Entrust IdentityGuard Mobile Smart Credential 3.2

PIV-D Technical Integration Guide

Document issue: 1.1

Date of Issue: November 2019

Contents

Introduction to Entrust Datacard IdentityGuard Smart Credential Services

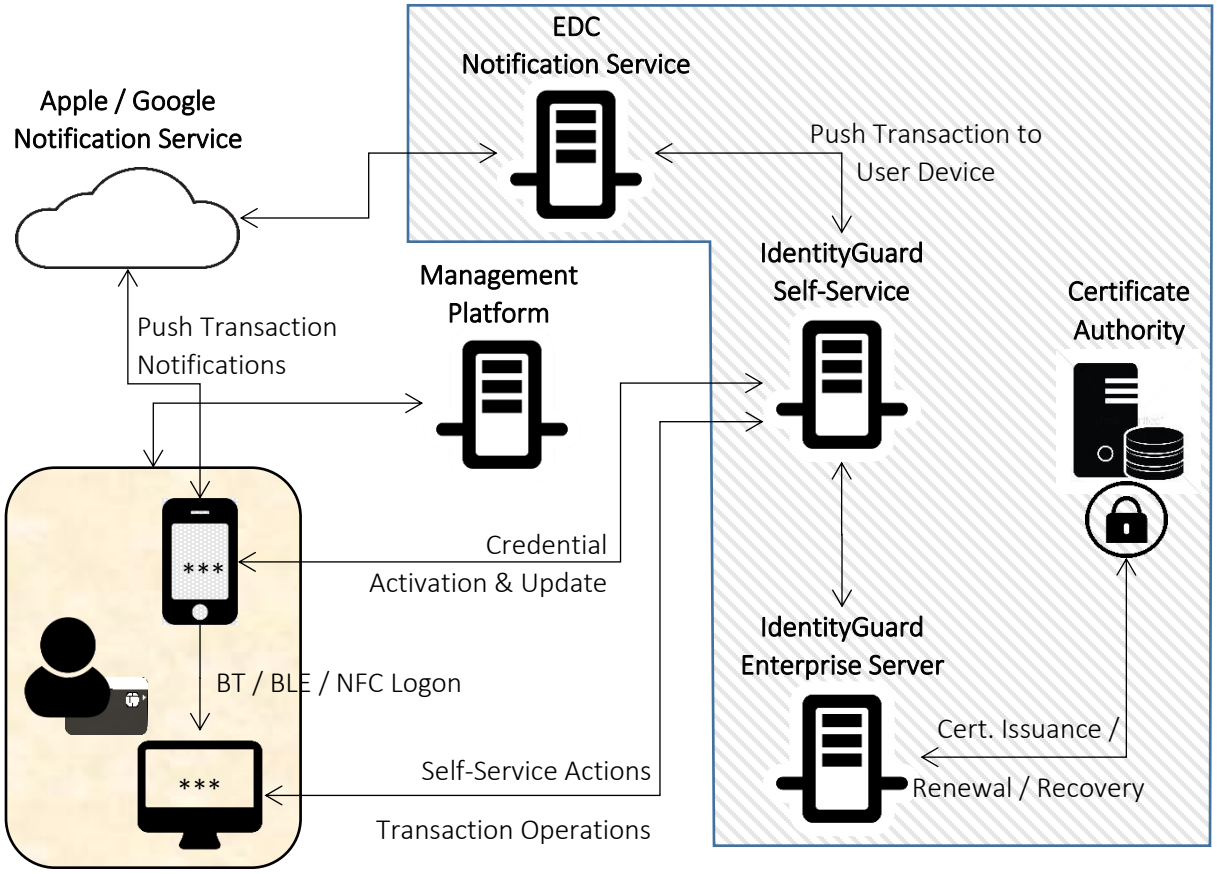
Entrust Datacard IdentityGuard has long offered support for PIV (NIST SP 800-73) in the form of physical cards. In 2012 IdentityGuard introduced a mobile version of the PIV card as part of our mobile smart credential offering, which enabled customers to create PIV smartcards on their mobile devices for authentication, signing, and encryption. In 2014 IdentityGuard introduced support for Derived PIV (NIST SP 800-157), known also as PIV-D, to the mobile smart credential solution. With the introduction of this support, government agencies have been able to issue mobile versions of their physical PIV cards to enable employees to authenticate themselves to systems, sign and encrypt data, all while remaining in compliance with the strict requirements of the standards.

As part of this offering, Entrust Datacard released a Software Development Kit (SDK) for mobile smart credential to allow partners and 3rd party integrators to leverage our PIV and PIV-D solutions for building their own PIV and PIV-D compliant applications and MDMs.

Entrust Datacard IdentityGuard Mobile Smart Credential Services Architecture

A full architecture for the Entrust Datacard IdentityGuard Smart Credential involves a number of Entrust Datacard components, as well as a number of external components. The architectural diagram below illustrates a complete deployment with all optional components included.

