White Paper

Author:

Nipun Dev

User Identity Certificate & Configuration Data Provisioning in SUP 2.1.3

(with Afaria Integration)

May 2012

Table of Contents

Overview

This document describes a cross-platform means for client application code to retrieve provisioning information and dynamically generated certificates from an Afaria server. This allows the distribution of provisioning data and certificates to the device without the manual user entry of data or without the manual file transfers that might otherwise be required to achieve the same end.

Certificate Request to CA is a SCEP based request for a new generated certificate using the user & the challenge password. The request is made by the Afaria client thru server on behalf of the application. On a similar note, applications can also receive provisioned settings from Afaria server. Initial Application settings can be installed on the SUP client using Afaria. From 2.1.1, online applications would be able to directly consume additional custom settings set using Afaria server.

SUP 2.1.3 Documentation Link:
http://infocenter.sybase.com/help/index.jsp?topic=/com.sybase.infocenter.pubs.docset-SUP-2.1.2/doc/html/title.html

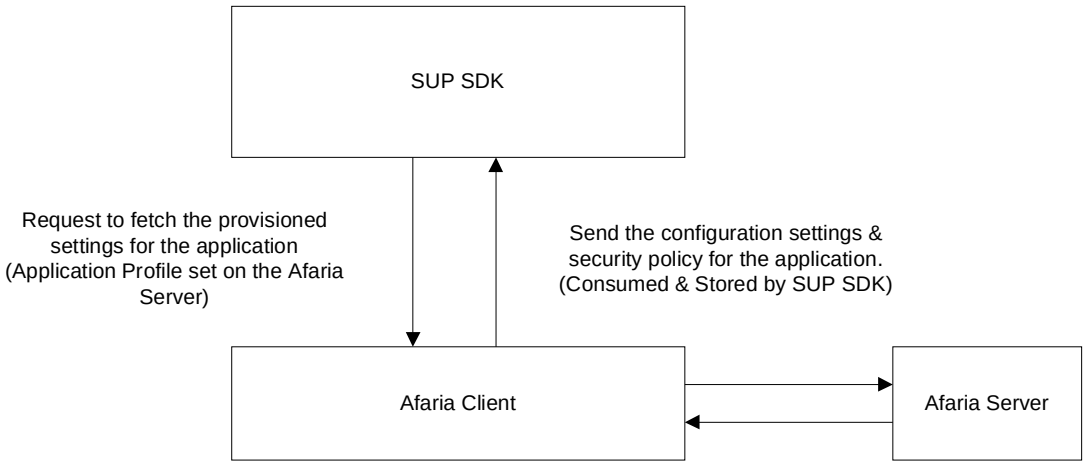
The document also describes recommendation for applications to provision certificates using SUP OData SDK WITHOUT Afaria Integration. These options use other capabilities of device platform and SUP SDK to provide the certificate to applications.

Also at the end have outlined a small section on sharing of certificates between applications.

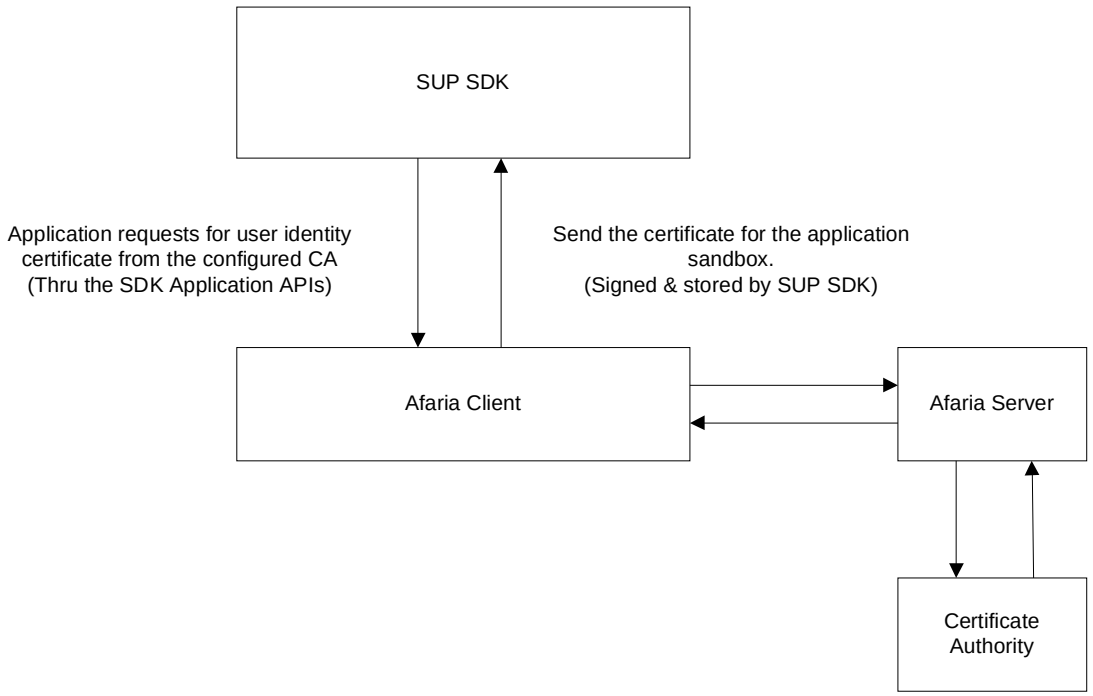
Component Interaction (Afaria based Provisioning)

