Hypori User Guide

Common Criteria Configuration and Operation

Version 4.2.0

Acknowledgments

Hypori uses open source and copyrighted third-party software as part of its Virtual Mobile Infrastructure product. Copyright information, licensing agreements, and general acknowledgments for third-party software usage are listed in separate documents, which are available on request. Contact your Hypori representative for more information.

Contents

1 Introduction and System Overview

Welcome to the *Hypori User Guide – Common Criteria Configuration and Operation*. This section describes the Hypori virtual mobile device experience for users who connect to a Hypori Virtual Device through the Hypori Client. It also provides a brief overview of the Hypori system.

The Hypori platform hosts virtualized devices in the cloud, providing access to these devices through the Client app on your mobile device. The following diagram shows how these Hypori components interact.

The Hypori Virtual Device runs your apps on a secure server.

The Hypori Virtual Device and the Client communicate through secure encrypted protocols.

The Client connects you to your apps running on the secure server.

1.1 Hypori VMI System Overview

The Hypori system is a Virtual Mobile Infrastructure (VMI) platform. Users running the Hypori Client on their mobile devices access Hypori Virtual Devices, which are virtual Android devices running on a server in the cloud. The Virtual Device contains the operating system, data, and applications, and it uses TLS 1.2 encryption to communicate securely with the Hypori Client.

The Hypori VMI platform includes the following components:
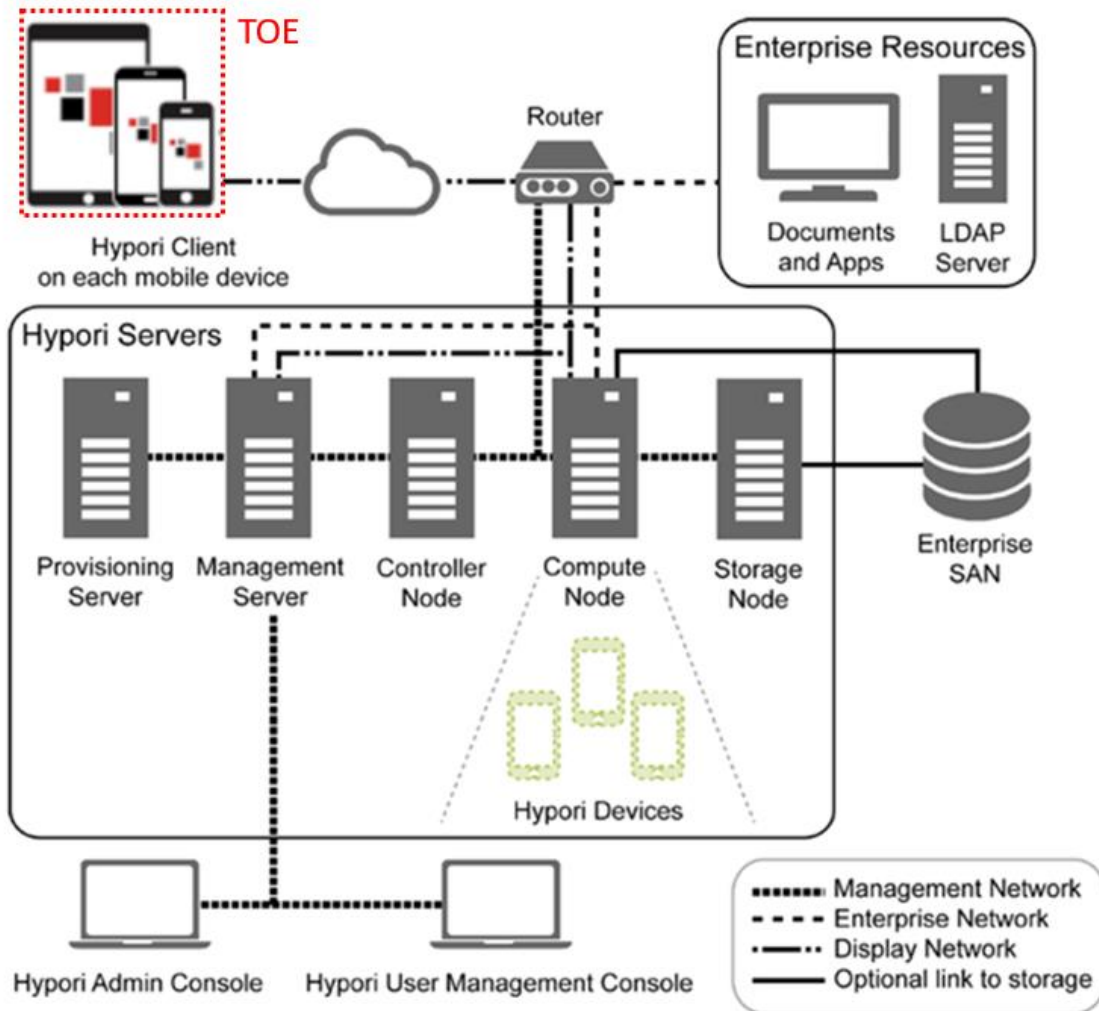
The Hypori system includes:

- **Hypori Client:** A thin client that installs on the user's mobile device and communicates with the Virtual Device on the server through secure encrypted protocols.
- **Hypori Device:** An Android-based virtualized version of the user's mobile device.
- **Hypori Servers:** The cloud server cluster that hosts the Hypori Virtual Devices.
- **Hypori Admin Portal:** A web app used to manage the Hypori system.
- **Hypori User Management Console:** A web app used to manage users within a domain.

2 Common Criteria Evaluation

Hypori has evaluated the security features of the Hypori Client version 4.2.0 under the Common Criteria Evaluation and Validation Scheme (CCEVS). The evaluation demonstrates that the Hypori Client conforms to the security requirements specified in *Protection Profile for Application Software* when installed and operated in accordance with the *Hypori Virtual Mobile Infrastructure Platform 4.2.0 Hypori Client (Android) Security Target*, the *Hypori Virtual Mobile Infrastructure Platform 4.2.0 Hypori Client (iOS) Security Target and the Hypori Virtual Mobile Infrastructure Platform 4.2.0 Client (Windows) Security Target*. CCEVS has posted the results of the evaluation to the National Information Assurance Partnership (NIAP) Product Compliant List (https://www.niap-ccevs.org/CCEVS_Products/pcl.cfm). The posting includes the validation certificate, CCEVS Validation Report, Security Target, and applicable guidance. Note that the functionality described in this guidance documentation is limited to the security functionality described in the Security Target. Other product functionality is not applicable to the claimed Protection Profile and was therefore not examined as part of the Common Criteria evaluation of the Hypori Client product.

The evaluated configuration also includes several assumptions and requirements that must be met by the intended environment in order for the installed Hypori Client 4.2.0 to be in the evaluated configuration. These are as follows:

- The TOE relies upon a trustworthy computing platform for its execution. This includes the underlying operating system and any discrete execution environment provided to the TOE.
- The user of the application software is not willfully negligent or hostile, and uses the software within compliance of the applied enterprise security policy.
- The administrator of the application software is not careless, willfully negligent or hostile, and administers the software within compliance of the applied enterprise security policy.

3 Guidance Documentation

The Hypori Client Guidance Documentation applies in the evaluated configuration along with this Common Criteria specific guidance. The general guidance covers Android 8.1, 9, and 10, and on iOS version 12 and iOS 13 (with the exception of iOS 13.1, due to known incompatibility), and on Windows 10 v1809 and v1903 operating systems. There is no version-specific configuration. Cipher suites are determined by choice of Android, iOS, or Windows version, not the Hypori Client configuration.

