Widevine Level-1 Provisioning Models

version 1.2

tinskip@google.com

Contents

materially required to perform or implement any of the listed items.

References

1. Widevine Security Integration Guide for CENC
2. Widevine DRM - Getting Started with Devices

Terms and Definitions

- **DRM License:** An object containing secret cryptographic keys used to decrypt premium media content, along with policy information regarding requirements and restrictions for using the keys. The license is individualized for each device (i.e. it is non-transferrable). Successful delivery and application of content keys, and enforcement of the enclosed policies are the end-goals of the DRM process.
- **DRM Certificate:** An RSA-based proprietary-format certificate generated by Widevine, and used as an authentication token for DRM servers and clients.
- **DRM Device Certificate:** A DRM certificate provisioned to a specific device to use with a specific content provider's license service.
- **DRM Service Certificate:** A DRM certificate assigned to a content provider, and which is used to authenticate its servers and hiding device identifying information.
- **Keybox:** A factory-provisioned device-unique object containing secret cryptographic key material used as a Widevine device root of trust.
- **OEM Certificate:** An X.509 RSA-based certificate trusted by Widevine as a device root of trust to bootstrap the DRM Device Certificate provisioning process.
- **Pre-Provisioning Key:** A secret cryptographic key assigned to the device type. The mapping between System ID and Pre-Provisioning key is 1:1.
- **SPOID:** Stable Per-Origin IDentifier. A 128-bit value (GUID) associated with a device, which is unique per content provider, and stable across device power washes, factory resets, etc.
- **System ID:** A numeric identifier assigned to a specific device type (make / model) upon device type registration.
- **Widevine Device Root of Trust:** An OEM-provisioned cryptographic token used to establish device authenticity in the form of a Keybox or an OEM Certificate.

Introduction

This document shall describe the various supported modes of provisioning Widevine-enabled devices with a Widevine DRM root of trust for purposes of DRM license acquisition. The processes described in this document are dependent on Widevine Provisioning and Licensing Protocols, as well as the OEMCrypto Hardware Abstraction Layer, and apply only to Widevine Level1 compliant devices.

Installing a Widevine DRM Certificate on a device first requires that the device have a root of trust provisioned on the device by the OEM. This OEM provisioned root of trust is used as authentication when provisioning a Widevine DRM root of trust.

