DIGITAL TRUST
from Silicon to Services

intercede

MyID

Virtual smart card management for Windows

Say goodbye to passwords and hello to increased security and convenience with virtual smart cards for Windows devices.

Microsoft® Windows® 8 introduced the concept of virtual smart cards (VSCs). VSCs use the Trusted Platform Module (TPM) - a dedicated secure hardware processor built into the majority of PCs - to store and use keys in a cryptographically secure manner.

Using a virtual rather than a physical smart card can reduce the cost and complexity of deployments because there is no need to supply cards, readers and middleware to every user.

Like any secure device and credential, VSCs must be managed. MyID® from Intercede® provides VSC management capabilities from issuance through to credential end of life. Linking to user data stores MyID effectively binds the person to the VSC. This chain of trust is essential to ensure that the user is who they claim to be and that the credential on the VSC can be trusted.

The secure audit and reporting built into MyID also ensures that organizations are in full control of which identities and credentials are in use and which can be trusted.

Multiple mobile platforms

With your existing Cloud services

Using the latest mobile phone security features

How it works

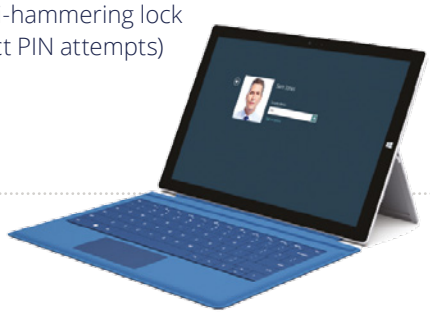
MyID acts as a link between the user data store (e.g. directory or HR system), credentialing authority (PKI), devices (TPM-equipped laptop or tablet) and the user. The sequence below is a typical example of initial provisioning via a self-service model:

1. The employee is already using a laptop or tablet equipped with an embedded TPM, but is logging on to the domain with a username and password
2. Either an IDMS (such as Microsoft FIM) instructs MyID to issue a VSC to the user, or a MyID operator uses MyID to select the user that needs the VSC from the directory
3. MyID generates a 'job' to be collected
4. The next time the user logs onto Windows they are notified that they have a VSC to collect
5. The user decides to collect the VSC now and is guided through a simple self-service app
6. During the self-service process MyID communicates securely with the TPM to create a VSC
7. MyID prompts the user to choose and verify a PIN for the VSC
8. MyID then generates keys on the VSC via the cryptographic functions build into Windows (no additional middleware is required)
9. Private keys remain protected by the TPM and public keys are formed into a certificate request
10. MyID sends the certificate request to the certificate authority (CA), e.g. the certificate services capability built into the Windows Server
11. MyID retrieves the certificates from the CA
12. MyID writes the certificates to the VSC
13. The process is complete and the employee can now use their VSC in the same manner as a physical smart card

Lifecycle management

In addition to issuing VSCs, MyID provides full lifecycle management including:

- Remote unlock (VSC becomes locked due to incorrect PIN entries while the user is offline)
- Temporary VSC replacement (forgotten laptop)
- Permanent VSC replacement (new laptop)
- VSC recovery, including archived encryption keys (lost laptop)
- Remote revocation of VSC (stolen laptop)
- Erasure of VSC (user no longer has access rights)
- Reset of TPM anti-hammering lock (multiple incorrect PIN attempts)



Features and benefits

What can VSCs do for you?

- **Enhance security** by using commercial off-the-shelf (COTS) products; user authentication can be enhanced quickly and efficiently
- **Save you money** on the purchase of smart cards and readers -VSCs can be deployed with no material cost and do not suffer from the normal wear and tear associated with physical cards
- **Two-factor authentication to secure cloud services** allows you to ensure that only users with strong credentials and appropriately configured devices have access to online services
- **Make credentials less likely to become lost or misplaced** as they are bound to devices that the owner uses on a day to day basis. Owners are also likely to notice the loss of these devices more quickly than they might with a conventional smart card

Key features:

- Simple self-service provisioning of VSCs and certificates to TPM-equipped devices such as laptops and tablet devices running Microsoft Windows 8 or above
- Solution also available on Windows 7
- Integrates with existing Microsoft infrastructure such as Active Directory, Microsoft FIM and Microsoft Certificate Services
- Supports key recovery, allowing VSCs to be used for ecure email
- Supports multiple VSCs per TPM, allowing devices to be shared by multiple users with distinct identities
- Option to only issue VSCs to known users on known devices, allowing control of who has access to resources and from which device

@ info@intercede.com www.intercede.com intercedemyid
Suite 920, 1875 Explorer Street, Reston, VA 20190, USA +1 888 646 6943