Information about Hypori and the Hypori product and its components can be found at http://www.hypori.com

4 Required Permissions

4.1 Android Permissions

The Hypori Client for Android requires permission for installation. The following permissions are requested during the Client installation on Android devices:

- Access Network
- Read phone status and identity
- Call phone
- Take pictures and videos (Camera)
- Record audio (Microphone)
- GPS and network-based location
- Find, use, add, and remove accounts and set passwords
- Access and change network state
- Access Wi-Fi connection state information
- Retrieve running apps
- Change audio settings
- Read and enable/disable sync settings
- Install/uninstall shortcuts
- Prevent phone from sleeping
- Receive boot completed
- Full network access
- View network connections
- Enable Bluetooth connections
- Use fingerprint/touch ID
- Access flashlight
- Enable vibrate

A brief summary that describes how these Android permissions are used is given in the following subsections.

4.1.1 Access Network

The Hypori Client must access networks to communicate with the Virtual Device. It can use any of the provided networks (WiFi, 4G/LTE, 3G) when they are active.

4.1.2 Read phone status and identity

The Hypori Client uses the call information (specifically signal strength) on the mobile device to pass to the Virtual Device so that the information is displayed in the status bar of the Virtual Device.

4.1.3 Call phone

The Hypori Client can initiate a voice call, bypassing the Dialer interface to confirm the call.

4.1.4 Take pictures and videos (Camera)

The Hypori Client provides remote access to the device's camera to multimedia apps that use the camera in the Virtual Device or to set up your account using the QR code.

4.1.5 Record audio

The Hypori Client provides access to the device's microphone to enables voice recording and phone apps in the Virtual Device.

4.1.6 GPS and network-based location

The Hypori Client provides access to the GPS sensors and the Wi-Fi location services of the mobile device for authentication with the Hypori server and for apps in the Virtual Device that require these services.

4.1.7 Add, remove accounts and set passwords (Deprecated)

The Hypori Client uses the Android Account Manager APIs to manage Hypori Client accounts on the mobile device.

4.1.8 Access and change network state

The Hypori Client accesses the state of the cellular network interface to determine connectivity, capture statistics, and state that can be communicated to the Virtual Device so that network information can be displayed in the Virtual Device's status bar.

4.1.9 Wi-Fi connection information

The Hypori Client uses the Wi-Fi signal information (specifically signal strength) on the mobile device to pass to the Virtual Device so that the Wi-Fi connection information is displayed in the Virtual Device's status bar.

4.1.10 Retrieve running applications (Deprecated)

As part of the algorithm for detecting compromised devices, the Hypori Client can retrieve the list of running applications to determine if any known root and super user processes are running that indicate a compromised device.

4.1.11 Change audio settings

The Hypori Client can modify audio settings for audio applications running in the Virtual Device.

4.1.12 Read and enable/disable sync settings

The Hypori Client can enable and disable its sync adapter as well as control the polling rate for gathering notifications from the Virtual Device.

4.1.13 Install/uninstall shortcuts

The Hypori Client can install and uninstall application shortcuts to access apps in the Virtual Device.

4.1.14 Prevent device from sleeping

If so configured, the Hypori Client can operate in the background for one minute after the user's phone or tablet has gone to sleep (screen is black). While it is sleeping, it acquires a lock on the Wi-Fi service to keep the Wi-Fi from turning off and disconnecting from the Virtual Device.

4.1.15 Receive boot completed

The receive boot completed permission (run at startup) is used to receive notifications after the system finishes booting up.

4.1.16 Full network access

The Internet permission is required by the Hypori Client to create socket connections to Hypori servers.

4.1.17 View network connections

The Hypori Client uses the view network connections permission to determine if the network is present and online.

4.1.18 Enable Bluetooth connections

The Hypori Client uses the Bluetooth permission to discover and connect to paired Bluetooth devices.

4.1.19 Use fingerprint/touch ID

The Hypori Client uses the fingerprint permission to enable a Biometric Authentication Factor in the form of a fingerprint. The Hypori Client supports biometric fingerprint ID capabilities if the mobile device's underlying platform supports biometric authentication.

4.1.20 Access flashlight

The Hypori Client uses the mobile device's flashlight when the Client scans the QR code during the account provisioning process.

4.1.21 Enable vibrate

The Hypori Client uses the mobile device's vibrator to provide silent notification alerts.

