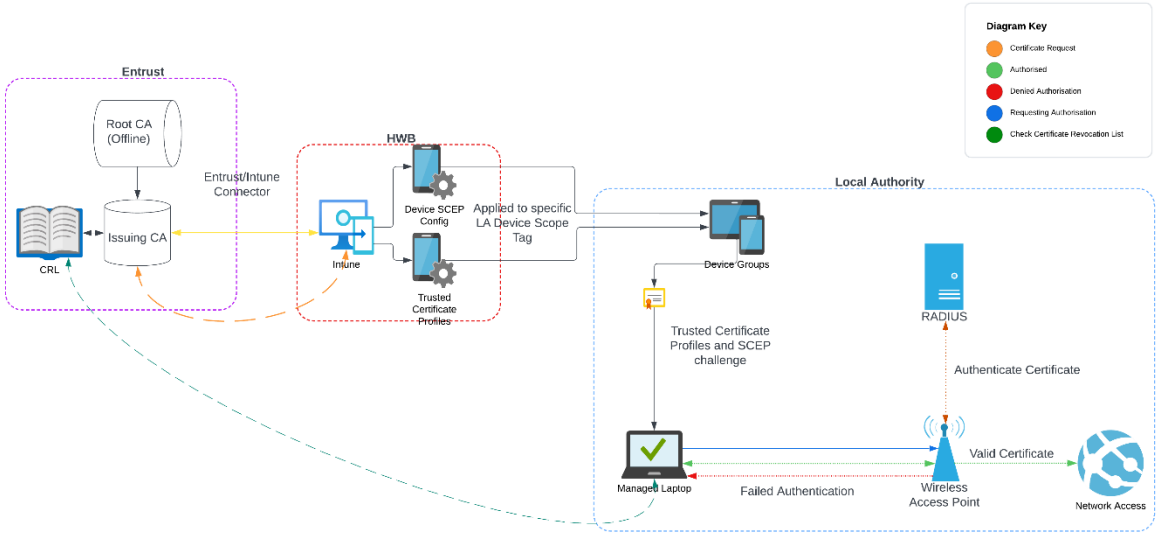
Public Key Infrastructure

Overview

This section provides information on the Hwb PKI solution, giving an overview of key components, how to deploy profiles to your managed devices and common considerations for each operating system, using the SCEP protocol.

The Hwb PKI solution supports the Education Digital Standards [Wireless Networking Standards - Hwb (gov.wales)] (E5) to facilitate access to wireless networks via certificate based authentication.



Infrastructure

The Hwb and Entrust solution for the PKIaaS is a high-assurance, high-availability setup. With all PKI solutions, there must be a Root Certificate Authority. In addition, for added layer of assurance and security, an Issuing Certificate Authority.

Root CA

The Root CA is an Offline Root CA. This is in-line with PKI best practice and ensures the high-assurance setup. The Root CA setup was done under an audited process, during a key-signing ceremony, with Entrust operatives and Hwb representatives in attendance.

During the key signing ceremony, there were 2 layers of security added, to create the high assurance for the Root CA.

Layer 1:

4 cards were created by 4 different authorised personnel. 2 from Entrust and 2 from Hwb. Each card has a different password. These cards are used to create a cypher, using the Hardware Security Module (HSM), to encrypt the Root CA.

Layer 2:

3 secure passwords were created by 3 authorised personnel, 2 from Entrust and 1 from HWB, to secure the software used to create the Root CA private/public keys.

The Root CA can only be initiated by an HSM. The HSM will need a quorum of 2/4, which means that 2 of the 4 cards created are needed to initiate it, along with the passwords associated with each. All 3 passwords are needed to initiate the software.

The cards are stored in 3 different locations across the country.

The Root CA is kept offline. It is only initiated once every 12 months, to updates the SRL, which is the CRL for the Root.

No other Issuing CA's can be created, without having the Root CA online and to authorise the new Issuing CA. This is also done as a security measure, to ensure only valid and trusted Issuing CA's are created.

The Root CA is located within a secure facility, which is monitored 24/7 by CCTV and security personnel.

Issuing CA

The Issuing CA is a cloud hosted solution. Each Issuing CA must be authorised and trusted by the Root CA, by using the Root cypher to produce a key and CSR. The Issuing CA is used to authorise the issuance of a digital certificate, on receipt of a valid certificate signing request (CSR). The requesting device/user must have the valid public key pair, for the Root and Issuing CA certificates, to create a trusted chain. Without this pairing, the certificate is deemed untrustworthy.