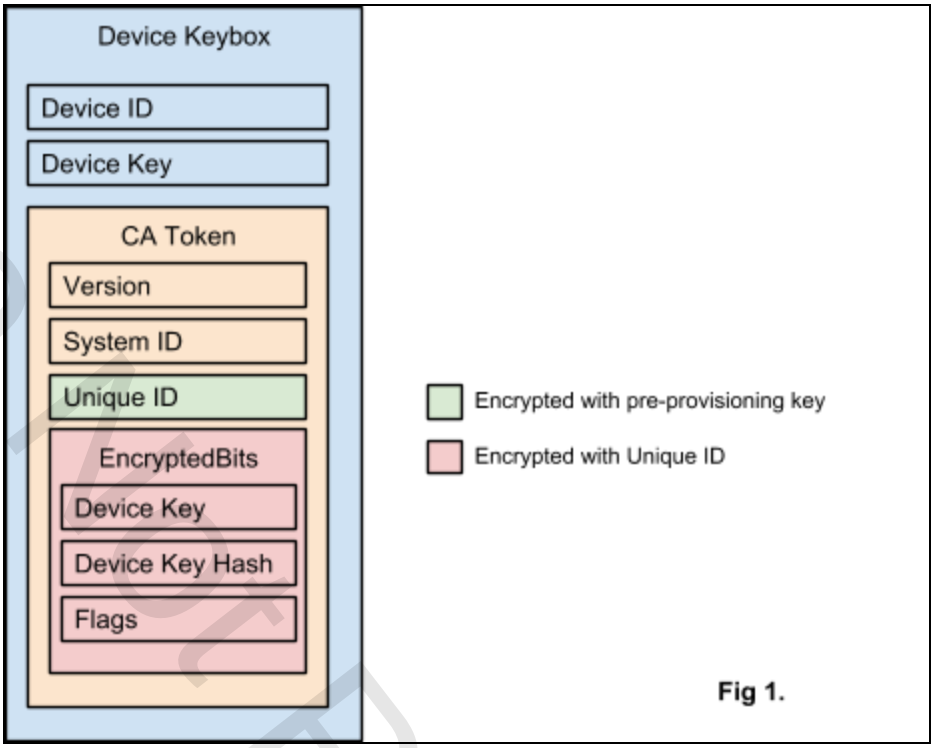
Provisioning 1.0

Provisioning 1.0 was meant to only work with Widevine License Servers. Because of this it uses a shared secret as both device root of trust, and to retrieve DRM licenses.

The Device Keybox

In the Provisioning 1.0 model, the Device Keybox is used as a device root of trust directly for obtaining DRM licenses from the Widevine License Servers. This approach has the disadvantage of not being sharable with partners who want to operate their own License Servers. Because of this, this application of the Device Keybox has been deprecated, and should only be used by Widevine “Classic” client devices.

The following illustration shows the contents of the Widevine device keybox:



The Device Keybox uses AES-128 keys. Each device is factory provisioned with a device-unique keybox. When a DRM license is needed, the CA Token in Fig. 1 above is sent to the DRM License Server to authenticate the device.