PROVISIONING

Configuration settings



Certificate Provisioning



IT Enablement

The following are the Enterprise IT responsibilities:-

- Enterprise IT provides a secure channel to distribute the challenge code for procurement of certificate from CA after validating user identity.
- Challenge code issued is not re-usable and/or expires.
- Certificate Authority (CA) is configured to support SCEP policy.
- The SCEP request will always result in a different certificate being generated and returned.
- Registration Authority must be introduced to verify user certificate requests to the CA.
- Afaria is a requirement for the applications that need to dynamically generate certificates on client requests.

Administrative Tasks

The administrative tasks on the Afaria server for provisioning data and certificates are documented & details on this are available at the SUP 2.1.3 Guides.
More details on this can be seen with SUP 2.1 documentation at this location:

http://infocenter.sybase.com/help/topic/com.sybase.infocenter.dc01205.0212/doc/pdf/sup_system_administration.pdf

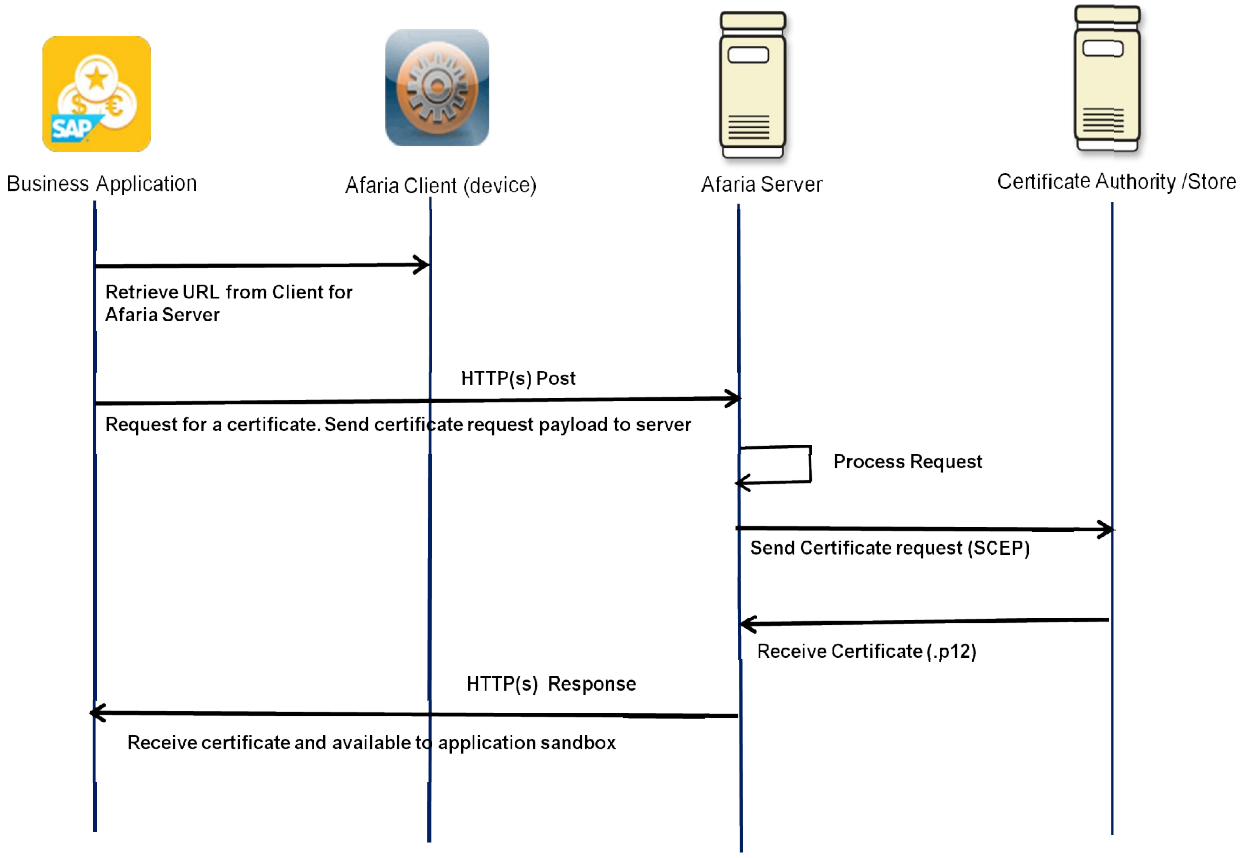
Configuration Data Provisioning with Afaria

