Entrust IdentityGuard Mobile Smart Credential 3.2 with Blackberry UEM 12.9

PIV-D Technical Integration Guide

Document issue: 1.0
Date of Issue: July 2018

Contents

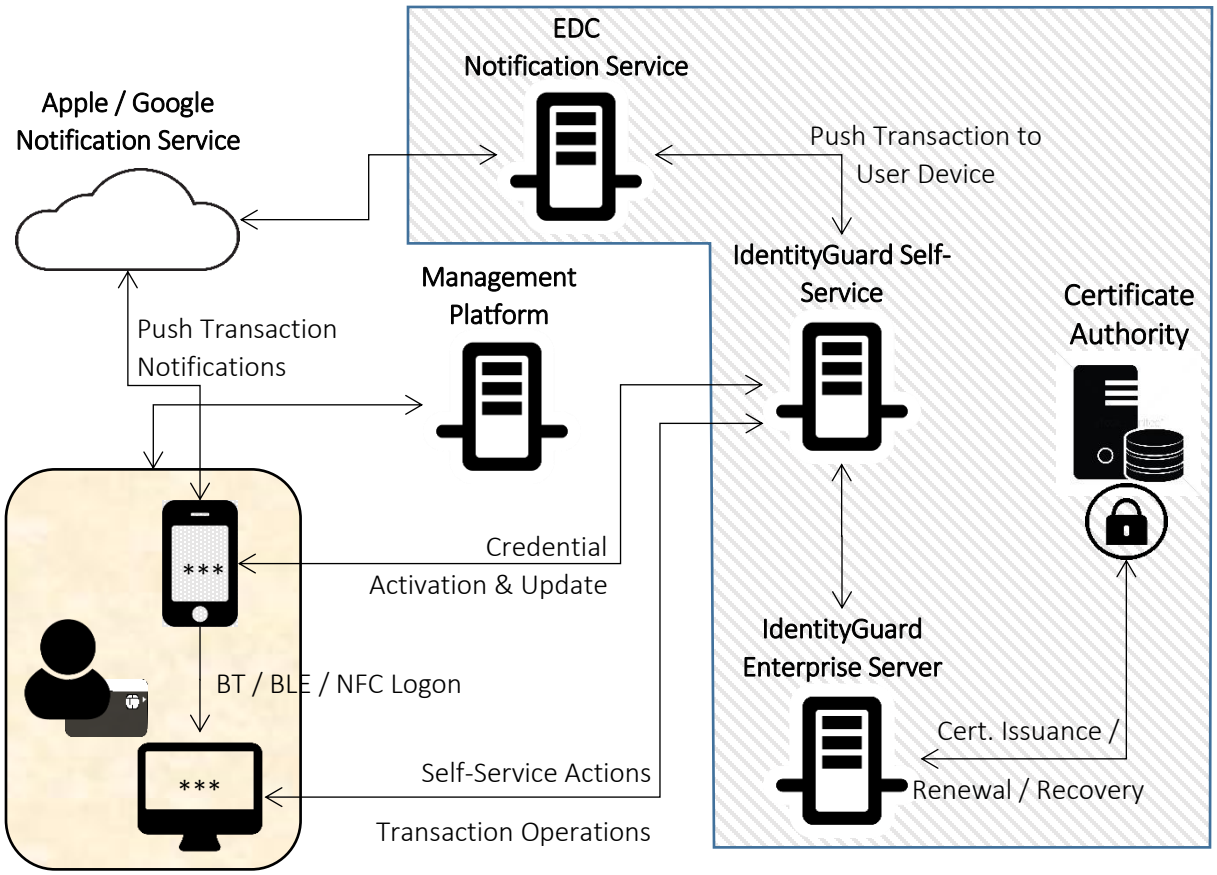
Introduction to Entrust Datacard IdentityGuard Smart Credential Services

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 BlackBerry UEM Server platform deployment is integration is described later in this document. The BlackBerry UEM Client application is loaded onto the user's device and communicates with the BlackBerry UEM Server 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
- Smartcard logon to Microsoft Windows and Apple Mac desktops

This table identifies the features supported by the BlackBerry UEM Server solution.

