

MyID Enterprise Service Description

(formerly known as MyID Enterprise for Symantec)

Introduction

MyID Enterprise (formerly known as *MyID Enterprise for Symantec*) is a comprehensive suite of management tools specifically designed to deploy smart cards and support a wide variety of smart card types and workflows. This suite of tools provides an enterprise with a fully featured card management system to address smart card lifecycle. In addition, this suite of tools includes a role-based management interface for enterprises to enroll applicants; graphically personalize smart cards; deploy Public Key Infrastructure (“PKI”) certificates; manage cryptographic keys; capture and install biometric data; as well as perform ‘one pass’ issuance of contact and contactless cards. Furthermore, this suite of tools enables agencies to easily enforce and manage rigid regulatory requirements by logging all system activity into a security audit database with extensive reporting capabilities.

MyID Enterprise is based on the standard MyID product from DigiCert’s supplier, Intercede Ltd. *MyID Enterprise* provides all the features available in Intercede’s MyID. In addition, the product is compatible with the DigiCert PKI Platform (formerly known as Symantec Managed PKI) (“MPKI”) Service to offer agencies a pre-packaged and integrated card management system (“CMS”) and PKI solution.

Capabilities

MyID Enterprise provides the following key capabilities:

- **Flexible Business Process Adaptation**

Define enterprise-specific enrollment and issuance processes within *MyID Enterprise*. An enterprise can configure the enrollment process for on-line pre-registration of applicants with multiple witnessing and authorizations stages. Also, an enterprise can decide which card production model – immediate, batch, or outsourced – works best for the issuance process. Furthermore, an enterprise can incorporate existing manual processes into the overall workflow sequence through scripted mechanisms.

- **Enroll and Identity-Proof all Applicants from a Single Interface**

Register applicants through the workflow interface of *MyID Enterprise*. This interface enables an enterprise to efficiently and securely collect and verify data entered by form entry, document scanning, and biometric capture devices. In addition, this interface strictly controls access to applicants’ data through a role-based, smart card authenticated management console.

- **Full Lifecycle Management of Smart Cards**

Manage the entire lifecycle of PKI certificates, biometrics, and other credentials held on the smart cards via a single consistent user interface in *MyID Enterprise*. An enterprise can request, issue, renew, replace, unblock, and revoke these cards according to well-defined policies. In addition, an enterprise can fine-tune the precise behavior for each process through sophisticated custom scripting.

- **Multiple Roles and Card Profile Support**

Access to each phase of the issuance process is strictly controlled through defined administrator roles in *MyID Enterprise*. These roles provide an enterprise procedural and data access control in a strongly authenticated manner. In addition, an enterprise can define the content, appearance, and issuance policy of a card via a card profile. Moreover, an enterprise can define as many card profiles as required to represent permitted combinations of content.

- **Supports Contact and Contactless Cards**

Configure card content based on enterprise-specific requirements for physical access control systems (“PACS”). *MyID Enterprise* supports a wide range of cards from multiple vendors and has fully integrated support for hybrid contactless cards required PACS.

- **Technology Vendor Independence**

Select most appropriate technologies based on enterprise-specific needs. *MyID Enterprise* supports a wide range of smart cards and middleware; USB devices; biometric solutions; LDAP directories; card printers; and identity proofing systems from multiple vendors.

- **SDK for System Integrators**

Integrate *MyID Enterprise* quickly with third-party systems using application program interfaces (“APIs”) available in the software development kit (“SDK”). This SDK offers an enterprise the ability to respond to events from external applications or use *MyID Enterprise* events to trigger actions to other applications. In addition, the SDK comes with an interactive project design tool to enable the rapid development of customized solutions.

- **Full Audit Trail and Flexible Reporting**

Design, view, and print customized reports from *MyID Enterprise*. Since all system activities are logged into a security audit database, an enterprise can produce these reports by taking advantage of the integrated support for the Crystal Reports reporting tool.

Technical Specifications

MyID Enterprise supports the following software and hardware components. Please see MyID product documentation for detailed information.

- **Server Platforms**

Windows Server 2012 R2

Windows Server 2016

- **Client Platforms**

Windows 10

Windows 8.1

Microsoft Windows 7 SP1

iOS 12.0, 11.0, 10.0

Android 9.0, 8.0, 7.0, 6.0

- **Web Browsers**

Microsoft Internet Explorer 11

- **Web Servers**

Microsoft Internet Information Services (IIS)

- **LDAP Directories**

Microsoft Active Directory

LDAP v3 compliant directory

- **Databases**

SQL Server 2016 SP2

SQL Server 2014 SP3

SQL Server 2012 SP4

- **PKI Certificate Authorities**

DigiCert PKI Platform for Shared Service Provider (formerly known as Symantec™ Shared Service Provider PKI)

