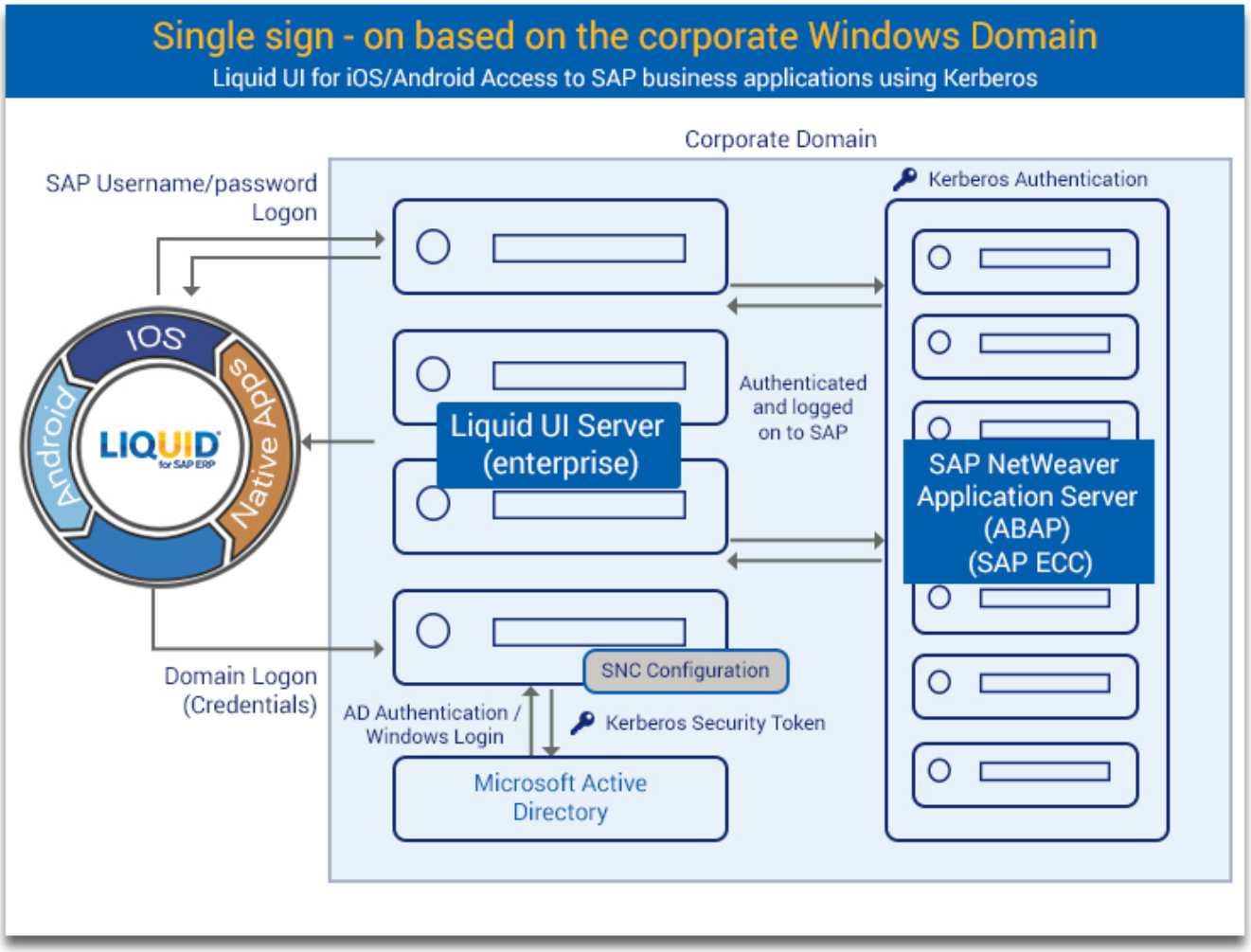
Android Introduction
2.3.07 Single Sign-On

Purpose

In a default SAP setup, organizations use different usernames and passwords to log into SAP systems. Companies have standardized this using the Windows Active Directory with Kerberos. The Single Sign-On feature simplifies this process and is quite easy to set up on SAP GUI.

Single Sign-on is an authentication process that enables users to access multiple apps with a single set of login credentials. Liquid UI supports Single Sign-On (SSO) for user authentication on Android. It eliminates the need for IT for managing thousands of usernames and passwords. With the Single Sign-On feature, Liquid UI users can enter a domain username and password to log into SAP. Users will now have to remember a single set of login credentials to gain access to SAP.

Architecture



Mechanism

- Enter Domain credentials on Liquid UI for Android native SAP logon screen.
- The credentials are transmitted to the Liquid UI Server and then to Microsoft Active Directory.
- The Active Directory upon receiving the request sends the Kerberos token to the Liquid UI Server.
- Liquid UI Server forwards the Kerberos token to the SAP Application Server (ABAP).

Using the Single Sign-On feature, users can log into SAP ERP systems through one of the four methods listed below.

1. **Domain credentials**

   Configurations:

   - Valid Windows Domain Login Credentials
   - Kerberos Configuration on SAP ECC (Transaction: RZ10)
   - Liquid UI Server v3.5.549.0 and later
     - The Liquid UI Server should be on the same domain
     - Kerberos DLL is distributed as part of the Liquid UI Server installation. Older Version: Make sure that you have Kerberos library (32bit:gsskrb5.dll, 64bit:gx64krb5.dll) files under the LiquidUIServer (or GuXTWSServer) folder.
   - Configure Liquid UI Server with sapproxy.ini file
   - Configure Secure Network Communication in SAP GUI (if it doesn't exist)
   - Login to Liquid UI for Android using Windows Domain Credentials

2. **Portal**

   Configurations:

   - Configure Liquid UI Server with sapproxy.ini file

3. **Key-certificate pair**

   Configurations:

   - Valid Windows Domain Login Credentials
   - Liquid UI Server v3.5.561.0 and later
     - The Liquid UI Server should be on the same domain
   - Obtaining Certificate
   - Import the certificate into Liquid UI Server and SAP System
   - Import the key-certificate pair into SAP Server
   - Import Synssl.dll, version 2.0.0.0 and later
   - Configure Liquid UI Server with sapproxy.ini file
   - Login to Liquid UI for Android using Windows Domain Credentials

4. **Key-certificate pair with Cyber safe**

   Configurations:

- Valid Windows Domain Login Credentials
- Liquid UI Server v3.5.584.0 and above
    - The Liquid UI Server should be on the same domain
- Generating certificate using openssl.exe
- Import the certificate into Liquid UI Server and SAP System
- Import the key-certificate pair into SAP Server
- Install Cyber Safe on Liquid UI Server, and configure.
- Configure Liquid UI Server with sapproxy.ini file
- Check SSO running successfully
- Login to Liquid UI for iOS using Windows Domain Credentials

The user can create a domain name on the “Secure Network Communications” (SNC) and use this domain name for multiple logins. Liquid UI server authenticates users through Windows Active Directory for our Liquid UI for Android. The users will now have to remember a single set of logins(username and password) to manage the database.

Each method has different configurations with the Liquid UI Server. Refer to the Single Sign-On Configuration article to learn more in detail.

Also, Liquid UI Server supports advanced features such as two-factor authentication along with interchangeable support for Kerberos, key-certificate pairs, etc. to fulfill the most complex customer requirements of SAP ERP.

Unique solution ID: #1987
Author: Sarvani Kusuri
Last update: 2022-09-14 07:02