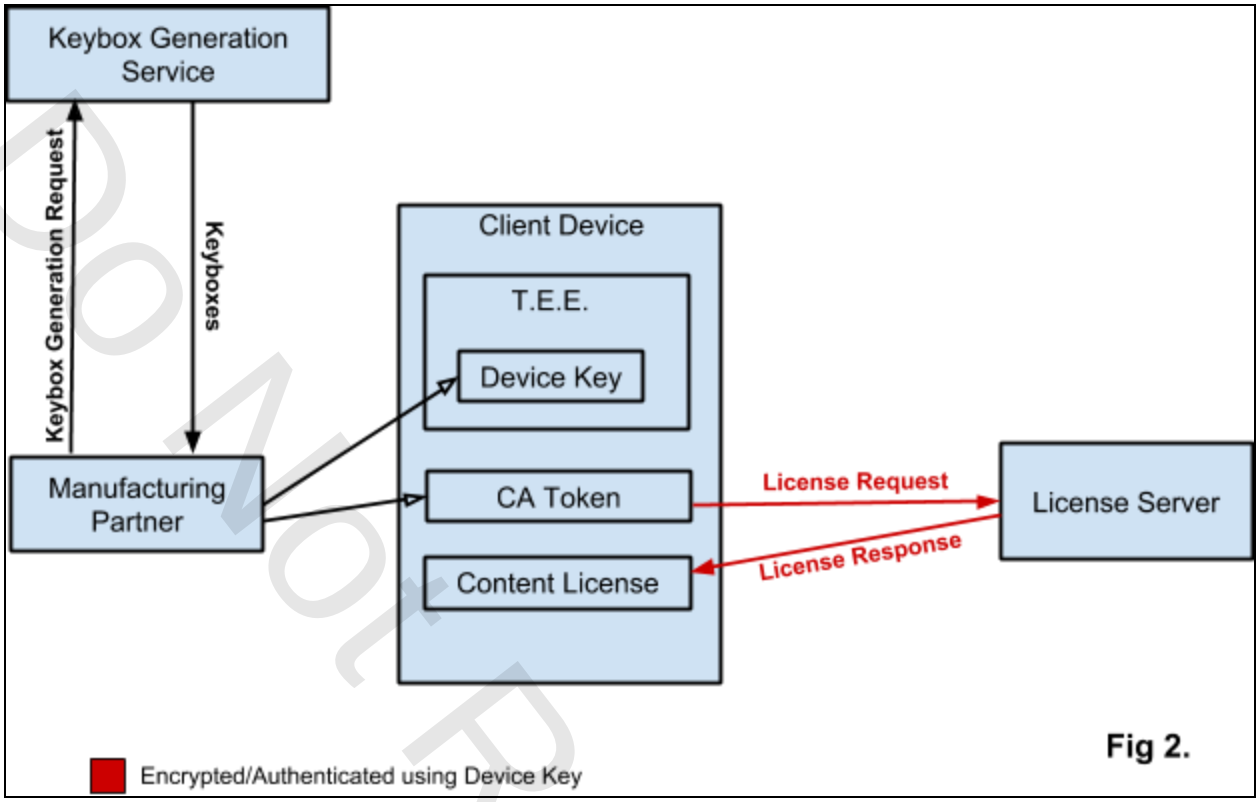


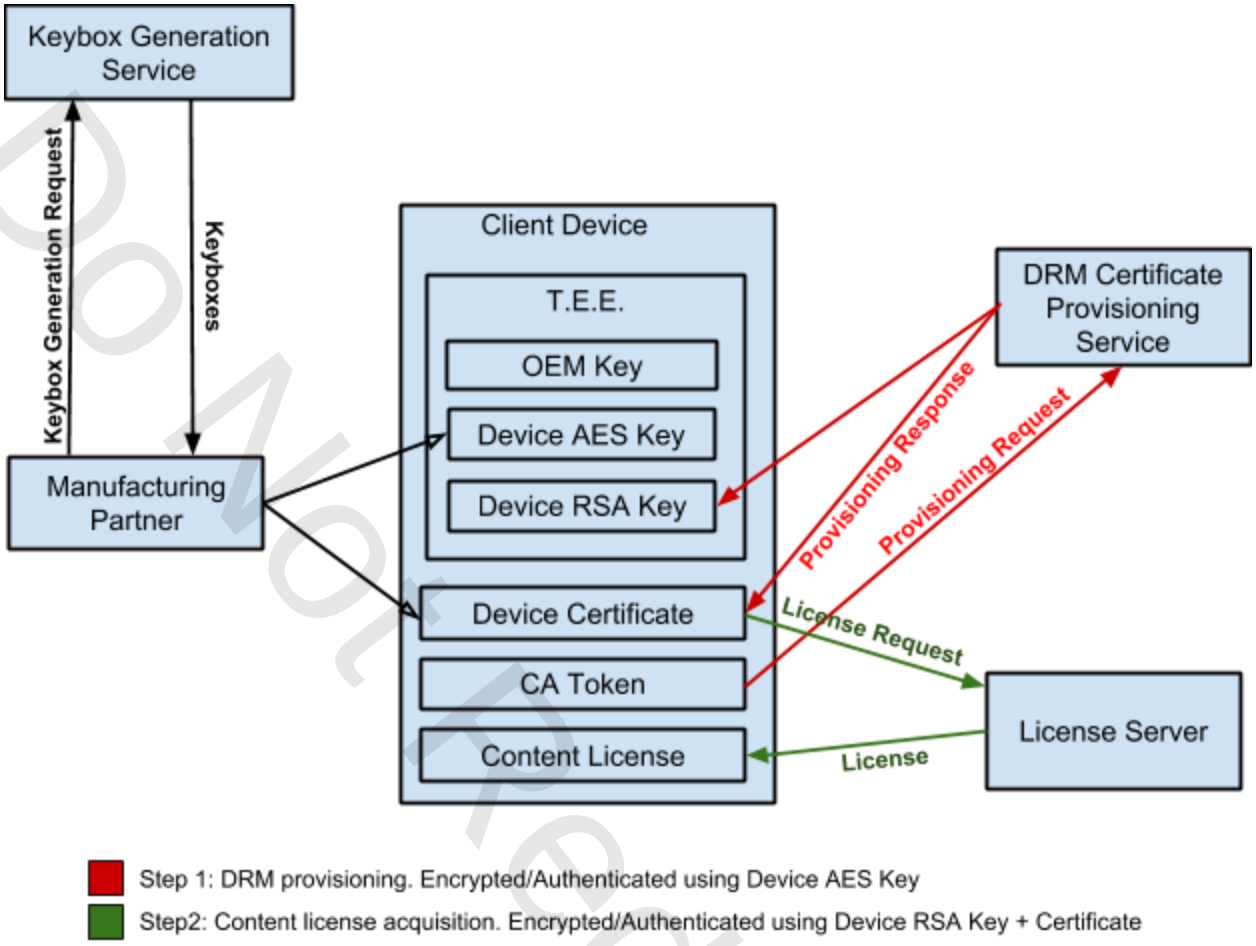
Fig 2.

