



# Intercede MyID 7.1

## Allgemeine Funktion

**CRYPTAS it-Security GmbH**

Modecenterstrasse 22/B2  
A-1030 Wien

[www.cryptoshop.com](http://www.cryptoshop.com)  
[www.cryptas.com](http://www.cryptas.com)

## Allgemeines zur Funktion von Intercede MyID

Intercede MyID ist ein leistungsstarkes Werkzeug zur Verwaltung von Smartcards und Smart Tokens. Mit ihm kann der gesamte Lebenszyklus von Smartcards oder Smart Tokens von der Ausstellung über Erneuerung oder Ersatz bis zum Einzug abgebildet und verwaltet werden. Alle notwendigen Prozesse und Operationen sind in Intercede MyID bereits vorbereitet und können nach geringer Konfiguration sofort ausgeführt werden, ohne dass eine mühevoll Implementierung von Prozessen und der dazu notwendigen Infrastruktur notwendig wäre. Intercede MyID bietet dazu viele vorbereitete Operationen wie etwa automatische Verständigung, Zertifikatserneuerung, Zertifikatswiderruf, Pin Management, Rollenmanagement, Recovery Funktionen, Benutzerunterstützung, Massenausstellung und Bedruckung. Darüber hinaus werden alle Informationen zu Karten, Karteninhabern und Zertifikaten an einem zentralen Ort gespeichert.

### Schutz des Zugriffs auf die Smartcard Verwaltung

Der Zugriff auf alle Einstellungen oder Operationen, die mit der Ausstellung oder Verwaltung der Smartcards zu tun haben, wird mittels Smartcard gesichert. Optional wird eine alternative Anmeldung mittels Authentisierungsfragen angeboten, die für Benutzer einen sehr eingeschränkten Zugriff auf Selbsthilfefunktionen wie etwa Entsperren gesperrter Karten oder Ausstellen von Ersatzkarten ermöglicht.

### Pin Management

Intercede MyID bietet alle notwendigen Funktionen und Prozesse, die zu einem Einsatz von Smartcards mit PIN Schutz notwendig sind:

- Jede Smartcard erhält eine individuelle PUK, die dann in der Datenbank verschlüsselt abgelegt wird.
- Ein, eventuell von Werk aus eingestellter, initialer PUK (Admin Pin) wird vom System vor der Nutzung der Karten geändert.
- Dem Benutzer wird bei der Ausstellung der Smartcard eine PIN zugewiesen
- Der Benutzer wird per Email (optional) über seine PIN informiert.
- Der Benutzer kann seine PIN selbst ändern oder zurücksetzen oder seine Karte im Notfall entsperren (optional)
- Der Administrator konfiguriert eine PIN Policy, in der die Länge der PIN und die Kriterien (Sonderzeichen, Ändern bei erster Anmeldung) definiert sind.

### Unterstützung von Biometrischer Authentisierung

Wenn die Smartcard oder das Token biometrische Erkennung unterstützt, so kann durch MyID die Nutzung der biometrischen Merkmale anstelle der PIN ermöglicht oder erzwungen werden. Benutzer können ihre biometrischen Merkmale auch ohne Unterstützung durch den Helpdesk (persönliche Abholung durch den Benutzer bei der Ausstellung) selbständig in die Karte an „Selfhelp“ Terminals oder an ihrem eigenen PC (optional) einlesen.

#### Skalierbarkeit:

Intercede MyID kann auch sehr große Organisationen unterstützen. Durch die Trennung der einzelnen Operationen vom zentralen Datenbanksystem (ActiveX Client für Webinterface) wird die Anzahl der unterstützten Benutzer praktisch nur durch die mögliche Größe der Datenbank und die Leistungsfähigkeit des Webserver begrenzt. MyID unterstützt auch Architekturen mit mehreren Windows Domänen und verschiedenen Standorten. Weiters ist MyID sehr gut in seinem Aussehen („Look and Feel“) an die Ansprüche eines Unternehmens anpassbar.

#### Delegation der Prozesse:

Durch die Definition von Rollen und die Zuordnung von Rechten zu diesen, können viele Aufgaben und Prozesse direkt von den Personen ausgeführt werden, in deren Verantwortungsbereich die Verwaltung der Mitarbeiter selbst liegt.

