at a glance

- PKI and FIDO2 credential issuance and lifecycle management
- PACS integration for physical and logical access with one key
- Certificate renewal, PIN unlock, updates, and revocation
- Full audit trail for regulatory compliance and reporting
- Air-gap-capable on-premises or private cloud deployment
- Scalable from hundreds to millions of users



The Joint Solution Advantage

The **Swissbit iShield Key 2** is a high-assurance FIDO2 and PKI security key, manufactured in Germany to the highest quality standards. MyID® CMS from Intercede adds the enterprise management layer that organisations need to deploy, operate and maintain iShield Key 2 devices across their workforce: from first issuance through to replacement and revocation.

PKI + FIDO2: One Key, One Platform

MyID CMS manages both X.509 PKI certificates and FIDO2 passkeys on the iShield Key 2 from a single administration platform. IT teams issue PKI certificates for network logon, email encryption and document signing, while FIDO2 credentials protect web and cloud application access. Both credential types are phishing-resistant and managed through the same central management platform.

PACS: Physical and Logical Access on One Device

MyID CMS can be integrated with Physical Access Control Systems (PACS) so that physical access credentials stored on the iShield Key 2 are managed alongside logical credentials. When a user's employment ends or their key is lost, a single action in MyID CMS can revoke both logical and physical access simultaneously. This removes a critical gap between IT and facilities security teams.

Secure Hardware. Enterprise-grade Management.

Key advantages

- **Government-grade credential management:** 20+ years trusted by governments, aerospace & defense, and financial institutions across 20+ countries
- **CA independent:** giving customers choice of PKI platform
- **Proven scale:** from a few hundred users to millions of credentials under management
- **Air-gap capable:** full on-premise or private cloud deployment providing data sovereignty
- **API-first:** full REST APIs for integration into existing business infrastructure

Standards and Compliance

The combined solution is designed for high-assurance, regulated environments and supports the following standards and frameworks:

- FIPS 140-3: iShield Key 2 hardware cryptographic module validation
- FIPS 201 / PIV: MyID CMS offer full compliance for high assurance environments
- FIDO2 / WebAuthn: hardware-bound, phishing-resistant authentication for web and cloud
- NIS2 / DORA: phishing-resistant MFA aligned to EU critical infrastructure and financial services mandates

Sovereign by design: Made in Germany

Swissbit iShield Key 2 is manufactured in Germany, providing verifiable supply chain integrity for authentication hardware. This is critical for government agencies, defense contractors and regulated industries where hardware provenance is a security and procurement requirement. MyID CMS is developed by Intercede in the UK and supports on-premise deployments that keep credential data within your jurisdiction, delivering an authentication stack with full data sovereignty.

Who It's for?

Government and defense: high-assurance, air-gap capable deployments with NIST-compliant authentication.

Financial services: DORA-compliant, phishing-resistant MFA with full credential audit trails.

Critical infrastructure and healthcare: NIS2-aligned strong authentication with physical access control.

Enterprise IT: scalable passwordless access across Active Directory, Entra ID and hybrid environments, supporting broad rollout.