




Why Yubico and MyID® work seamlessly together, to deploy and manage digital credentials on YubiKeys.

Yubikeys provide the highest level of assurance, MyID enables you to deploy and manage their lifecycle simply and at scale for both PKI and FIDO.

Review our features matrix below to see why MyID is the most feature rich credential management system for managing your YubiKey devices.

 MyiD Feature	 Key Benefits	YubiKey Security Series	YubiKey 5 Series	YubiKey 5 FIPS Series	YubiKey Bio Series - FIDO Edition
Security and Configuration with the YubiKey					
Secure the device by setting administrator and smartcard YubiKeys at assignment	Ensure access to administrative features of the YubiKey is restricted to your installation of MyID, using a secure management key diversified from a Hardware Security Module		Y	Y	
Communication to the YubiKey administrative functionality protected by 'Secure Channel Protocol'	Ensures low level communication to the device is secured, using global platform protocols		Y	Y	
Record the firmware version of the device in the MyID audit	Track the versions of devices in your environment to ensure they are up to date and has no vulnerabilities.		Y	Y	
Set enabled/disabled YubiKey features at assignment, and prevent modification of the settings	Control which features and interfaces of the token are available to be used (e.g. FIDO, Smartcard, OTP, NFC) Unique key for the device is set to prevent tampering with the settings outside of your MyID installation		Y	Y	
Lock the user PIN at issuance	Forces the user to reset the device PIN before it can be used, which can be an operator led or self service activity		Y	Y	
Set a randomised user PIN at issuance	The user PIN can be sent to the user in an email, ensuring an administrator does not have access to the device credentials		Y	Y	
Erase all credential content from the device and reset to standard settings	Resets content and security YubiKeys back to the CMS default settings		Y	Y	
Set touch & PIN policy on the device	For the primary certificate containers on the device, set TOUCH POLICY (never/always/cached) PIN POLICY (never checked, once per session, always checked) SET PIN RETRIES (can set PIN retries and PUK retries values)		Y	Y	
Require FIPS certified YubiKeys	Issuance of any credentials from MyID is blocked unless the YubiKey has been FIPS certified (using built in attributes of the device for verification)		Y	Y	

 MyID Feature	 Key Benefits	YubiKey Security Series	YubiKey 5 Series	YubiKey 5 FIPS Series	YubiKey Bio Series - FIDO Edition
Certificate Management on YubiKeys					
Generate cryptographic keys on the device for use in certificate requests	Maintain high levels of security compliant with best practice and security standards.		Y	Y	
Write issued certificates to the containers on the device	Simplify deployment of PKI		Y	Y	
Inject cryptographic keys generated off device to the containers on the device	Used where the certificate is to be later recovered, for example certificates that encrypt data		Y	Y	
Add recovered certificates to the key history containers on the device	Allows older encryption certificates that are still required for data decryption to be stored on the device		Y	Y	
Add additional identity certificates to the YubiKey history containers on the device	For privileged user authentication e.g. server administrators with separate windows accounts		Y	Y	
Remove certificates and keys from the device	Ensure only the correct credentials are deployed and available.		Y	Y	
Authentication with YubiKeys & MyID					
Integrate FIDO MFA to your WebAuth/OpenID Connect compatible systems	Uses MyID authentication server to support Identity Provider features	Y	Y	Y	Y
Integrate certificate based MFA to your WebAuth/OpenID Connect compatible systems	Uses MyID authentication server to support Identity Provider features		Y	Y	
Logon to Windows with a YubiKey with primary identity certificate (Smartcard)	Protect your system access with high assurance credentials		Y	Y	
Logon to Windows with a YubiKey with additional identity certificate (Smartcard)	Requires Yubico minidriver to be installed		Y	Y	
Limit authentication to MyID for administration to High Assurance FIDO tokens only	Ensure privileged access to MyID uses highest level of authentication	Y	Y	Y	Y
FIDO Management on YubiKeys					
Policy control to define the issued FIDO token as basic or high assurance level	MyID authentication server can limit authentications to high assurance tokens only	Y	Y	Y	Y
Policy control to require multi factor authentication capability on the FIDO token	Choose the level of security appropriate for the information or systems you are protecting	Y	Y	Y	Y
Enforce Authenticator Attestation Check	Verify your device is a genuine YubiKey before use	Y	Y	Y	Y
Require Client Side Discoverable Key	A simplified user log on without entering a user name.	Y	Y	Y	Y
YubiKey Lifecycle Administration					
Role based YubiKey request process	Create requests for YubiKeys with available profiles (defining credential content, issuance process and security policy) based on administrator role	Y	Y	Y	Y
Disable/enable issued YubiKey preventing use of credentials	To ensure lapsed credentials or compromised devices are immediately revoked.	Y	Y	Y	Y
Request replacements and renewals of an issued YubiKey	Simplify lifecycle management for lost or expiring devices	Y	Y	Y	Y
Cancel and unassign a YubiKey, removing all authentication capabilities managed by MyID	Immediate revocation enhancing security	Y	Y	Y	Y
View a persons token assignment and lifecycle event history	Full visibility of credential management lifecycle events for simplifying audit compliance	Y	Y	Y	Y
Multi-step issuance process with additional approval stages	Policy controlled device issuance enabling an organisation to choose the level of security that best fits their requirements	Y	Y	Y	Y
Audit trail for lifecycle management activities	Full visibility of credential management lifecycle events for simplifying audit compliance	Y	Y	Y	Y