Mobile OS Support	
Apple iOS	9, 10, 11
Google Android	4.4, 5, 6, 7, 8
PIV	
PIV	√
PIV-D	√
Credential Update	√
Multiple Identities	√
Export to Key Chain – Supported for Android, not for IOS	√
Onboarding – Activation and Update	
QR Code	√
Smartcard Logon :	
To support a "Virtual Smart Card" using your mobile device, install a driver in the PC/Mac and that lets the Mobile device be seen as a Physical SC. If supporting, prioritize Windows BT and Mac BLE. Interaction is between the Device and the PC.	
Windows BT	
Windows NFC	
Apple Mac BLE	
PIV / PIV-D Container Support	
PIV Authentication	√
PIV Authentication + Signing	√
PIV Authentication + Signing + Encryption	√

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**.** BlackBerry UEM Server can support these combinations.

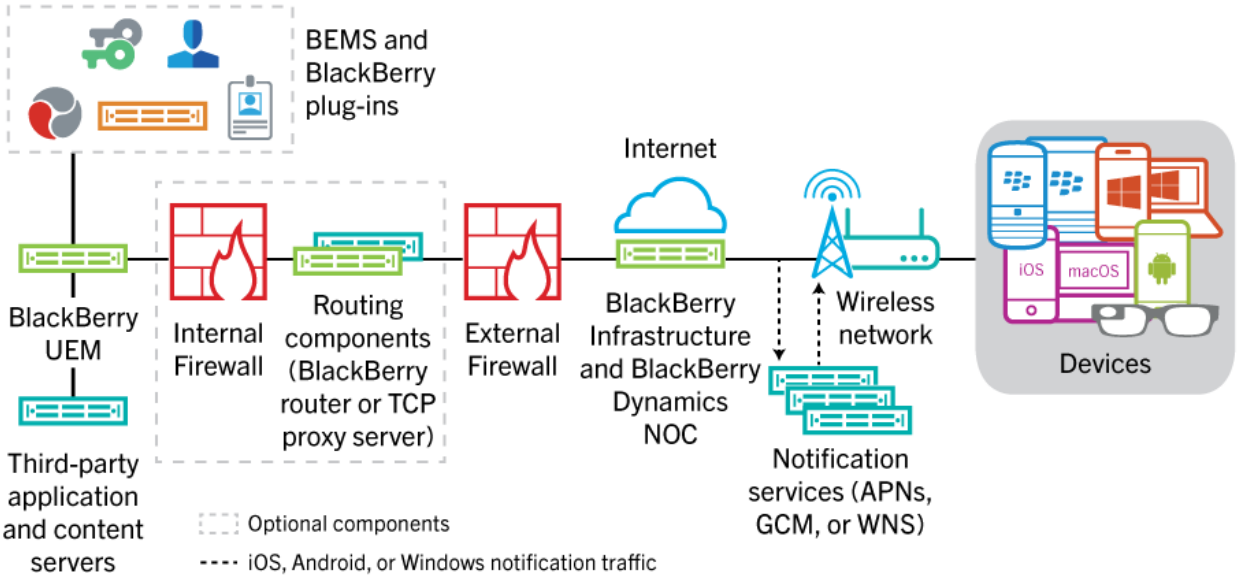
- 1 key-pair, ex. when you require PIV Authentication certificates
- 2 key-pair, ex. when you require PIV Authentication and Digital Signature certificate
- 3 key-pair, ex. when you require PIV Authentication, Digital Signature certificate, and PIV Key Management (encryption) certificates