#### Beispiele:

- Das Ausstellen und Einziehen von „Company ID Cards“ geschieht direkt bei der Personalabteilung selbst.
- Tageskarten oder Gästepässe werden von den Abteilungsleitern zugeordnet und ausgegeben
- Der Helpdesk reaktiviert gesperrte Karten

#### Integration in Microsoft Umgebungen

- MyID verwendet Microsoft Active Directory als Verzeichnisdienst
- MyID verwendet Microsoft Exchange Server zur Verständigung der Benutzer
- MyID verwendet Microsoft SQL Server als Host für seine Datenbank
- MyID verwendet Microsoft IIS Server als Host für sein Webinterface
- MyID verwendet die in Windows Server 2000 oder 2003 mitgelieferte, in Active Directory integrierte PKI zum Erstellen der Zertifikate

#### Unterstützung anderer Umgebungen

- MyID kann jedes andere LDAP Verzeichnis nutzen (Beispiele: Lotus Domino, iPlanet und andere)
- MyID verwendet kann die PKI Systeme namhafter anderer Hersteller zum Erstellen der Zertifikate verwenden (Beispiele: Entrust Security Manager, Cybertrust, Verisign und andere)
- MyID kann Oracle 10 als Host für seine Datenbank nutzen

## Komponenten von Intercede MyID

Intercede MyID besteht aus 4 Komponenten:

- Der Application Server
- Die MyID Datenbank
- Die Security Management Console
- ActiveX Client für die Security Management Console

Intercede MyID baut in seiner Funktion auf bestehende Komponenten der IT Infrastruktur auf (die folglich vorhanden sein müssen):

- Ein Verzeichnisdienst (LDAP Directory, Microsoft AD)
- Eine Public Key Infrastructure
- Ein SQL Server
- Ein Web Server
- Die zu den verwendeten Smartcards oder Token passende „Middleware“ (ausgerollter CSP, PKCS#11)

Der Application Server:

Die Intercede MyID Applikation ist für die Kommunikation zwischen allen beteiligten Komponenten von MyID sowie der PKI und dem Verzeichnisdienst zuständig. Sie schreibt in und liest aus der MyID SQL Datenbank, erledigt alle zertifikatsbezogenen Aufgaben (Anforderung, Ausstellung, Sperrung) und liest benutzerbezogene Informationen aus dem Verzeichnisdienst. Der Dienst läuft unter einem Dienstkonto, das mit einem Key Recovery Zertifikat ausgestattet sein muss und entsprechende Berechtigungen zum Ausstellen und Verwalten von Zertifikaten in der Certification Authority und an den jeweiligen Certificate Templates braucht.

Die MyID Datenbank:

Die MyID Datenbank enthält alle notwendigen Information zu den ausgestellten Smartcards und den darauf befindlichen Zertifikaten. Sie enthält ebenfalls Informationen zu Personen, die mit Zertifikaten ausgestattet wurden sowie deren Berechtigungen und Rollen. Darüber hinaus werden auch Konfigurationseinstellungen, Informationen zur PKI und dem Verzeichnisdienst, Druckvorlagen und Profilen dort abgelegt. Die Datenbank kann als zusätzliche Datenbank auf einem bestehenden SQL Server betrieben werden. Sie ist in Klartext, einzelne Felder mit sicherheitsrelevanten Informationen (z.B. PUK) sind jedoch verschlüsselt.

Die Security Management Console:

Die Security Management Console von Intercede MyID ist ein Webinterface zur Administration von MyID und zur Ausstellung und Verwaltung von Smartcards und Tokens. Zugriff auf diese Konsole wird sowohl von Administratoren und Helpdesk Technikern als auch von Benutzern benötigt. Das Webinterface kann als Applikation (cgi) auf einem bestehenden Webserver laufen und benötigt ein Dienstkonto (Domain User) mit Berechtigungen in der MyID Datenbank.

Der ActiveX Client:

Zum Zugriff auf die Security Management Console wird ein ActiveX Client benötigt, der beim erstmaligen Besuch der Webseite automatisch heruntergeladen wird. Alternativ dazu ist ein Rollout mittels Softwareverteilungssystem möglich. Dieser Client wird aber nur zur Verwaltung von MyID und zum Ausstellen, Erneuern oder Einziehen von Smartcards benötigt. Es ist also nicht notwendig, ihn flächendeckend auszurollen. Die Anmeldung und Nutzung von Smartcards und Token an Computern funktioniert selbstverständlich auch ohne diesen Client.

Voraussetzungen bei der vorhandenen Infrastruktur:

- PKI-Policy Statement und Revocation List müssen für alle Benutzer verfügbar sein
- Der Webserver für die Management Console sollte für Helpdesk oder „Selfhelp“ Terminals erreichbar sein
- Das Root Certificate der unternehmenseigenen PKI muss für alle Client Computer vertrauenswürdig sein
- Das genutzte LDAP Verzeichnis muss zur Windowsanmeldung genutzt werden können (kein Problem bei Active Directory)

CRYPTAS it-Security  
Modecenterstrasse 22/B2  
A-1030 Wien, Austria  
T +43 (1) 798 96 96 – 0  
F +43 (1) 798 96 96 – 99  
info@cryptas.com

[www.cryptoshop.com](http://www.cryptoshop.com)  
[www.cryptas.com](http://www.cryptas.com)