4.2   iOS Permissions

The Hypori Client for iOS requires permission to access the mobile device's features and services. The following permissions are required for proper operation of the client for all use cases:

- Background Operation
- Camera
- Location
- Microphone
- Photo Library
- Notifications

Some permissions must be granted expressly by the user. In some cases, the permission is requested when the Client application is first launched. In other cases, the user may be prompted when the permission is first needed. In one case, it must enable the permission manually if it is required.

A brief summary that describes how these iOS permissions are used is given in the following subsections.

4.2.1   Background Operations

The Hypori Client can be configured to receive notifications. The background operations permission is required to receive notifications when the application is not active. To enable this capability, the user must enable the permission in the iOS settings – it is disabled by default.

4.2.2   Take pictures and video (Camera)

The Hypori Client uses remote access to the device's camera to support multimedia applications that use the camera in the Virtual Device. It can also use the camera when scanning a QR code during account provisioning. The user is prompted for access to the camera when the application is first started.

4.2.3   GPS and network-based location

The Hypori Client provides access to the GPS sensors and the Wi-Fi location services of the mobile device for authentication with the Hypori server and for apps in the Virtual Device that require these services. The user is prompted for access to location information when the application is first started.

4.2.4   Audio input (Microphone)

The Hypori Client provides access to the microphone and audio recording capabilities on the mobile device to support apps in the Virtual Device that require audio input. Access to the microphone is requested the first time an application in the virtual device needs to use the microphone.

4.2.5 Access photo library

The Hypori Client supports access to the camera for video recording and taking pictures. This function in iOS requires the application register for permission to access the photo library – iOS will prompt the user for this permission when a photo or video is stored on the device. However, the Hypori Client never stores the photo or video on the device and never attempts to pick and upload a photo or video from the device, thus there should never be a prompt for this permission.

4.2.6 Enable notifications

The Hypori Client uses the mobile device's notifications permission to support notification display features. The user is prompted for permission to post notifications when the application is first started.

Note: End users can enable or disable these permissions from the mobile device's iOS settings app. Some services used by the client (such as Bluetooth) may result in iOS asking the user for permission, but this is outside of the control of the Hypori Client and thus is not an explicit permission that we request.

4.3   Windows Permissions

The Hypori Client for Windows 10 requires permission to access the mobile device's features and services. The following permissions are required for proper operation of the client for all use cases:

- Internet Connectivity
- Bluetooth
- Graphics Capture
- Location
- Microphone
- Private Network Usage
- Certificate Store Usage
- Camera
- Background Tasks (Notifications)Background Operation

Some permissions must be granted expressly by the user. In some cases, the permission is requested when the Client application is first launched. In other cases, the user may be prompted when the permission is first needed. In one case, it must enable the permission manually if it is required.

A brief summary that describes how these Windows permissions are used is given in the following subsections.

4.3.1 Internet Connectivity

The Internet Connectivity permission is required by the Hypori Client to create socket connections to Hypori servers.

4.3.2 Bluetooth

The Hypori Client uses the Bluetooth permission to discover and connect to paired Bluetooth devices.

4.3.3 Graphics Capture

The Hypori Client Graphics Capture permission enables the user to take screen captures when connected to the Virtual Device.

4.3.4 Location

The Hypori Client provides access to the GPS sensors and the Wi-Fi location services of the mobile device for authentication with the Hypori server and for apps in the Virtual Device that require these services.

4.3.5 Microphone

The Hypori Client provides access to the microphone and audio recording capabilities on the mobile device to support apps in the Virtual Device that require audio input.

4.3.6 Private Network Usage

The Hypori Client Private Network Usage permission is used to access Intranet networks that have an authenticated domain controller, or that the user has designated as either home or work networks.

4.3.7 Certificate Store Usage

The Hypori Certificate Store Usage permission is used to store the User TLS client key.

4.3.8 Camera

The Hypori Client uses remote access to the device's camera to support multimedia applications that use the camera in the Virtual Device. It can also use the camera when scanning a QR code during account provisioning.