Integration Guidelines

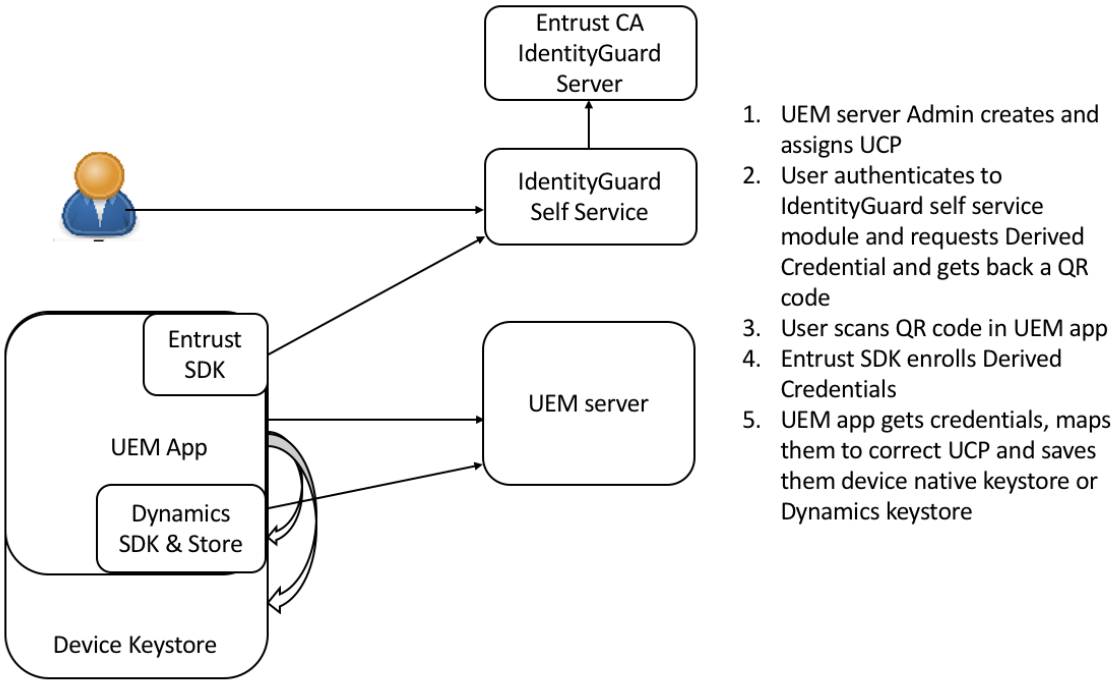
Overview

Introduction to BlackBerry UEM

1. High level overview of BlackBerry UEM: http://help.blackberry.com/en/blackberry-uem/12.9/overview-and-whats-new/what_is_BlackBerry_UEM.html
2. High level architecture diagram. For more detailed Architecture information, please refer to the documentation here: http://help.blackberry.com/en/blackberry-uem/12.9/architecture/ake1452094272560.html



3. High level diagram of Entrust Smart Credentials in BlackBerry UEM



Requirements for using BlackBerry UEM

The BlackBerry UEM Derived Credentials solution has been validated against with Entrust IdentityGuard 12.0.

Configuration

To use the Entrust Derived Credentials feature in BlackBerry UEM Server, the customer needs the following:

1. BlackBerry UEM Server UEM 12.9 or higher server.
2. Entrust IdentityGuard 12.0 configured with SmartCredentials.
    a. Entrust Self-Service Module needs to be configured with QR code.
    b. Entrust Self-Service Module needs to accessible outside the enterprise firewall.

Application Management

The only mobile side app needed for Entrust PIV/PIV-D integration is the BlackBerry UEM Client app, that is already present on UEM activated devices. For more information on BlackBerry UEM Server App Management, please refer to the documentation here: http://help.blackberry.com/en/blackberry-uem/12.9/administration/managing-apps.html

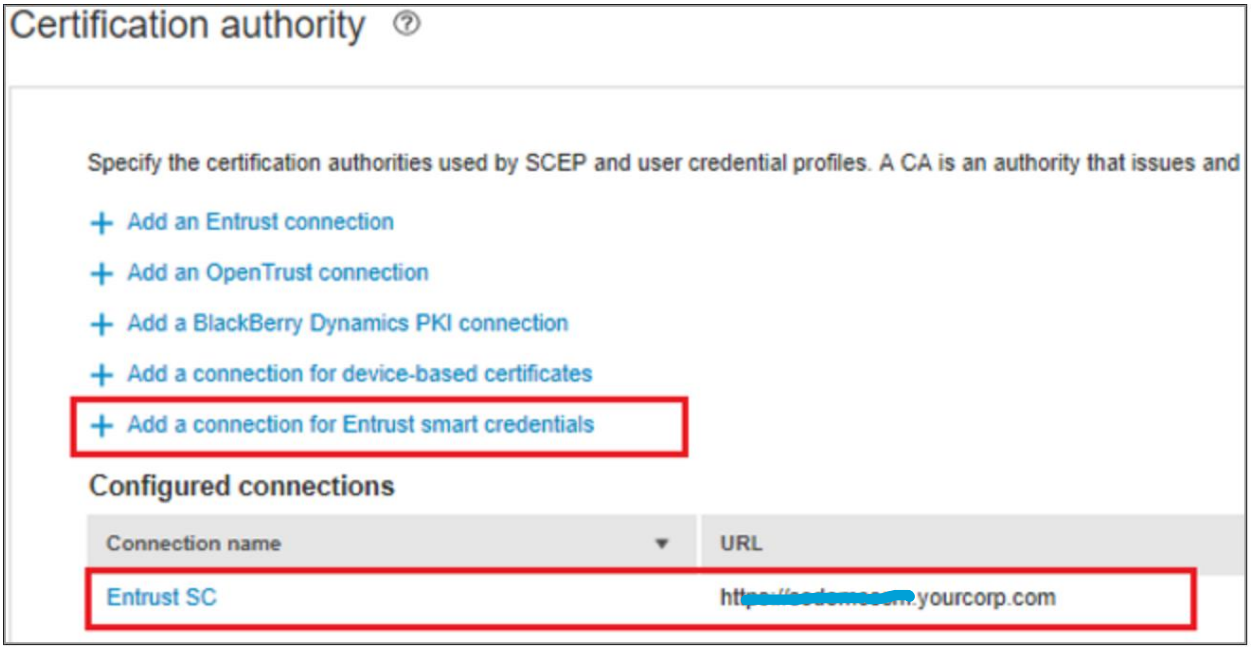
User Enrollment and Lifecycle Management