Afaria can be used to provision the initial settings to the application. SDK provides APIs to install the client specific settings on the client like host, port, farm Id, SUP Public key etc. Apart from that Admin can provide additional custom settings which can be read by application as a collection <key, value> from 2.1.1 release onwards.

Application can also deploy custom settings using Afaria. SUP SDK provides API

Developer reference for settings provisioning can be found at the SDK developer guide:
http://infocenter.sybase.com/help/topic/com.sybase.infocenter.dc01708.0212/doc/pdf/sup_devguide_odata_sdk.pdf

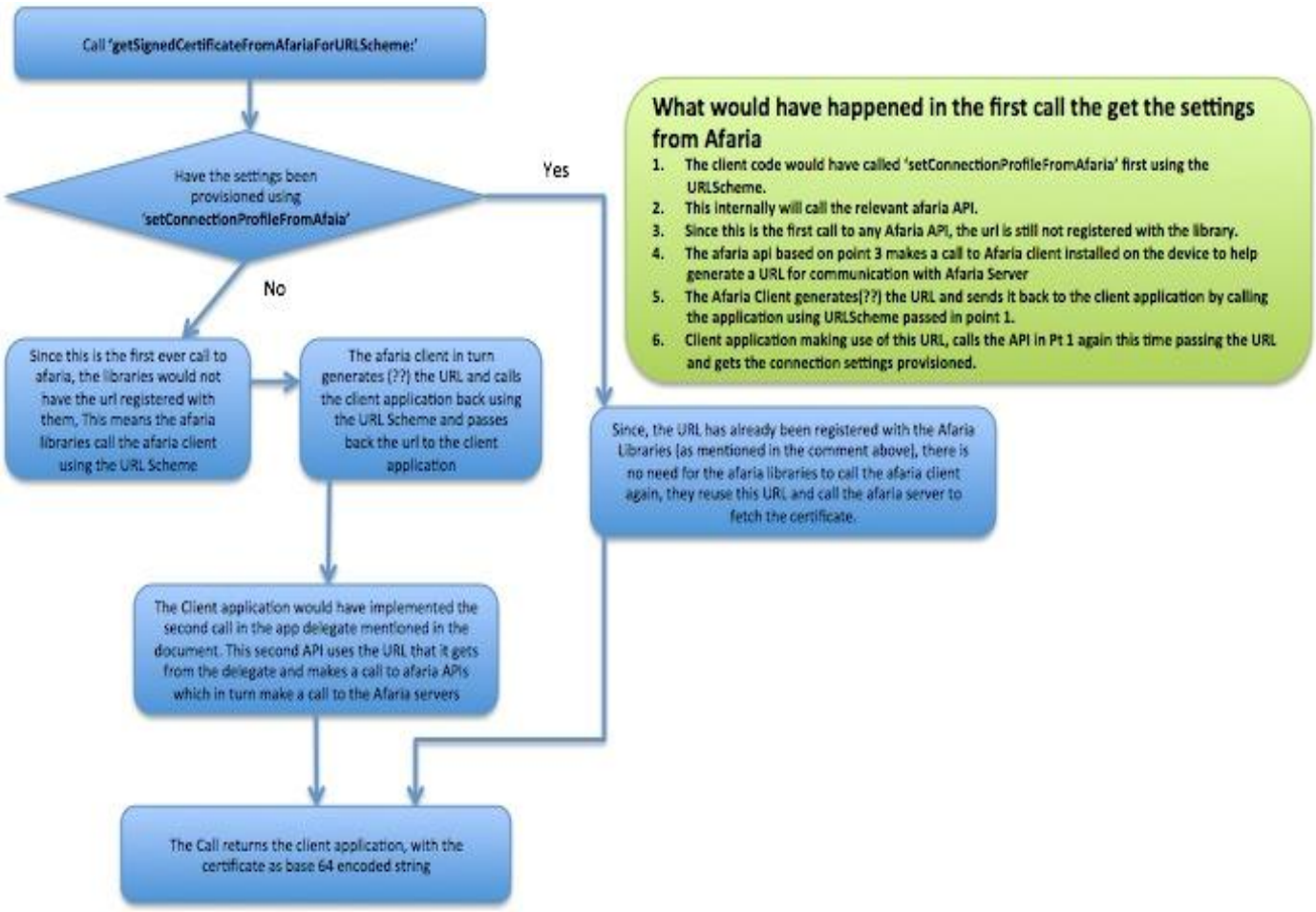
Provision dynamically created certificates with Afaria