4.3.9 Background Tasks (Notifications)

The background operations permission is required to receive notifications when the application is not active.

5 Controlling Hypori Client Settings

Settings for the Hypori Clients can be controlled completely by the Hypori Server using client policies. Client policies and their configuration are described in the "Hypori Client" section (chapter 9) of the *Hypori Administrator's Guide – Server Release 4.9.0 v1.2.*

The following is an example of a client policy expressed in JSON that sets each client setting. The result of this policy is that the user will only be able to access and configure the key account information used by the client to connect to the Hypori Server.

```
{
  "version" : {
    "major" : 1,
    "minor" : 0
  },
  "android" : {
    "require-device-admin" : false,
    "disable-camera" : false,
    "password-age-days" : 30,
    "password-quality" : "unspecified"
  },
  "hypori" : {
    "remember-password" : false,
    "allow_phone_dialer_bypass" : false,
    "bluetooth-enable" : false,
    "client-launcher-enable" : true,
    "push-notifications-enable" : true,
    "notification-interval" : 300,
    "disconnect-policy" : "delayed1",
    "debug-user-options" : {
      "allow-unsavory-devices" : false,
      "disable_logging" : false,
      "enable-screenshots" : false,
      "logging-level" : "debug"
    },
    "debug-settings" : [ "connectRestart" ]
  }
}
```

Note that other values for these policies are valid (these are chosen for illustration), but the act of specifying these setting policies results in them being inaccessible and unable to be set by the user of the Hypori Client.

6 Updates and Update Verification

Hypori distributes the Hypori Client as an .APK file for Android devices, an .IPA file for iOS devices, and a Windows standard .appx file for Windows devices. You may obtain the installation package through Google Play, the Apple App Store, Microsoft Store, your enterprise IT group, or directly from Hypori. Users obtain Hypori Client updates using Android or iOS update mechanisms or from your IT group. Hypori digitally signs the Hypori installation packages as well as updates and includes the corresponding public key certificate in the package. Android and iOS devices will install an update only when the certificate in the update matches the certificate in the installed Hypori Client. The Android and iOS operating systems will report success or failure of the update process.

If the application is installed using the Apple App Store or the Google Play Store, it may be updated automatically if your App Store or Play Store is configured to do so. If it is not, selecting the "update" option for the application in the Store application will verify that the application package is valid and install it over the older version.

The Hypori Windows Client is updated by downloading the latest software version from the Microsoft Store. Updates are automatically handled by the Windows Operating System, so notifications will be given to the user about existing application updates. Hypori digitally signs the installation package as well as updates and includes the corresponding public key certificate in the package. Windows will install an update only when the certificate in the update matches the certificate in the installed client. The client is signed with a unique certificate. It can be delivered via the Microsoft Store or the enterprise IT group of the user.

If the application is installed using a Mobile Device Management (MDM) tool, the MDM tool will be able to push updates to the applications based upon the management policies of the administrators of the MDM tool. The application installation packages are made available from Hypori using the Hypori support portal at https://support.hypori.com.

If the installation is done manually by an administrator, they will need to follow Apple's guidance for enterprise installations and Google's guidance for installing an application from "unknown sources". In both cases, iOS and Android will only replace the existing application with the updated one if the signing keys are the same and that the new applications are signed properly and have not been tampered with.

The Hypori Client can be downloaded directly from Hypori.

For Android and Windows:

1. Customers will send an email to https://support@hypori.com requesting the client

2. Within the email customer must specifically ask for the client and inform the OS system they use.

3. Hypori Customer Success team will receive the request and process the request

4. Hypori Customer Success will retrieve the in production client.

5. Hypori Customer Success will upload the appropriate client to SalesForce (SFDC, Sales Force Dot Com) where the ticket is managed.

6. Hypori Customer Success will respond to the customer with a SFDC link (authentication not required) so the customer can download the client

7. The customer will have up to 48 hours to retrieve the client.

For iOS

1. If getting access to the app store is not possible, they can contact Hypori Support about options for a custom version.