Enrolling Users in BlackBerry UEM

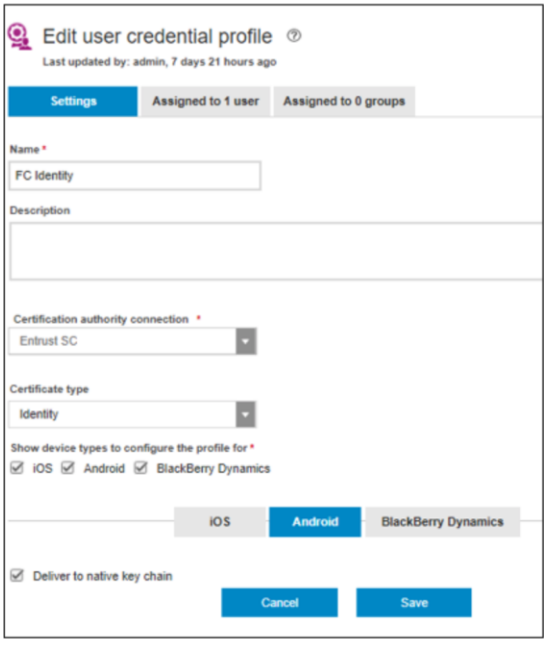
1. To use the Derived Credentials feature, end users need to activate their devices against the BlackBerry UEM Server.
2. To use Entrust Derived Credentials on a device activated against the BlackBerry UEM Server, the Admin and the End User need to do a set of actions.

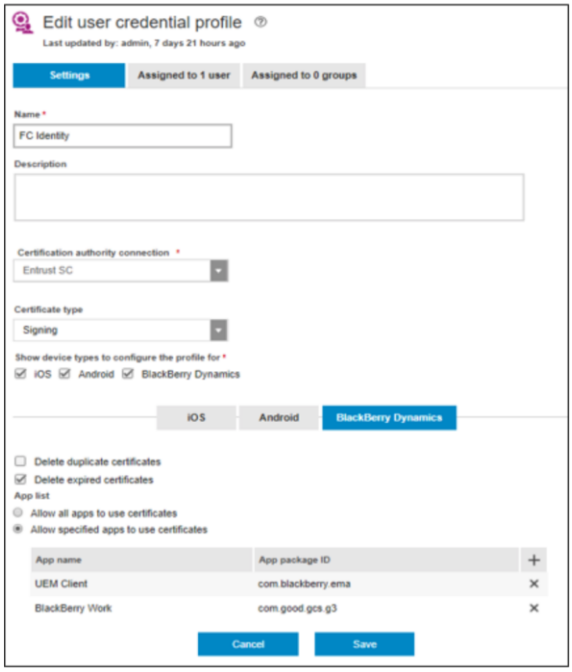
Admin Actions:

1. Connect BlackBerry UEM Server to your organization's Entrust IdentityGuard server to use Entrust smart credentials. Detailed steps here: http://help.blackberry.com/en/blackberry-uem/12.9/administration/olz1527687948568.html



2. Create a user credential profile to use Entrust smart credentials on devices. Detailed steps here: http://help.blackberry.com/en/blackberry-uem/12.9/administration/vum1527699046234.html