Intune Connector

The Intune Connector is an Azure Enterprise Application. It is the link between the Azure Hwb tenancy and Intune setup and the Entrust Issuing CA. When a device requests a certificate, it is sent through the connector to validate the request, to pass onto the CA. It is also used to allocate the certificate received from the CA to the requesting device.

Intune Configuration Profiles

There are three configuration profiles setup per operating system, which Hwb have already provided for you.

Trusted Certificate

Two of the profiles for each operating system is a Trusted Certificate. These profiles contain the public certificate for the Root and Issuing CA and must be deployed to any device group requiring a certificate. This is to ensure a trusted certificate chain is in place.

The naming conventions for these profiles are:

- LA Code-HwbPKI-Root-TrustedCert
- LA Code-HwbPKI-Issuing-TrustedCert
- LA Code-HwbPKI-iOS-Root-TrustedCert
- LA Code-HwbPKI-iOS-Issuing-TrustedCert
- LA Code-HwbPKI-MacOS-Root-TrustedCert
- LA Code-HwbPKI-MacOS-Issuing-TrustedCert

For example, 667-HwbPKI-Root-TrustedCert

SCEP Profiles

One SCEP profile per operating system has been created. These profiles contain the information to form a CSR for the CA. The Common Name (CN) of each profile, under Subject name format, should not be amended, but the Subject Alternative Name (SAN) can be modified to your preference. The CN contains a unique identifier for your LA and so must remain unmodified. The validity of these certificates is set to 1 year, from date of issuance.

The naming conventions for these profiles are:

- LA Code-HwbPKI-SCEP
- LA Code-HwbPKI-iOS-SCEP
- LA Code-HwbPKI-MacOS-SCEP

Warning: DO NOT change the CN field of the SCEP profile. If a unique identifier is needed, please make use of the SAN.

It is recommended that you should test these profiles on a small number of devices, in the first instance, to ensure your RADIUS server, Wi-Fi systems and Wi-Fi profiles have been configured to authorise and authenticate the issued digital certificates. Once you are satisfied it all works as it should, then you can rollout the setup to the rest of your devices.

Considerations and Scenarios

Scenario 1

Certificate Expiry date approaching (Windows): -

A device certificate is expiring within the 20% parameter, i.e. 73 days.

Outcome: The device sends a renewal request. A new certificate is issued and replaces the old one. The old certificate serial in Entrust is marked as expired. Renewal requests will continue, until renewal is successful.

Certificate Expiry date approaching (iOS/MacOS): -

Outcome: The device sends a renewal request. The device must be unlocked (if MacOS device has just been switched on, you must login to unlock the keychain and remain logged in) while synching with Intune. If the renewal was not successful, the expired certificate will remain on the device and Intune does not trigger a renewal thereafter. Intune does not offer an option to redeploy expired certificates.

To renew, the device must be removed from the device group that has the SCEP profile assigned, then readded to force a new SCEP to request a new certificate.

Scenario 2

Certificate has expired (Windows): -

The device certificate has expired but the device has not been on for some time, an unsuccessful renewal, or has missed the renewal period.

Outcome: The device must join another Wi-Fi SSID or be on a LAN connection. This will allow it to communicate and sync with Intune. Once this has been completed, the device can then request an updated certificate. Once the new one has been added to the store, the device can then join the correct Wi-Fi SSID.

Certificate has expired (iOS/MacOS): -

Outcome: The device must join another Wi-Fi SSID or LAN (MacOS). It will then need to be removed from the group containing the SCEP profile. Sync device. The device will then need to be readded into the group and synced, to force a new certificate to be issued.

Scenario 3

Autopilot Reset (Windows Only): -

When a Windows device needs a reset, the admin clicks on the Autopilot Reset button in Intune. This will remove any user profiles, user installed apps and return the device to the default build.

Outcome: The device thinks it is a new device and requests a new certificate. This is added to the Personal certificate store. The issue is the old certificate still exists in the store. There are now 2 personal certificates. If another Autopilot reset is initiated, another certificate is requested and added to the other certificates. Please delete the old certificate after reset.

Note: A Design Change Request has been submitted to Microsoft to change this behaviour

Further Information & Support

If you need further information or any support from Hwb, please email support@hwbcymru.net or call 03000 25 25 25