



With MyID organisations have the enterprise ready software they need to deploy crypto based strong authentication using FIDO and PKI based credentials.

	FIDO	FIDO + MyID
Authentication server	✓	✓
Attestation check	✓	✓
Person / key binding		✓
Issuance policy		✓
Revocation		✓
Centralised audit		✓

DEPLOY FIDO ACROSS YOUR WORKFORCE AND SUPPLY-CHAIN

MyID + FIDO FOR IT TEAMS



- Control how users authenticate with FIDO, based on defined security policy
- Simplified policy-driven FIDO credential issuance that requires minimal IT effort
- Enable access to multiple systems with one FIDO credential, utilising MyID’s plugin with Active Directory Federated Services (ADFS) and REST integration APIs
- Control on revocation or replacement of FIDO credentials if employees lose or damage their credentialed device, change roles, or leave the business
- Management software that integrates into your existing IAM infrastructure for quick, easy deployment

MyID + FIDO FOR YOUR END USERS



- Simplified, passwordless login to corporate resources
- Remote access via smartphone, USB token, or laptop
- Single credential for remote access and login to cloud-based systems

MyID + FIDO FOR YOUR COMPANY




- Strong crypto-backed authentication to protect against the threat of data breach
- Enhanced user experience for employees who no longer have to remember numerous passwords, improving productivity and user satisfaction
- Reduction in IT help desk demands through password resets, system lockouts, and remote working access issues
- Capacity to extend strong authentication to the supply-chain by credentialing suppliers who access internal business systems with FIDO credentials


MULTI-DEVICE STRONG AUTHENTICATION

MyID supports a wide range of FIDO devices, including iOS and Android mobile devices, USB tokens including YubiKeys, and smart cards.


MOBILE




SMART CARD




USB TOKENS




PLATFORM AUTHENTICATORS




Fingerprint



PIN



Facial Biometric



Uniquely, MyID provides management over multiple authentication technologies and form factors, enabling organisations to mix and match technologies that best fit their needs and required levels of security, enabling a unified approach to issuing and managing FIDO and PKI credentials.

For example, an organisation could use:

- PKI based USB tokens for remote workers
- PKI based smart cards for finance staff, including signed and encrypted email
- Virtual smart cards for temporary workers
- FIDO security keys for the supply-chain and contractors

MyID provides unified credential management for all of these user groups from one single point, controlling policy, visibility and lifecycle management independent of the technology in use.

HOW DOES IT WORK?

ISSUANCE

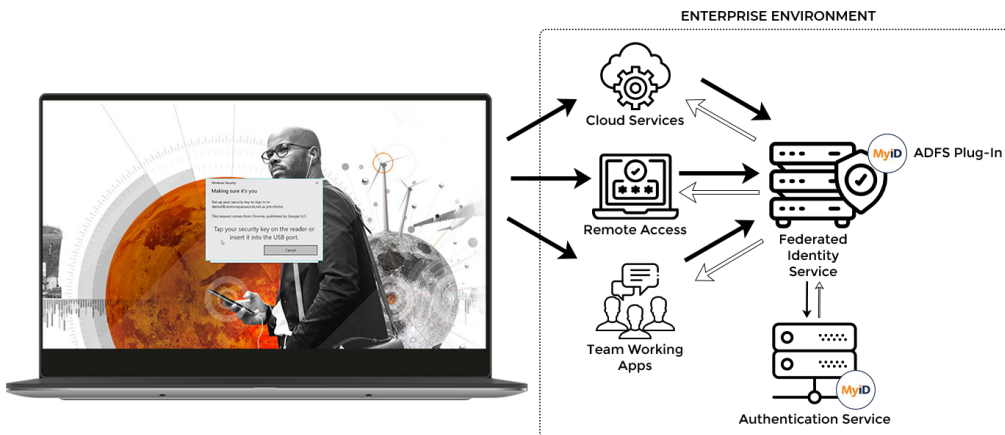
- MyID provides control over which groups of users can receive FIDO tokens
- Requests for new FIDO credentials can be operator-led, via API or self-service
- Issuance policy defines how a user must authenticate before collecting their FIDO credentials, options include, OTP, existing smart card, integrated Windows authentication and an existing FIDO key
- MyID binds a FIDO key to a user at issuance, keeping track of who has which FIDO credentials