The above diagram shows the provisioning and application of device keyboxes in Provisioning 1.0

Provisioning 2.0

In the Provisioning 2.0 model, the OEM factory-provisioned keybox is used as a root of trust to securely install a unique Device DRM Certificate and matching RSA private key on the Client Device. This certificate + RSA key pair is then used to authenticate the Client Device and secure media licenses, and may be used by external partners to deliver licenses, as it is based on Public Key Cryptography. Provisioning 2.0 requires functionality present in OEMCrypto v8 and newer.

The following illustration shows the storage of the Keybox on the Client Device, the device certificate provisioning, and a license request leveraging the certificate:



Provisioning 3.0

The Provisioning 3.0 model uses an OEM-generated device root of trust which may be installed by the OEM at the factory or Over The Air. This OEM root of trust, or OEM Certificate can then be leveraged by Widevine or other content providers to provision devices with provider-specific DRM certificates. Provisioning 3.0 requires functionality optionally present in OEMCrypto v12 or newer.

OEM Certificates

OEM Certificates are those which are installed onto devices by OEMs along with their corresponding private keys. There are two types of OEM certificates:

1. **Intermediate OEM Certificate:** Generated as a CA certificate signing request (CSR) for a specific device type (make/model/year), and signed by Widevine. This CA certificate can be used by the OEM to generate a OEM device (leaf) certificate for each device.
2. **OEM Device Certificate:** Generated by the OEM, and signed by the device type Intermediate OEM CA certificate, this certificate is provisioned onto the device by the OEM along with its corresponding private key. It is later used to request provider-specific Widevine DRM certificates.

NOTE: Widevine provides tools to help the OEM generate and manage Intermediate and Device OEM certificates. However, secure storage of private keys is the responsibility of the OEM.

Factory Provisioning

This is the most common method of device provisioning, during which the OEM provisions a device-unique OEM Device Certificate and private key onto devices before they leave the factory.