 MyID Feature	 Key Benefits	YubiKey Security Series	YubiKey 5 Series	YubiKey 5 FIPS Series	YubiKey Bio Series - FIDO Edition
YubiKey Lifecycle Administration Cont/...					
Lifecycle management via REST APIs	Simple integration into your existing IDAM solutions	Y	Y	Y	Y
Set fixed or policy driven expiry date of credentials	Flexible control of the life time of a credential supporting both permanent and temporary workers	Y	Y	Y	Y
Token assignment reports based on device type, profile & user group	Ensuring operational management information is easily available to those who need it	Y	Y	Y	Y
Administrator assignment of a YubiKey to a person (face to face)	High security issuance of devices		Y	Y	
Request updates to security policy/authentication capabilities on an issued YubiKey	Ensure devices in the field are configured to the latest security standards		Y	Y	
Administrator controlled PIN Reset of a YubiKey with policy driven authentication requirements	Simple interfaces for helpdesk to assist users in unlocking their devices		Y	Y	
Remote PIN Reset using 'Challenge Response' mechanism for pre-windows logon	Offline unlock capability ensuring high levels of service		Y	Y	
Restrict issuance to 'known' devices	Allows YubiKeys to be pre-registered in MyID to prevent unknown devices being used		Y	Y	
Assign 'Additional Identities' to the user	Add privileged access certificates to the YubiKey, representing a different UPN/Windows Account to the primary certificates		Y	Y	
YubiKey Lifecycle Self Service					
Secure remote self service activation (FIDO credentials)	"No software installation required, uses browser, any operating system Registers the token with MyID Authentication Server"	Y	Y	Y	Y
Self service collection of a YubiKey after authentication with a trusted certificate (Derived Credentials)	"Meets NIST SP800-157 process requirements for 'PIV Derived Credentials' Any TLS/SSL authentication certificate can be used, if issuer is trusted by the MyID server (configuration)"	Y	Y	Y	Y
Secure remote self service activation (Smartcard Certificates)	Self Service App manages collection process on Windows computers, including authentication before collection		Y	Y	
Self service PIN Change	Allows the user to change the user PIN to a new value at any time		Y	Y	
Reset PIN of the YubiKey before Windows Logon (Challenge Response)	MyID Windows credential provider supports process in conjunction with YubiKey minidriver		Y	Y	
Self Service collection of updates/re-provision of all issued content	"Self Service App allows update or full reconfiguration of the YubiKey 'in the field' User authenticates with device PIN for additional security Automated or operator requested updates for the device, including certificate renewals"		Y	Y	

Contact us now to discover how MyID and YubiKey's can benefit the security of your organisation:

info@intercede.com

+44 (0)1455 558 111

+1 888 646 6943