In such scenario, a unique certificate is generated on behalf of the application at the server. This would require the Afaria client to send a request to Afaria server on which the server using the SCEP protocol would contact the CA to have a certificate generated.

Developer reference for certificate provisioning on all platforms can be found at the SDK developer guide:
http://infocenter.sybase.com/help/topic/com.sybase.infocenter.dc01708.0212/doc/pdf/sup_devguide_odata_sdk.pdf

IOS Application Flow



Similar approach is followed on Blackberry & Android without the application context switch.

Limitation with Afaria based certificate provisioning

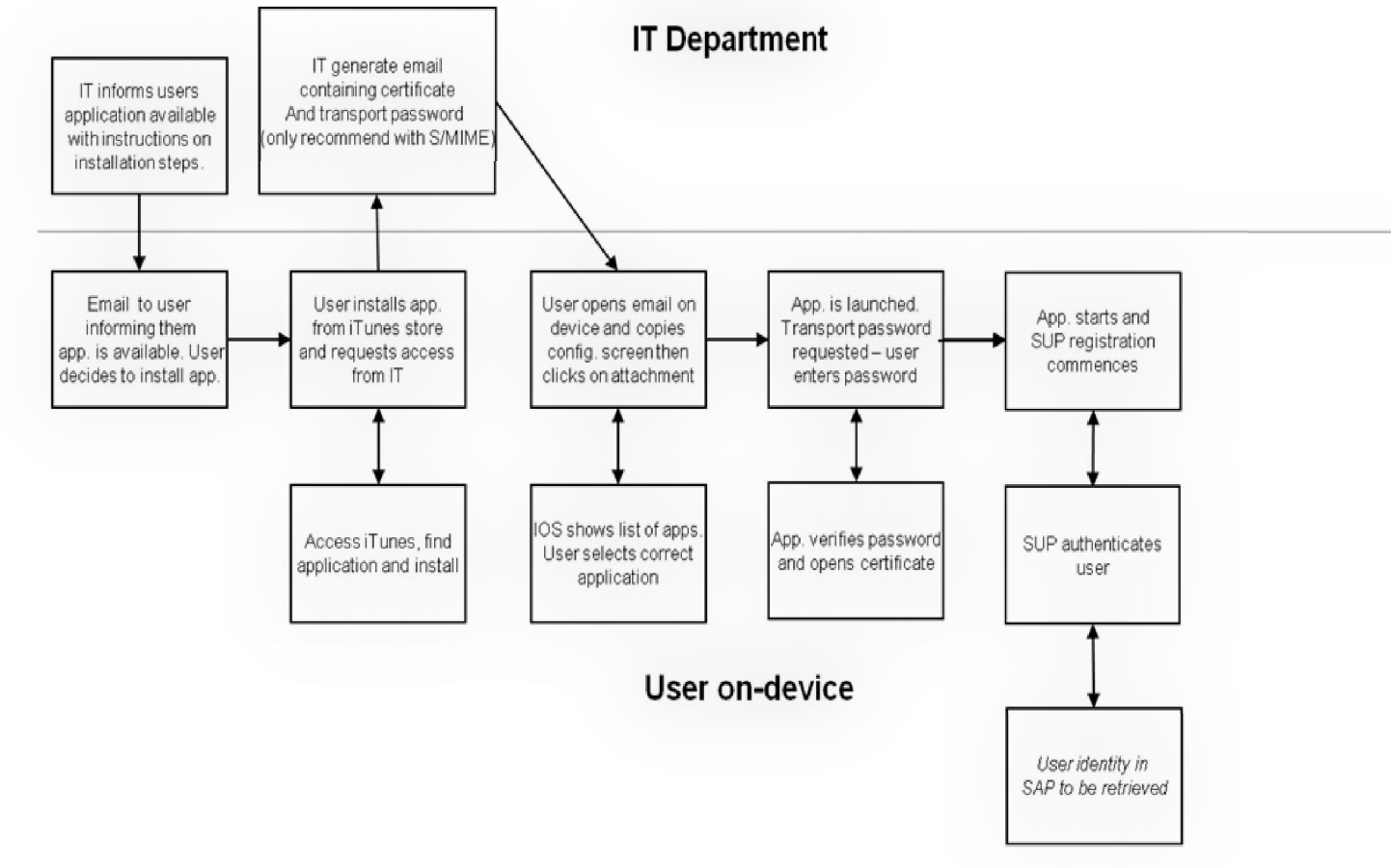
- The application developer must ensure that the common name passed into the function is verified, Afaria makes no attempt to verify the identity of the certificate requestor.