See the User Guide – Android Client Version 4.2 – v.1.1, Section "*Client Requires Software Update"* for additional details on the Android updates.

See the User Guide – iOS Client Version 4.2 – v.1.1 – Section "*Hypori Client Requires a Software Update*" for additional details on the iOS updates.

See the User Guide – Windows Client Version 4.2 – v.1.1, Section "*Client Requires Software Update*" for additional details on the Windows updates.

7 Provisioning of Hypori Client Credentials

To configure a Hypori Client account, the user must provide a hostname and port for the Hypori server, a name for the account, an optional password (to access the server) or other authentication factor (like an RSA passcode), and a client certificate/credential. While the server's hostname and port can be provided to the user via some communication and the password for the user is an existing password from an enterprise account (like an Active Directory account's password), the certificate and associated credential is chosen from one of potentially many that exist in the Android Keystore System, the iOS keychain services, or the Windows Certificate Stores.

> *Note: The Hypori Client can support a Remember Password setting for each account. Administrators should not enable this functionality in the evaluated configuration. This setting is controlled using client policies on the Hypori Server.*

The 4.2 version of the Hypori Client **does not create credentials**. When using the "Add Account" screen with QR code or OTP options or a provisioning deep-link, the Hypori Client acquires the user's credentials from the Hypori provisioning server and installs it into the Android Keystore System, iOS keychain, or the Windows Certificate Stores on the mobile device and directs the Hypori Client's user to name the account to associate it with the installed credential.

See the User Guide – Android Client Version 4.2 – v.1.1, Section "*Setting up an Account*" for additional details on the Android updates.

See the User Guide – iOS Client Version 4.2 - Version 4.2 – v.1.1, Section "*Setting up an Account*" for additional details on the iOS updates.

See the User Guide – Windows Client Version 4.2 – v.1.1, Section "*Setting up an Account*" for additional details on the Windows updates.

7.1 Android Credential Provisioning

Android provides The Android Keystore System to securely store and use cryptographic keys. The Hypori Client uses the Android Keystore System's APIs to access and authenticate the user to Hypori Servers. There are two primary use models for the Android Keystore System:

1. The system-wide Android KeyChain is used when the user's credentials are to be shared across multiple applications. The credentials are maintained in the underlying system key store and the user or administrator grants access to various applications to access the credentials in the Android KeyChain.
2. The application-specific Android Keystore provider can be used when the user's credentials should not be shared across multiple applications.

There are many possible mechanisms to create and install credentials into the Android Keystore System.

- The user can be directed to a self-provisioning portal using Microsoft certificate services or equivalent, and download the credentials to the device and load them into the Android KeyChain.
- The Hypori Client can be used to contact the Hypori provisioning portal and download the user's credentials and store them into either the Android KeyChain or via the application-specific Android Keystore provider. The destination is controlled by administrator policies. The Hypori Provisioning Portal is described in the User Guide Android Client Version 4.2 – v.1.1, Section "*Acquiring a Certificate*" for additional details.
- An administrator can manually install the credentials by downloading a .p12 file to the device (perhaps using a USB cable connected to a provisioning laptop). After the .p12 file

is downloaded, the certificate and keys must be installed into the Android KeyChain by the user via the Android Settings application or another application capable of loading the p12 file.

- If permitted, the user can have the .p12 file delivered to them in a secure email or some other secure file transfer mechanism. After receiving the .p12 file, the user can load the credentials into the Android KeyChain.

Note: The Hypori Client supports proposed DoD architectures for delivering derived credentials to a mobile device. For Android devices, DISA's "Purebred" provisioning service may create and install the credentials directly into Android's system-wide KeyChain. The user configures the Hypori Client to use that credential when creating the user's Hypori Client account.

7.2   iOS Credential Provisioning

iOS provides the Secure Enclave for secure storage of cryptographic keys using the iOS Keychain APIs. Unlike Android, the iOS keychain cannot be shared by non-Apple applications, thus each application can only access their own keys.

