ENTRUST and INTERCEDE MyID: SECURING THE ENTERPRISE WITH STRONG AUTHENTICATION

Weak authentication solutions present a major risk to businesses, they also deliver a poor user experience, slow down productivity and drain IT resources.

Together Entrust and Intercede present a proven solution for IT leaders to operate and manage strong authentication across their workforce.

A COMBINED SOLUTION FOR

- Large enterprises who want to use the most secure method of multi-factor authentication for their workforce

- IT leaders who understand the inherent weakness of passwords and one-time password (OTP) solutions and want crypto-protected multi-factor authentication (MFA)

- Organisations looking to establish trusted identities across their user base to enable secure remote working

- Organisations looking to support bring-your-own-device (BYOD) policies

- Organisations looking to deploy smart cards as part of their IAM technology mix, along with the flexibility to issue credentials to other form factors including USB tokens and virtual smart cards

- Organisations that demand strong protection of their private keys using Hardware Security Modules (HSM)

- IT leaders looking for a proven solution to issue and manage end user credentials at a scale running from hundreds to millions

- IT leaders who want a well-integrated solution that will fit into existing IT architecture and business processes

- IT leaders who want to deliver seamless strong MFA for end users, across smart card, mobile devices, USB tokens and virtual smart card technology

WHY USE ENTRUST PKI AND HSMs WITH MyID

Through Entrust PKI and Hardware Security Modules (HSM) technology, managed by MyID credential management software, IT leaders have a proven end-to-end solution to provision cryptographic protected credentials using public key infrastructure (PKI).

Unlike passwords, OTPs or other MFA solutions, PKI strongly binds digital identity to an individual. An identity that is secured by cryptography, simple for employees to use and easy to manage for IT teams.

- Deploy cryptographically protected digital identities with Entrust Certificate Authority together with MyID

- Establish a strong hardware-backed root of trust with an Entrust nShield HSM protecting keys for the CA and MyID

- Create person-bound digital identities through MyID Enterprise's integration with Microsoft Active Directory

- Deploy digital identities to the technology your users want to use as part of their day to day role

- Have the control your IT team needs to set and enforce security policies, replace and remove user credentials, all backed up by a central signed audit trail for non-repudiation of operations
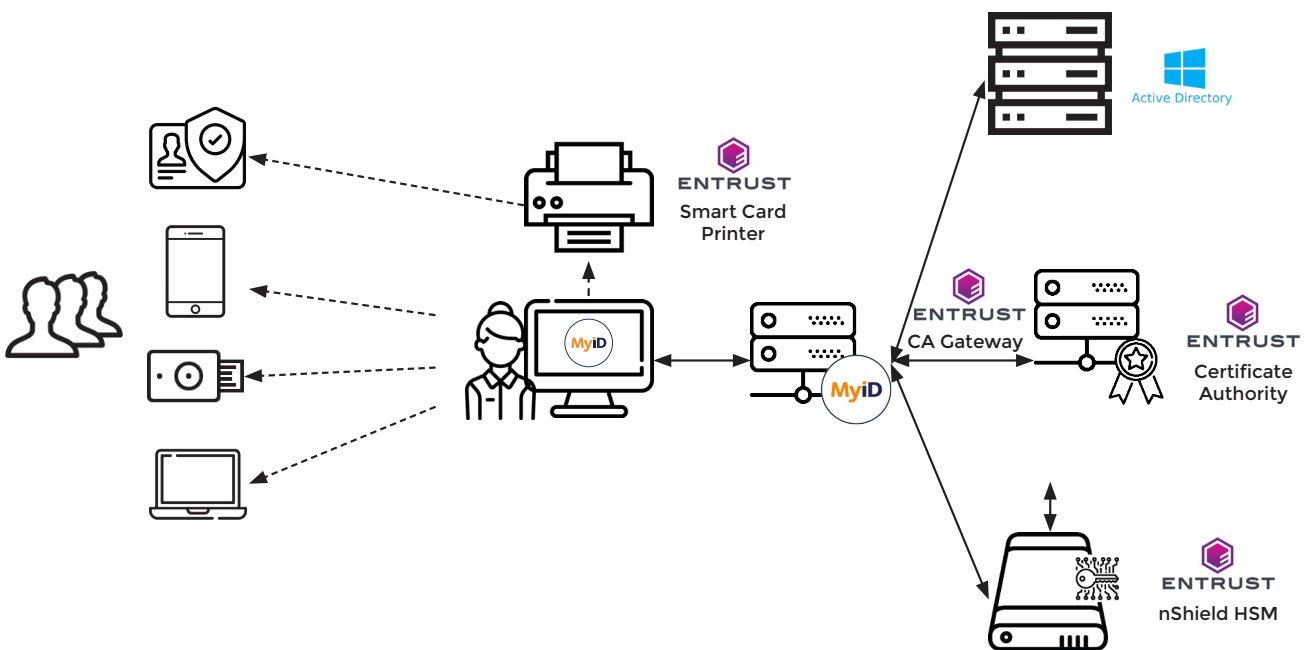
HOW THE SOLUTION WORKS