Figure 1 Entrust Datacard Smart Credential Architecture



* Components in the hashed region are provided by Entrust Datacard
** Components on the rounded rectangle represent the user and their devices
*** The mobile app is built using the IdentityGuard Mobile Smart Credential SDK. The desktop (Windows / MAC) has the appropriate Entrust Datacard Smart Credential Bluetooth Reader driver software installed

The IdentityGuard Enterprise Server and IdentityGuard Self-Service Module can be deployed in a number of HA configurations, as well as placed within a DMZ depending on deployment requirements. The Certificate Authority can be either the Entrust Authority Security Manager may be deployed on the customer premises, or provided by Entrust Datacard as a managed service. As well, US Federal customers may choose to leverage the Entrust Datacard Derived as a Service offering.

The VMware Workspace ONE platform deployment integration is described later in this document. The VMware PIV-D Manager application is loaded onto the user's mobile device and communicates with the VMware Workspace ONE management platform and the various Entrust Datacard IdentityGuard products in order to securely issue, maintain, use, and retire the various keys and certificates as required by the PIV and PIV-D standards.

Entrust Datacard IdentityGuard Mobile Smart Credential Services Capabilities

The Mobile Smart Credential solution offers a number of capabilities around such topics as:

- Mobile device support
- PIV and PIV-D container support
- Onboarding and maintenance of PIV and PIV-D credentials

This table identifies the features supported by the VMware Workspace ONE solution.

Note: Unless otherwise specified current support is for VMware PIV-D v1.0+ and Workspace ONE UEM Console v9.3+.

*Bluetooth login features require iOS PIV-D 1.4+ and Android PIV-D 1.3+.
**PDF signing with Workspace ONE PIV-D Manager requires iOS and Android v1.5+.

Function	Apple iOS	Google Android
Mobile OS Support	iOS 9+	6.0+ (7.0+ for Samsung KNOX)
PIV	√	√
PIV-D	√	√
Credential Update	√	√
Multiple Identities		
Certificate	√	√
Certificate Revocation	√	√
PIV Authentication	√	√
PIV Authentication + Signing	√	√
PIV Authentication + Signing + Encryption	√	√
PIV Encryption Key Recovery	√	√
Certificate export to Key Chain	√	√
QR Code	√	√
Secure E-mail	√	√
Secure website link	√	√
Android NFC login for MS Window		
Android Bluetooth login for MS Windows	√	√
Android Bluetooth LE login for MacOS	√	√
iOS Bluetooth LE login for MS Windows	√*	√*
iOS Bluetooth LE login for MacOS	√*	√*
Out of band authentication via push notification		
Authentication support for access to • VPN • WIFI • Cloud Applications	√	√
Third Party Application Integration	√	√
Native email encryption (s/mime)	√	√
Document digital signing	√**	√**
E-mail digital signing	√	√

Preparing Your Certificate Authority

The Entrust Datacard IdentityGuard smart credential services can be configured to communicate with either the Entrust Authority Security Manager CA, or Microsoft's CA. Please refer to your CA's documentation to determine how to administer it.

For the purposes of this integration, your organization must configure digital IDs which support the following types of key-pairs and certificate**.** The following bullets must be updated by the partner.

- 1 key-pair, ex. when you require PIV Authentication certificates
- 2 key-pair, ex. when you require PIV Authentication and Digital Signature certificate
- 3 key-pair, ex. when you require PIV Authentication, Digital Signature certificate, and PIV Key Management (encryption) certificates

Integration Guidelines

Overview

Introduction to VMware PIV-D Manager

VMware PIV-D Manager is a mobile application that integrates with various Derived Credential solution providers enabling the use of Derived Credentials with VMware Workspace ONE UEM.

Requirements for using VMware PIV-D Manager

Please provide all of the minimum Entrust Datacard products and product versions that are required by your solution.

Configuration

Configuring the VMware PIV-D Manager for iOS involves adding the PIV-D Manager as a public application, determining how end-users receive it, and configuring PIV-D settings for each vendor.

1. Navigate to **Apps & Books > Applications > Native > Public** and select **Add Application**.
2. Select the desired **Platform**.
3. Select **Search App Store** from the **Source** field to find the application.
4. Enter "VMware PIV-D Manager" as the keyword in the **Name** text box to find the application in the app store.
5. Select **Next** and use **Select** to pick the application from the app store result page. The **Edit Application** window displays.
6. Select **SDK Tab** and either select the default SDK Profile or a custom SDK Profile.
7. Select **Save & Assign** and then **Add Assignment**.
8. Assign the app to the correct smart groups and deploy the app.

Application Management

Administrators can use the VMware Workspace ONE Console to deploy, manage, and retire applications (including PIV-D) on enrolled mobile devices. In addition to this, security policies such as encryption, passcode, and DLP can be enforced to applications managed by VMware Workspace ONE.

