MyID PIV (Personal Identity Verification) Service Description
(formerly known as MyID PIV (Personal Identity Verification) for Symantec)

Introduction

MyID PIV (Personal Identity Verification) (formerly known as *MyID PIV (Personal Identity Verification) for Symantec*™) is a comprehensive identity and card management system to assist the United States Federal Government agencies in meeting the requirements in Homeland Security Presidential Directive -1 2 ("HSPD-12"). This system provides agencies a single interface for registering, identity proofing, issuing, and maintaining Personal Identity Verification ("PIV") cards for employees of these agencies according to the processes defined in Federal Information Processing Standards ("FIPS") Publication 201-1. In addition, this system has a role-based management interface for agencies to enroll applicants; graphically personalize PIV cards; deploy PIV applets and Public Key Infrastructure ("PKI") certificates; manage cryptographic keys; capture and install biometric data; as well as perform 'one pass' issuance of contact and contact less cards. Furthermore, this system enables agencies to easily enforce and manage rigid regulatory requirements by logging all system activity into a security audit database with extensive reporting capabilities. Finally, this system is compatible with the DigiCert PKI Platform for Shared Service Provider (formerly known as Symantec Shared Service Provider PKI) ("SSP")) service to offer agencies a pre-packaged and integrated PIV and PKI SSP solution.

Capabilities

MyID PIV provides the following key capabilities:

- **Flexible Business Process Adaption**

Define agency-specific enrollment and issuance processes within *MyID PIV*. An agency can configure the enrollment process for on -line pre-registration of applicants with multiple witnessing and authorizations stages. Also, an agency can decide which card product ion model – immediate, batch, or outsourced – works best for the issuance process. Furthermore, an agency 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 PIV*. This interface enables an agency 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 PIV cards**

Manage the entire lifecycle of PKI certificates, biometrics, and other credentials held on the PIV cards via a single consistent user interface in *MyID PIV*. An agency can request, issue, renew, replace, unblock, and revoke these cards according to well-defined policies. In addition, an agency 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 PIV*. These roles provide an agency procedural and data access control in a strongly authenticated manner. In addition, an agency can define the content, appearance, and issuance pol icy of a card via a card profile. Moreover, an agency can define as many card profiles as required to represent permitted combinations of content.

- **Supports Contact and Contactless Cards**

Configure card content based on agency-specific needs for physical access control systems ("PACS"). *MyID PIV* 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 agency-specific needs. *MyID PIV* 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 PIV quickly with third-party systems using application program interfaces ("APIs") available in the software development kit ("SDK"). This SDK provides an agency the ability to respond to events from external applications or use *MyID PIV* 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 PIV.* Since all system activities are logged into a security audit database, an agency can produce these reports by taking advantage of the integrated support for

- **Support for PIV Certificate History**

Supports the certificate history features in SP-800-73-3.

Technical Specifications

MyID PIV 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

- **Signature Capture**

  Interlink Electronics ePad or ePad II

- **Biometric Readers**

  Secugen Biometrics

  Cross Match

- **Physical Access Control Systems**

  Lenel

  HID PIVClass

  Other PACS connectors available on request

- **Hardware Security Modules**

  Gemalto Safenet Network HSM

  Thales nCipher nShield HSM

* * *

* * *

MyID PIV For DigiCert SERVICES TERMS AND CONDITIONS

1. DEFINITION

"Agreement" means the applicable agreement, which is entered into between DigiCert and Customer and incorporates this Service Description by reference.

2. CUSTOMER'S OBLIGATION

(a) Customer Obligations. Customer is solely responsible for acquiring and maintaining requisite hardware on its premises for the Services described herein and maintaining the security of its network and computer systems. Customer is responsible for setting up first-level support to Customer's individual users.

(b) Customer's Warranties. In addition to the express limited warranties set forth in the Agreement, Customer warrants to DigiCert that Customer (i) will not monitor, interfere with, reverse engineer the technical implementation of, or otherwise knowingly compromise the security of any DigiCert system, software or Service and (ii) will comply with its obligations under HSPD-12 and the processes and obligations set forth in the Federal Information Processing Standards Publication 201-1.

(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.

3. DIGICERT'S OBLIGATIONS

(a) Installation. DigiCert shall provide sufficient man days to Customer for installation and provision of the *MyID PIV* services on 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. *MyID PIV* is based on the standard MyID product from DigiCert's supplier, Intercede Ltd. Notwithstanding anything to the contrary in the Agreement, this provision applies to support and maintenance with respect to *MyID PIV*. 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. Customer will initiate contact with DigiCert for all second-level and third-level support requests. The support and maintenance commitments of DigiCert are to provide telephone and email support to Customer during the support hours 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 PIV;* conduct initial assessment of incident; and provide solution or workaround if possible. The support and maintenance commitments of Intercede for *MyID PIV* 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 PIV.*

(c) Disclaimers. EXCEPT AS SET FORTH IN THIS SERVICE DESCRIPTION OR THE AGREEMENT, THE SERVICES AND THE SOFTWARE AND 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 no 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 terminates, (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.