Entrust nShield HSM - a hardware security module, secures private keys used by the CA and MyID to protect data at rest and in transit

Entrust Certificate Authority - generates trusted digital certificates used to identify end users, also provides secure key archive and recovery capabilities

Entrust CA Gateway - gives the ability to connect to the on-premise, cloud or hybrid CA technologies

MyID Credential Management System (CMS) - provides all of the business processes required to issue PKI based digital identities to end users on secure devices, including full lifecycle management. Out of the box Integration with Entrust Certificate Authority, Entrust nShield HSM, plus connectivity to sources of user data such as Active Directory or identity management systems.

BENEFITS OF ENTRUST WITH MyID

PROVEN INTEGRATION
Together Entrust Certificate Authority, Entrust nShield HSMs, and MyID credential management software have long standing, proven integrations currently managing millions of identities worldwide

MINIMISE DISRUPTION
Shaped around ease of use for operators and end users, MyID Enterprise connects into Entrust Certificate Authority and Entrust nShield HSMs and guides IT professionals through the process of setting up strong MFA in line with your organisation's security policies

DELIVER BEST PRACTICE AT SCALE
With Entrust and MyID organisations have the cornerstone technologies of a best-in-class strong MFA solution that has the capacity to scale up from deployments of the low thousands up to the millions

BE COMPLIANT
Strong authentication is increasingly being legislated by governments worldwide, MyID Enterprise can be configured with Entrust Certificate Authority and Entrust nShield HSMs to meet specific compliance demands Including FIPS 201

FLEXIBLE TO YOUR ORGANISATION'S NEEDS
Deploy and manage digital identities across smart cards, USB tokens, mobile and virtual smart cards, on-premise, in the cloud or as a hybrid deployment

JOIN A COMMUNITY OF ENTERPRISES AND GOVERNMENTS
Entrust and MyID are deployed across many of the world's enterprises and governments, issuing and managing millions of digital identities on their behalf today. Have confidence in a tried and tested solution

LOW TOTAL COST OF OWNERSHIP
By Integrating with existing in-house infrastructure and enabling automated processes, the solution minimises the cost of issuing and managing digital identities at scale

STAY IN CONTROL
With flexible policy control over who is issued which credentials and full auditing and reporting capability over which credentials are in use

OUR TECHNOLOGIES

Technology	Vendor	Product
Certificate Authority	Entrust	Entrust Certificate Authority
Hardware Security Module	Entrust	Entrust nShield HSM
Credential Management System	Intercede	MyID Enterprise MyID PIV

CONTACT US TO FIND OUT MORE

Contact us now to discover what MyID and Entrust has to offer your organisation:

info@intercede.com	+44 (0)1455 558 111	+1 888 646 6943
info@entrust.com	+1 888 690 2424	+1 952 933 1223