Provision pre-created Certificates without Afaria

There are situations where there is no need of dynamic certificate generation from the CA. There are pre-existing X509 certificates already issued by Enterprise IT. In such cases of single sign on there needs to be logic to determine that the certificate has already been deployed to the device and added to a common key chain that several application have access.

The following approaches are recommended possibilities for each of the platforms. SUP SDK APIs provide additional support to access the certificates from different ways apart from Afaria. For example for IOS the approach suggested relies on a custom SAP SSO application to provision the certificate on a shared key chain for IOS.

IOS



As an example on the above flow:

- On IOS, for installing/provisioning Pre-created Identity SSO certificates (without Afaria), you need to additionally make use of a custom SAP SSO Application (an example as developed by SAP IT - internal) installed on the device.
  Note: SAP Global IT would NOT ship this application as SAP Standard Application. This custom development has to be managed by the Mobile Application Development.

- The encrypted certificate is exported to a computer or WTS and then sent to the user's email address. The details on how to accomplish this is mentioned at this link:
  https://wiki.wdf.sap.corp/wiki/display/applemobile/Single+Sign-On#SingleSign-On-InstallingYourPersonalSSOIdentityCertificate

- On the device the certificate is unencrypted and installed on SUP Data Vault or the device key store securely. This is the responsibility of the SAP SSO Application; details of which can be seen at this location.
  https://community.wdf.sap.corp/sbs/thread/17299

- All SUP ODP Business applications which need to fetch this certificate need to be part of entitlement access group of the SAP SSO application.

- Using existing set of SUP SDK 2.1.3 APIs, one can consume these shared certificates from Data vault or key chain of SAP SSO Application in the end user business application.

- Post that the registration process is same as already outlined by SUP SDK with the X509 certificates.

Blackberry

- Import the certificate to the Blackberry Key Store

  1. Mount the directory on your system which has the certificate as the SD card.
  2. Open the certificate, enter the password when prompted.
  3. Go to menu, Import the certificate into key store.
  4. The certificate can also be synched thru the BB Desktop Manager.
  5. To be sure that the certificate is put to the key store,
  6. Go to menu->Applications->Files->My Files->Media Card.
  7. This will list all the files and also the keys and certificates in the key store

- Use SUP SDK 2.1 API s to fetch the certificate from store into the application.
- In case there are multiple certificates, there is a UI shown asking to select the relevant certificate.

- Post that the registration process is same as already outlined by SUP 2.1.3 with the X509 certificates.

Android

On Android, it's the simplest. The certificate can be read from any file share on the device using SUP 2.1.3 SDK APIs.

Sharing of certificates

Applications on a device can share certificates as and if allowed by the enterprise security of the organization.

SUP Data Vault can be shared across applications and thus possibly used to store and share certificates. The first application that requests for certificate shall create a standard shared vault and store the certificate. Any new applications installed can open the data vault and re-use the certificates. All application need to know the data vault ID and password. Standard usage policies of Data Vault apply here.

IOS

Another way if allowed by security policy is storing in the key chain by the first application. All applications which are part of the entitlement access group with this application can share this certificate from key chain as well.

Blackberry

Install & share the certificates thru Blackberry key store.

Android

Install & share the certificates thru the device security certificates store.

Special Note:

- Sharing of certificates is not advisable for highly critical applications.
- Only allow sharing of certificate between applications on a specific device.
- Govern grouping of apps sharing certificates