MyID PIV (Personal Identity Verification) for Symantec™
Service Description

Introduction

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-12 ("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 contactless 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 integrated with Symantec's Managed PKI Shared Service Provider ("SSP") service to offer agencies a pre-packaged and integrated PIV and PKI SSP solution.

Capabilities

MyID PIV for Symantec provides the following key capabilities:

- **Flexible Business Process Adaptation**

Define agency-specific enrollment and issuance processes within *MyID PIV for Symantec*. 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 production 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 for Symantec*. 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 for Symantec*. 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 for Symantec*. 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 policy 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 for Symantec* 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 for Symantec* 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 for Symantec 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 for Symantec* 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 for Symantec*. 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 the Crystal Reports reporting tool.

- **Support for PIV Certificate History**

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

Technical Specifications

MyID PIV for Symantec supports the following software and hardware components:

- **Server Platforms**

Microsoft Windows Server 2003 (Standard or Enterprise Edition, 32-bit) with no Service Pack, Service Pack 1, or Service Pack 2

Microsoft Windows Server 2003 Release 2 (Standard or Enterprise Edition, 32-bit) with no Service Pack, Service Pack 1, or Service Pack 2

Microsoft Windows Server 2008 Release 2

- **Client Platforms**

Microsoft Windows XP (Professional Edition) with Service Pack 2

Limited support for Windows Vista / 7

- **Web Browsers**

Microsoft Internet Explorer 7 or 8

- **Web Servers**

Microsoft Internet Information Server 5.0 or higher

- **LDAP Directories**

Microsoft Active Directory

- **Databases**

Microsoft SQL Server 2005 with Service Pack 1 or SQL Server 2005 Express

Microsoft SQL Server 2000 with Service Pack 3a and 4

Microsoft SQL Server 2008 R2

- **PKI Certificate Authorities**

Symantec SSP PKI

- **Smart Cards and USB Devices**

Aladdin NG-OTP

Axalto Cryptoflex (8K and 16K)

Axalto Cyberflex Access (16K, 32K, and 64K)

Axalto Cyberflex Access Developer

Axalto Cyberflex Campus

Axalto Cyberflex e-Gate

Gemplus GemSafe (GP8K and GP16K)

Gemplus Xpresso (16K, 32K, and 64K)

Gemplus Gem GXPRO

Gemplus Gem JCOP 41

Giesecke & Devrient SmartCafe Expert (32K and 64K)

Oberthur AuthentIC

Oberthur PIV Card

Gemalto PIV Card

Gemalto .NET Card

- **Card Readers**

ASEDrive IIIe

Axalto Reflex 20, 72, and USB

e-Gate USB Smart Card Reader

Gemplus GCR410, GemPC430, GemPC Twin, GemPC USB

Giesecke & Devrient PCT 200

Infineer / Tritheim SmartPort

Oberthur / CardMan Serial or USB

Omnikey CardMan Desktop Serial 1010, 2010, and 2011

Omnikey CardMan Desktop USB 2020, 3121, and 5121

Schlumberger Reflex Lite

SCM Microsystems SCR 331 USB reader

- **Card Printers**

Fargo DTC 525 with Windows 2000 PC/SC compliant smart card reader

Fargo HDP 600, 820, or 825 series with Windows 2000 PC/SC compliant smart card reader

DataCard SP35, SP55, or SP75 with Windows 2000 PC/SC compliant smart card reader

Magicard Rio/Tango 2e with firmware 3.13 or later

- **Signature Capture**

Interlink Electronics ePad or ePad II

- **Biometric Readers**

Precise 100 or 250 readers

Cross Match Verifier 300 or 310

Aware Preface

- **Adjudication Systems**

Aware Biometric Services Platform

Bio-Key Vector Segment Technology

- **Physical Access Control Systems**

AMAG / G4Tec MultiMAX Security Management 6.0.1

GE Picture Perfect 4.0 with import/export module

- **Hardware Security Modules**

SafeNet Luna SA

nCipher HSM

*** * ***

*** * ***

***MyID PIV For Symantec* SERVICES TERMS AND CONDITIONS**

1. DEFINITION

"Agreement" means the applicable agreement, which is entered into between Symantec 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 Symantec that Customer (i) will not monitor, interfere with, reverse engineer the technical implementation of, or otherwise knowingly compromise the security of any Symantec 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, Symantec 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 Symantec in connection with any such audit. If the audit reveals that Customer has underpaid fees to Symantec, such underpaid fees shall be immediately due and payable by Customer.

3. SYMANTEC'S OBLIGATIONS

(a) Installation. Symantec shall provide sufficient man days to Customer for installation and provision of the *MyID PIV for Symantec* services on Customer's premises and systems; provided however, that Customer shall purchase such man days at Symantec'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 Symantec.

(b) Support and Maintenance. *MyID PIV for Symantec* is based on the standard MyID product from Symantec's supplier, Intercede Ltd. Notwithstanding anything to the contrary in the Agreement, this provision applies to support and maintenance with respect to *MyID PIV for Symantec*. Symantec 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 Symantec for all second-level and third-level support requests. The support and maintenance commitments of Symantec are to provide telephone and email support to Customer during the support hours commensurate with the support level selected by Customer for Managed PKI Shared Service Provider Service or such other Symantec PKI solution for which Customer uses *MyID PIV for Symantec*; conduct initial assessment of incident; and provide solution or workaround if possible. The support and maintenance commitments of Intercede for *MyID PIV for Symantec* are to provide support to Symantec 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 for Symantec*.

(c) Disclaimers. EXCEPT AS SET FORTH IN THIS SERVICE 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). Symantec 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 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.