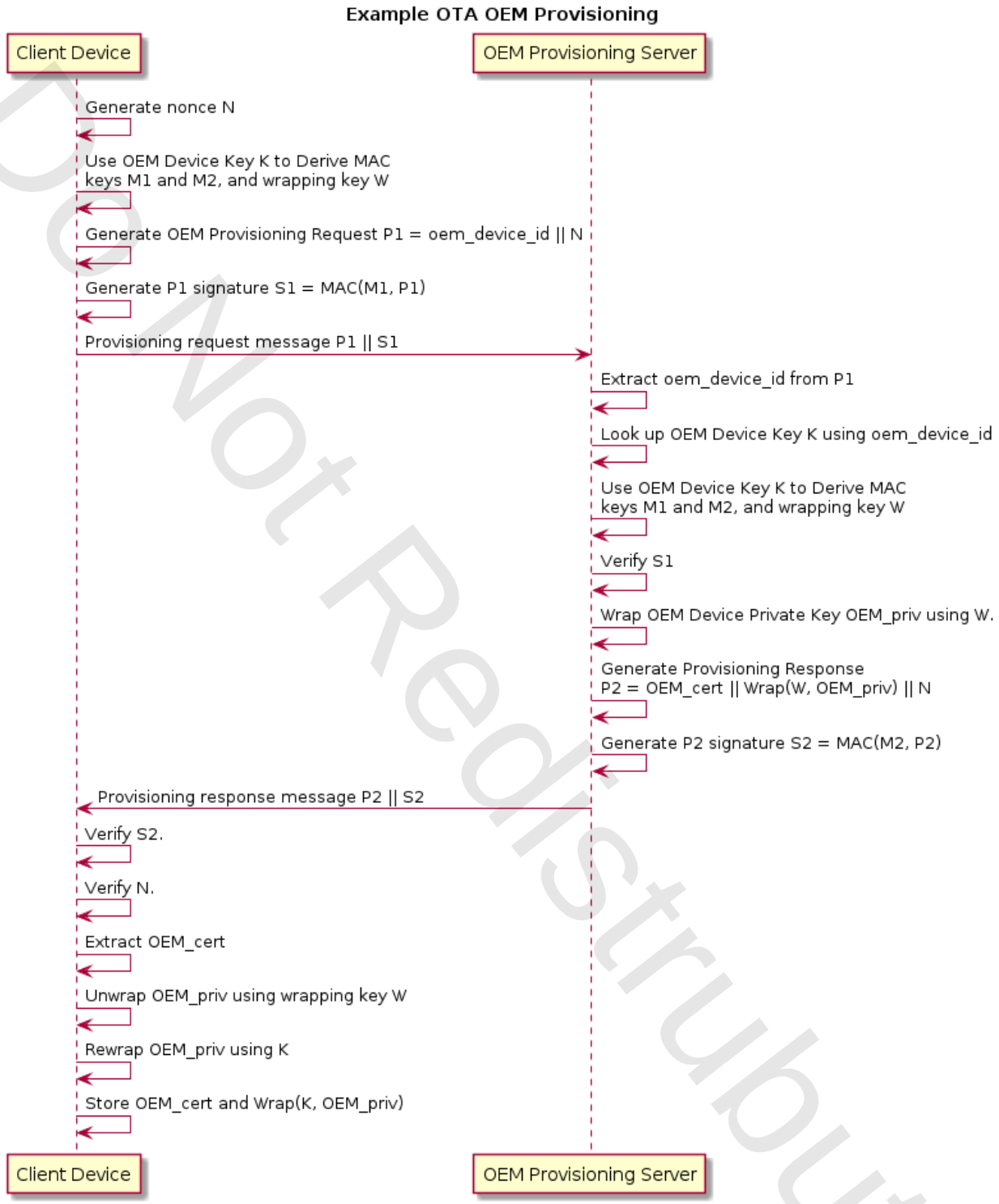
Out-of-Box Bootstrapping

The Widevine DRM system can be bootstrapped out-of-box given two important prerequisites:

1. The devices must have a working version of OEMCrypto v12 or higher, supporting Widevine Provisioning 3.0.
2. The devices must have some type of secure cryptographic secret which the OEM can leverage for bootstrapping the Widevine DRM (OTA provisioning). This secret shall be no less robust than an AES-128 key.
3. In the case of software implementations running on closed, secure booted devices, the device must be able to prove it is booted in a secure mode when provisioning and acquiring licenses.

Example: OTA Provisioning Using Secret OEM Device 128-bit Key.