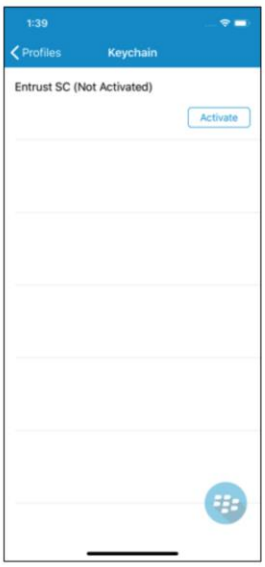


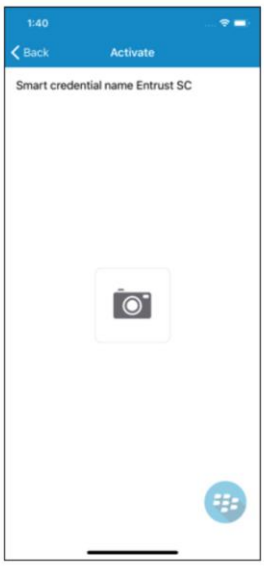
3. Assign the user credential profile to user accounts and user groups.

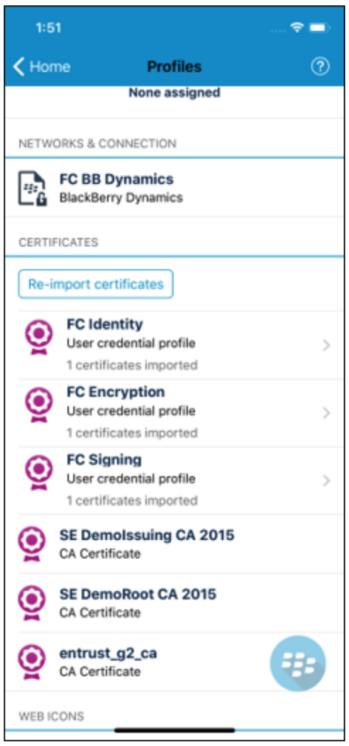
End User actions:

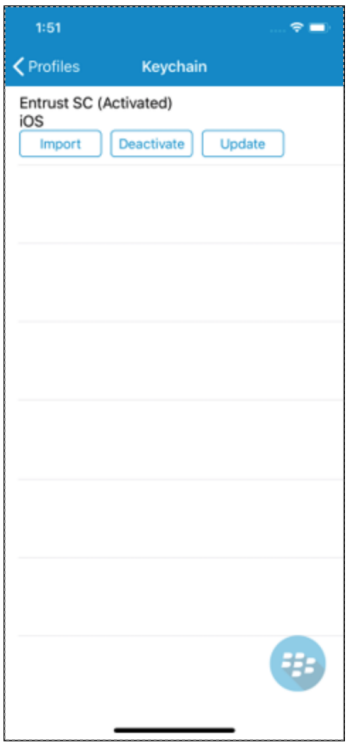
1. After a device receives the profile, users must log in to the Entrust IdentityGuard Self-Service Module to activate their smart credential.
2. The users them use the BlackBerry UEM Client to scan the QR code presented by the Entrust IdentityGuard Self-Service Module to add the smart credential to the device.