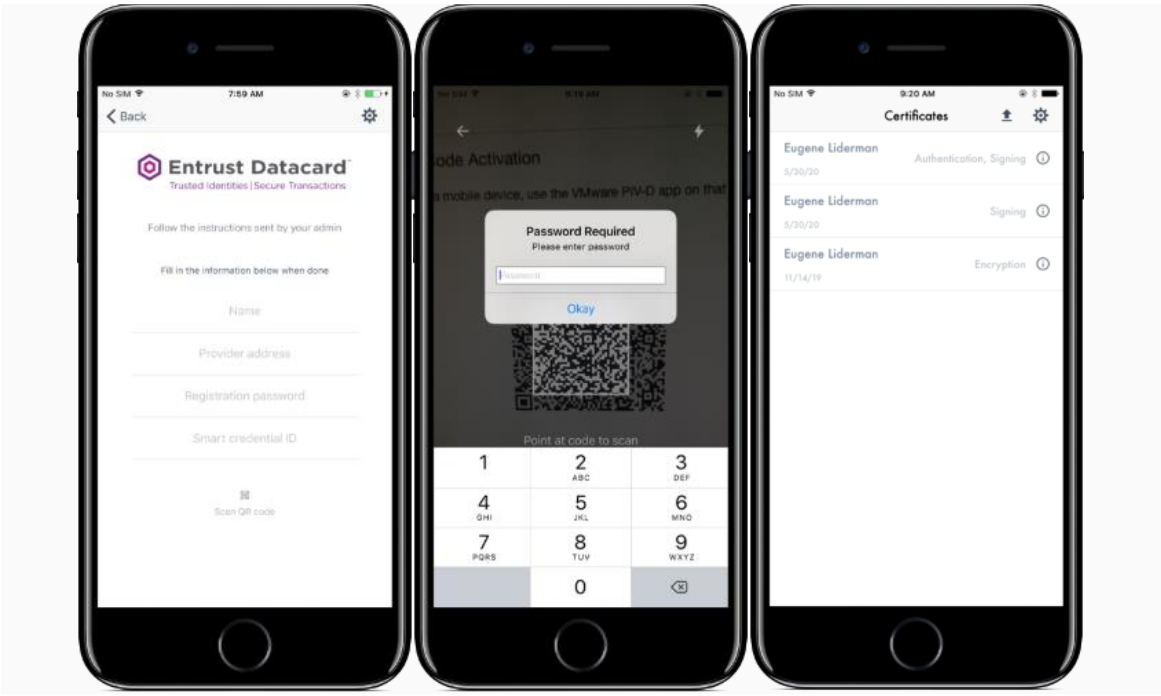
User Enrollment and Lifecycle Management

Enrolling Users in VMware PIV-D Manager

These steps assume the mobile device has already been enrolled in the Workspace ONE management either via the VMware Agent or Workspace ONE app.

To configure the VMware PIV-D Manager using Entrust IdentityGuard, complete the following:

1. Start the enrollment process by logging in to the Entrust IdentityGuard Self-Service Portal from your laptop/desktop computer with your existing smart card.
2. Once logged in, select on **" I'd like to enroll for a derived mobile smart credential"**.
3. Select **"I've successfully downloaded and installed the Entrust IdentityGuard Mobile Smart Credential application"** and click **Next**.
4. Enter a name under **Identity Name,** then select **VMware PIV-**D under the **Derived Mobile Smart Credential App** field.
5. Click **OK** A QR Code and a one-time password displays.
6. Launch the VMware PIV-D Application on your iOS Device and tap **Scan QR code** and then enter the one-time password.
7. Once the process is complete, you will be taken to the **Certificate** list view



Updating and Renewing Users in VMware PIV-D Manager

In the event a user needs to re-request derived credentials in PIV-D, click on the settings gear in the top right corner of the app and follow the instructions to re-fetch a new set of certificates. This will trigger the Entrust IdentityGuard Derived Credential Enrollment process again.

Reporting Lost or Compromised Identities in VMware PIV-D Manager

If the device is lost or compromised, the administrator will have the ability to perform an enterprise wipe on the device via the Workspace ONE UEM Console. This can be done by navigating to the device details view, finding the affected device, and then triggering the enterprise wipe option.

Alternatively, if the Workspace ONE Self Service Portal is enabled, the end user can log in to SSP to enterprise wipe their own device.

Encryption Key History Escrow and Recovery in VMware PIV-D Manager

If an app level passcode is enabled in VMware PIV-D manager, the key encrypting key used by PIV-D will be escrowed to the Workspace UEM Console during passcode creation. A user can utilize the forgot passcode workflow to retrieve the escrowed key encrypting key. To perform the forgot passcode workflow, the user will need to press the forgot passcode option on the passcode entry page, and then re-authenticate with the mode configured by the administrator. (Token, SAML, or Username / Password).

External Documentation

https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/services/WS1-PivD-Manager/GUID-AWT-PIVDINTRODUCTION.htmlhttps://docs.vmware.com/en/VMware-Workspace-ONE-UEM/services/WS1-PivD-Manager/GUID-AWT-CONFIGUREENTRUST.html