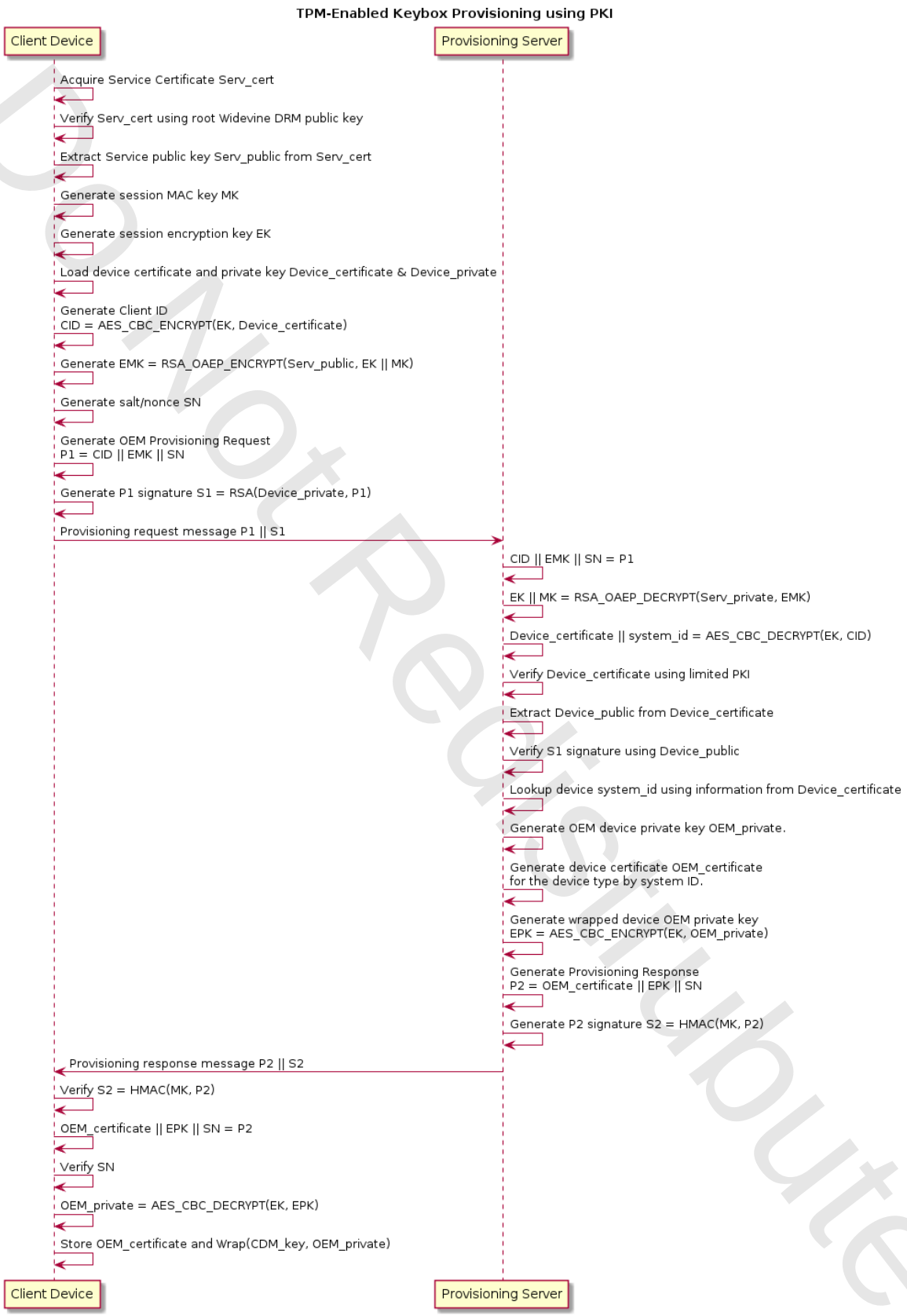
In this example, each device has a unique OEM Device ID, and AES-128 OEM Device Key which is known to the OEM.



NOTE: The above is just an example. Widevine reserves the right to audit an OEM's OTA provisioning protocol.

Example: OTA Provisioning Using PKI.

In this example, each device has a unique certificate and private key pair which can be authenticated and used to secure the provisioning transaction.