- **Smart Cards and USB Devices**

Smart Cards

- Gemalto IDPrime MD
- Gemalto IDPrime PIV
- NXP/Athena IDProtect
- Giesecke & Devrient Smart Café Expert
- Giesecke & Devrient PIV
- IDEMIA ID-One PIV
- IDEMIA ID-One Cosmo
- Safenet Assured Technologies SC 650
- TCOS
- Cryptas TicTok

USB Tokens

- Safenet eToken
- Yubikey

- **Card Readers**

HID/Omnikey

SCM Microsystems

Gemalto

- **Card Printers**

HID/Fargo

Datacard

Matica

Zebra

- **Virtual Smartcards & Devices**

Microsoft Virtual Smart Card

Intel Authenticate

Cryptas Virtual Smart Card

- **Physical Access Control Systems**

Lenel

Other PACS connectors available on request

- **Hardware Security Modules**

Gemalto Safenet Network HSM

Thales nCipher nShield HSM

MyID ENTERPRISE SERVICE TERMS AND CONDITIONS

1. DEFINITIONS

“**Agreement**” means the Master Services Agreement or such other agreement entered into between DigiCert and Customer under which the Services set forth in this Service Description are provided by DigiCert to Customer.

2. CUSTOMER’S OBLIGATION

(a) Customer Obligations. Customer is solely responsible for acquiring and maintains requisite hardware requirements on its premises for the Services herein and maintaining the security of its network and computer systems.

(b) Customer’s Warranties. In addition to the express limited warranties set forth in the Agreement, Customer warrants to DigiCert that Customer will not monitor, interfere with, reverse engineer the technical implementation of, or otherwise knowingly compromise the security of any DigiCert system, software or Service.

(c) Audit. Not more than twice a year, DigiCert may audit and inspect, at its own expense, Customer’s utilization of the Services contemplated in this Service Description in order to ensure compliance with the terms of this Service Description, the Services Order and the Agreement. Any such audit will be conducted during normal business hours of Customer upon reasonable written notice to Customer and will not unreasonably interfere with Customer’s business activities. Customer shall reasonably cooperate with DigiCert in connection with any such audit. If the audit reveals that Customer has underpaid fees to DigiCert, such underpaid fees shall be immediately due and payable by Customer.

(d) Compliance with Local Laws. Customer is responsible for ensuring that Customer’s acquisition, use, or acceptance of public and private key pairs generated by DigiCert in accordance with this Service Description complies with applicable local laws, rules and regulations – including but not limited to export and import laws, rules, and regulations – in the jurisdiction in which Customer acquires, uses, accepts or otherwise receives such key pairs.

3. DIGICERT’S OBLIGATIONS

(a) Installation. DigiCert shall provide sufficient man days to Customer for installation and provision

of the *MyID Enterprise* service on the Customer's premises and systems; provided however, that Customer shall purchase such man days at DigiCert's current rates under an SOW to be agreed upon by the parties. In the event that additional work is required due to unusual or particularly complex Customer systems or requirements, such additional work may be purchased separately from DigiCert.

(b) Support and Maintenance. DigiCert shall provide Customer with second-level, whilst Intercede shall provide third-level, support and maintenance in connection with the service contemplated in this Service Description for the fees set forth in the Services Order to which this Service Description is applicable. The support and maintenance commitments of DigiCert are to provide telephone and email support commensurate with the support level selected by Customer for DigiCert PKI Platform for Shared Service Provider or such other DigiCert PKI solution for which Customer uses *MyID Enterprise*; conduct initial assessment of incident; and provide solution or workaround if possible. The support and maintenance commitments of Intercede for *MyID Enterprise* are to provide support to DigiCert from Monday through Friday, 9:00 AM to 5:30 PM (GMT) excluding UK public holidays; perform complex analysis of incident; and correct errors in *MyID Enterprise*.

(c) Disclaimers. EXCEPT AS SET FORTH IN THIS SERVICES DESCRIPTION OR THE AGREEMENT, THE SERVICES AND THE SOFTWARE ARE PROVIDED "AS IS" AND WITHOUT ANY WARRANTIES WHATSOEVER, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE (ALL OF WHICH ARE HEREBY DISCLAIMED). DigiCert makes not warranty that the Services will be uninterrupted or error-free.

4. EFFECT OF TERMINATION OF SERVICES FOR ANY REASON

In the event of a termination of the Services contemplated herein for any reason, (i) Customer will immediately cease use of the Services, (ii) the rights to use the Services and any related software or other components will immediately terminate, (iii) Customer will permanently delete any software related to the provision of the Services from any storage media upon which such software is stored and (iv) neither party shall be relieved of obligations or liabilities which accrued prior to the date of termination.