DIGITAL TRUST
from Silicon to Services

intercede

Lifecycle management made simple with the MyID self-service app

Key features

- Cardholders are informed by MyID when there is an action that they need to perform
- Simple guided workflow to collect updates
- Secure process requiring two-factor authentication
- Works with existing implementations of MyID
- Actions are recorded in a central secure audit trail, which allows helpdesk operators to see which user has performed which action
- Supports multiple languages
- Designed to be accessible for users with a visual impairment – supports screen readers and will adopt high contrast settings in Windows

The challenge

Organizations often use smart cards to facilitate physical and logical access for employees that work on their premises, as well as employees who regularly work from home or travel on business who need to access the company network. In order to secure this process, each employee is issued a smart card that they use for two-factor authentication (something I have - the card, and something I know - the PIN) to resources.

Smart cards often require updates and changes after they have been distributed to users, and this process is called lifecycle management. Lifecycle management involves activities such as renewal of certificates, collection of updates (e.g. the new version of an applet) and policy changes (e.g. moving from an SHA1 certificate authority to an SHA2 certificate authority, resulting in the need to issue replacement certificates to an existing card, or starting to issue encryption certificates onto existing cards).

Users must be informed that there are actions to be completed, and a common way of doing this is by sending them an email. Unfortunately some users ignore emails, are too busy or simply forget about the task. In addition, when users respond to an email request and update their card, there is no easy way for a helpdesk administrator to track this.

In order to manage their smart card the employee needs to use the card management system (CMS). Non-technical employees may feel that this interface is too complex for them, which means that they either put off completing the required updates or simply ask the helpdesk for assistance.

The in-house helpdesk is made up of permanent support staff who are trained on all the functions of the CMS. These employees may have other duties apart from supporting the CMS that slow down their response time, or the employee may have to log a report and wait for somebody to assist them. This means that the employee is prevented from carrying out normal tasks such as logging onto the network or entering company sites, which lowers productivity and causes frustration for the user. The employee may even be forced to stop working until the helpdesk can assist them, which wastes time and costs the company money.

In order to ensure continuation of service and prevent 'down time' users need to be able to manage their own smart cards, with the helpdesk function available as back up rather than as the first resort for card management. This would also lead to cost savings through the employment of fewer helpdesk staff.

Multiple mobile platforms

With your existing Cloud services

Using the latest mobile phone security features

The MyID solution

The MyID® self-service app from Intercede® is an easy-to-use interface that is linked to an organization's existing MyID server. It allows employees to perform lifecycle management tasks independently from their own desktop without the need for training or help from an administrator. As long as the MyID app is installed, employees can request credentials for a range of devices including computers, tablet devices and smartphones.

When an employee logs on to the network, the MyID self-service app checks to see if there are any activities that the cardholder needs to perform. If there are, the user is notified of this by a pop-up balloon similar to that used by the operating system. The familiar appearance of the request means that users immediately recognize that action is required and proceed to the MyID self-service app. If a user decides not to complete the action then they are reminded each time that they log on that they still have updates or certificates awaiting collection.

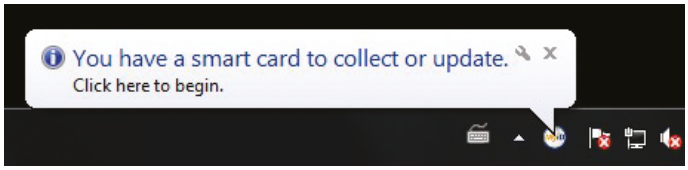
The MyID self-service app guides users through the process of managing their cards (e.g. applying updates or collecting new certificates) using clear, simple instructions, while recording the actions that have been taken in MyID to provide a secure audit trail. This allows administrators to track how many people have completed an update successfully and manage the rest by exception.

The MyID self-service app also supports the use of virtual smart cards using Windows® 8.

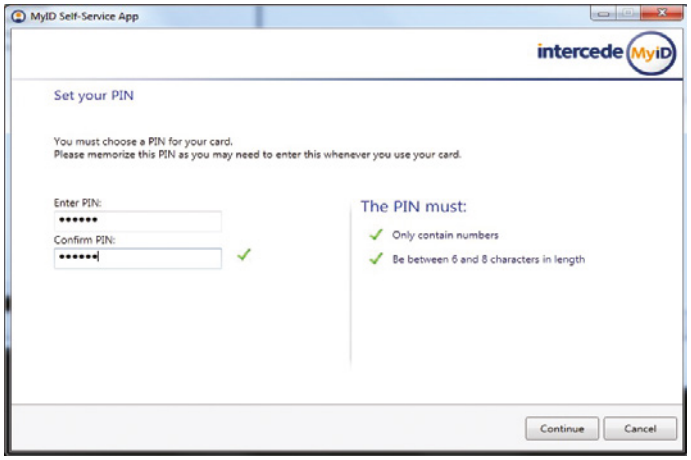
How does it work?

Certificate renewal

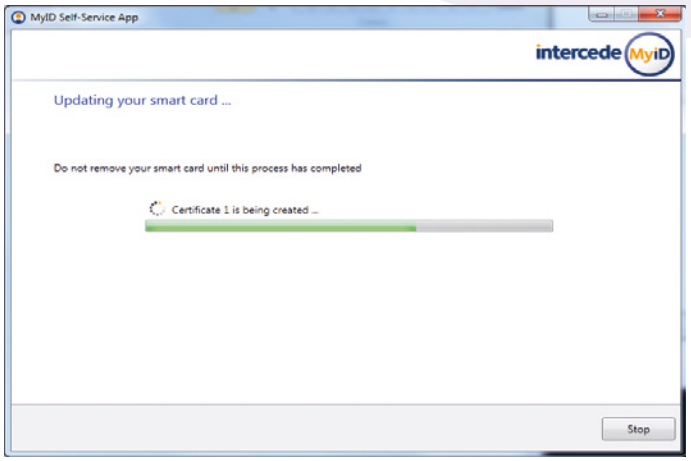
1. An employee's certificate is due to expire soon. This is flagged in MyID so that the employee can be notified in advance that they will need to renew the certificate for continued access
2. MyID automatically generates an update request for collection
3. The employee logs on to Windows
4. The MyID self-service app checks whether there are any jobs to collect
5. The app displays a pop-up balloon to let the employee know that action is required
6. The employee chooses to collect the job immediately and clicks on the balloon



7. The self-service app guides the employee through the process of collecting the new certificate via an easy-to-use interface. This may involve (configurable):
   - PIN entry
   - Fingerprint authentication
   - Validation of a one time password provided to the user
   - Acceptance of terms of use



8. Private keys are generated (on-card for signing keys and off-card and archived for encryption keys)
9. A certificate is retrieved from the certificate authority and written to the card



10. The successful collection is recorded in the central secure audit trail on the MyID server
11. The employee can now continue to use their card as normal

Policy change to enable secure email

1. A policy is changed to require secure signed emails when communicating financial information
2. A MyID administrator logs in to MyID and changes the policy for the organization's Financial Controller. In order for this employee to use the required secure email, encryption and signing certificates must now be written to his smart card
3. An administrator then uses MyID to request a card update for the Financial Controller
4. The Financial Controller logs on to Windows
5. He is notified that there is an update to collect and chooses to collect it immediately
6. The self-service app guides him through the process of generating, archiving and collecting new encryption and signing certificates via an easy-to-use interface
7. The successful collection is recorded in the central secure audit

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

FO/PACSLACS/A4/USEN/140327