iOS

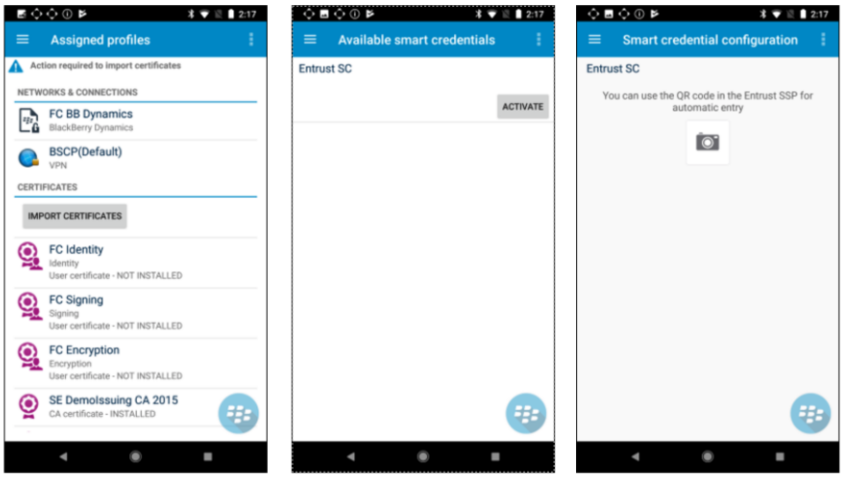


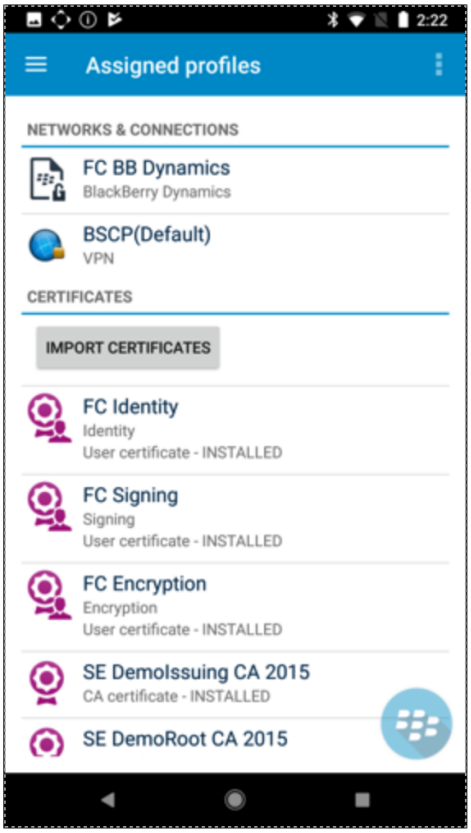


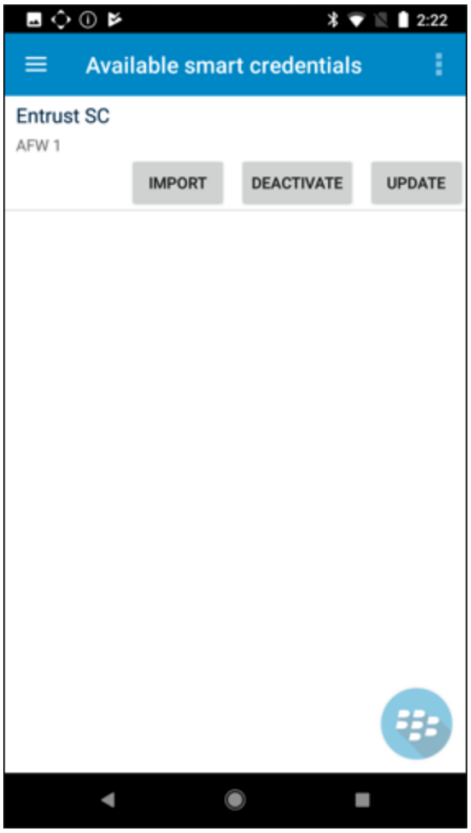




Android







3. The device will now have the Entrust Derived Credentials delivered to the certificate store in the Dynamics SDK (on iOS and Android) and to the native key chain (on Android).

Updating and Renewing Users in BlackBerry UEM Server

1. Users can update/renew their credentials when credentials have expired or compromised or they have otherwise been invalidated by the Admin on the Entrust server or the user has been instructed to get fresh credentials or wants to get a new credential for any reason.
2. To update their credentials, the user needs to use the Entrust Self-Service Module to generate a new QR code for an existing Smart Credential.
3. They then go to the BlackBerry UEM Client, select Import Certificates and get a screen that allows them to click on “Update” to read in the QR code from the Entrust Self-Service Module and update the Smart Credential on the device.
4. The updated Smart Credential is automatically pushed to the Apps/consumers on the device by the BlackBerry UEM Client.
5. In case the automatic push is not successful (user will get an error indicating that), clicking on the “Import” button does the same action. Screenshots of iOS and Android devices below. The Import process launches the same UI as a new smart credential activation process in the BlackBerry UEM Client UI.

Reporting Lost or Compromised Identities in BlackBerry UEM Server

The BlackBerry UEM Server does not participate in this process, the Admin would need to go the Entrust server to invalidate the lost/compromised identities or the End User can do that same using the Entrust Self-Service Module.

Encryption Key History Escrow and Recovery in BlackBerry UEM Server

1. Any BlackBerry or ISV app built using the BlackBerry Dynamics SDK (like BlackBerry Work) has the ability to store expired keys, including Encryption keys. This is controlled by the Admin using a setting in the user credential profile. The expired keys, in this case, are keys that were valid when they were retrieved from Entrust into the Dynamics SDK key store but have since expired.
2. BlackBerry UEM Server does not support the retrieval of already expired keys from Entrust.

External Documentation

1. Connect BlackBerry UEM to your organization's Entrust IdentityGuard server to use smart credentials: http://help.blackberry.com/en/blackberry-uem/12.9/administration/olz1527687948568.html
2. Create a user credential profile to use Entrust smart credentials on devices : http://help.blackberry.com/en/blackberry-uem/12.9/administration/vum1527699046234.html