The Hypori Client for iOS supports the following means to get the user's credentials into the iOS keychain for its use:

- The Hypori Client can contact the Hypori provisioning portal and download the user's credentials and install them into the iOS keychain. The Hypori Provisioning Portal is described in the User Guide iOS Client Version 4.2 – v.1.1, - Section "*Acquiring a Certificate*" for additional details.
- The Hypori Client can also import credentials from a ".p12 Document Provider" using the iOS Document Provider Extension and install them into the iOS keychain.
- An administrator can manually install the user's credentials into the Hypori Client's data storage by downloading a .p12 file using a USB cable connected to a provisioning laptop running Apple's iTunes. The admin must then configure the Hypori Client to import the credentials into the iOS keychain.

Note: The Hypori Client supports proposed DoD architectures for delivering derived credentials to a mobile device. On iOS devices, the Hypori Client can import credentials from the Purebred provisioning service. After the certificate import, the user configures the Hypori Client to use that credential when creating the Hypori Client account.

7.3   Windows Credential Provisioning

Windows securely stores a CA certificate for the server certificates in the platform's Windows Certificate Store during installation. (The user need not install a CA certificate when the CA is a platform trusted CA.)

- Once the Hypori account is set up, a certificate will need to be acquired and installed on your mobile device to satisfy the Hypori system's two-factor authentication requirement. On your computer, the certificate is acquired by clicking on the link provided by the Hypori Administrator. After entering the User ID and Password provided by the Hypori administrator, click **Log In**. At the bottom of the web page, click **Advanced** and then click **Download PKCS12 File**. Download the file to your Downloads folder. To install the certificate on Windows devices: Click the **green Download PKCS12** file link. The Certificate Import Wizard will open. The **Current User** is selected for Store location. The password for the private key is entered and "**Automatically select the certificate store based on the type of certificate"** is selected. The certificate will be imported and the

Certificate Store Selected will be automatically determined by the Certificate Import Wizard.

See the User Guide Windows Client Version 4.2 – v1.1, Section "*Acquiring a Certificate*" for additional details.

8 Reference Identifier for TLS

As part of setting up a new account on the Hypori Client, a user may receive enrollment instructions from the Hypori administrator. These instructions may come in the form of a web page or email and contain a link to the Hypori User Provisioning service. The user is provided with a QR code, a One-Time Password (OTP), or a deep link that is presented to the Hypori Provisioning service to automate several account-creation steps. The provisioning service provides the server hostname, port, and the user's client certificate to the Hypori Client and it generates and installs the client certificate for the account as described in section 7. Alternatively, the account information, including the certificate, can be configured manually by the user or administrator.

- See the User Guide – Android Client Version 4.2 – v.1.1, Section "*Setting up an Account*" for additional details on the Android updates.
- See the User Guide – iOS Client Version 4.2 - Version 4.2 – v.1.1, Section "*Setting up an Account*" for additional details on the iOS updates.
- See the User Guide – Windows Client Version 4.2 – v.1.1, Section "*Setting up an Account*" for additional details on the iOS updates.

The hostname of the server and the client certificate association provided by the provisioning server (or manually provided by the user or administrator) is saved as an account. The account represents the linkage between the user of the client and the particular Hypori server. The server certificate returned when connecting to the Hypori server includes the reference identifier associated with its DNS name and is validated against the hostname as required by the protection profile. The reference identifier in the client certificate is chosen by the administrator from one of several fields in the certificate during server configuration. When the client certificate is presented to the Hypori server, it is validated and the reference identifier is extracted and used to authenticate the user. See the *User Authentication* section inside chapter 8 of the *Hypori Administrator's Guide – Server Release 4.9.0, v.1.2* for how to configure and how to choose the reference identifier used to look up users in the directory server.

9 Verify Version of the Hypori Client

To verify the version of the Hypori Client, open the Hypori Client, but do not connect to the Virtual Device. On the Hypori Client Accounts or Setting screens, the footer at the bottom, lower right corner of the Hypori Client app displays the version number.