AUTHENTICATION

- MyID provides a built-in FIDO certified authentication server and integrates with your existing infrastructure by ADFS plug-in or OpenID Connect
- Authentication operations are centrally audited for visibility and tracking purposes

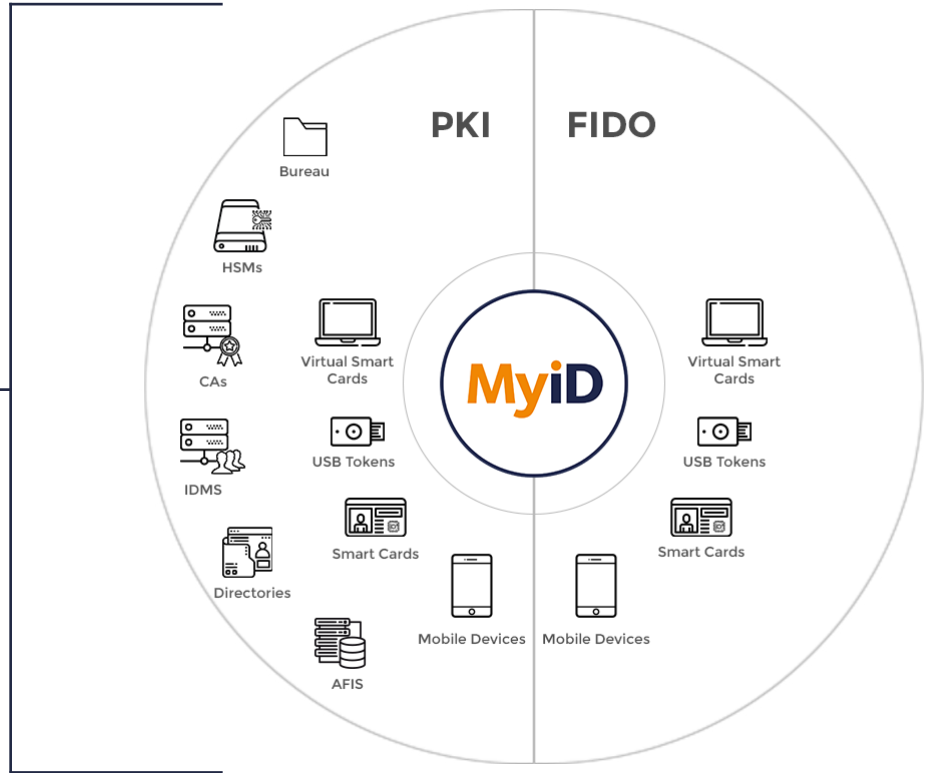
LIFECYCLE MANAGEMENT

- MyID keeps track of who has which FIDO credentials and provides visibility by enquiry, reports and API
- MyID provides organisations with the ability to revoke and replace credentials as employment status or rights change
- Lifecycle operations are audited, providing visibility and reporting over management operations
- Using IT-set security policies, the MyID authentication service will determine how a user is allowed to authenticate and guide the user through the authentication process
- Once authenticated, MyID authentication service will then communicate via the plug-in with ADFS to grant access to the end system



UNIFIED CREDENTIAL MANAGEMENT

One software platform to integrate, issue and manage PKI and FIDO



BENEFITS OF MyID + FIDO

CRYPTO BASED SECURITY

Deploy strong authentication across a broader user base

SIMPLE TO DEPLOY

MyID plugins and APIs offer unrivalled flexibility

ENHANCED CONTROL

Issue, revoke and replace FIDO credentials

COST EFFECTIVE DEPLOYMENT

Minimise investment in new tech and use what you have

OUTSTANDING USER EXPERIENCE

Simple PIN, fingerprint or facial biometric authentication

OPTIMUM MFA

Issue and manage PKI and FIDO from one system

FIND OUT MORE

Contact us now to arrange a MyID FIDO demo

info@intercede.com

+44 (0) 1455 558 111

+1 888 646 6943