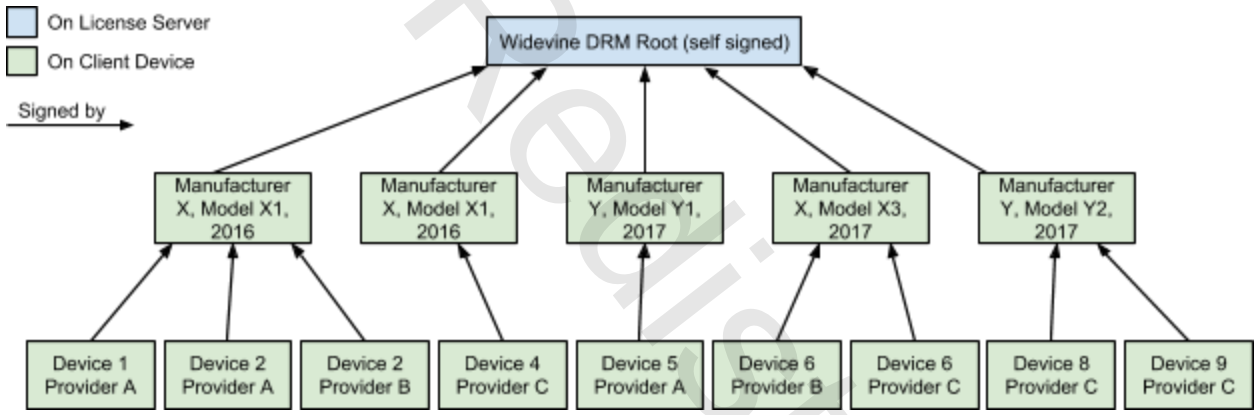
Device DRM Provisioning

Device DRM provisioning is the process by which a device receives DRM credentials to be used for license acquisition from a specific content provider. The provisioning may be performed by Widevine, or in some very specific circumstances, by the content provider itself.

Widevine DRM Provisioning

This is the most common form of device DRM provisioning. In this model, the client device contacts the Widevine DRM Provisioning Service to obtain DRM credentials for a specific content provider using the OEM Device Certificate as device root of trust for DRM provisioning. Once these credentials have been obtained, the device may store them and use them indefinitely to obtain media licenses from the content provider.

Widevine DRM Certificate Chain



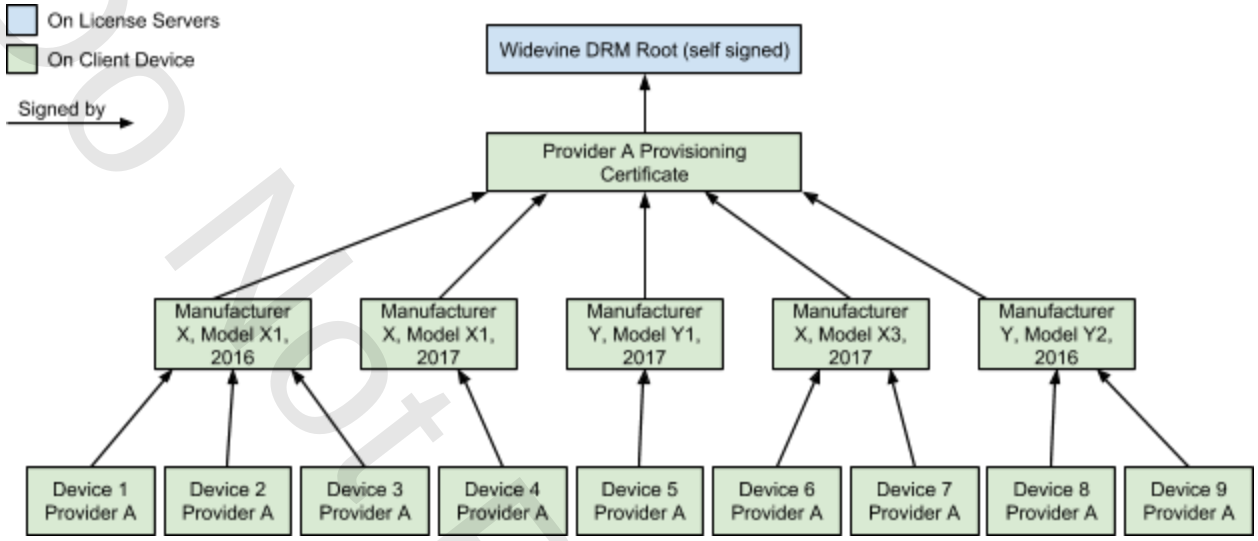
Each device may have a number of device DRM certificates, one for each content provider it has accessed. Each of these is signed by a common intermediate make / model type certificate, which in turn is signed by the Widevine DRM root certificate. The unit of revocation in this case is the device make / model. Revocation is performed by revoking the intermediate make / model type certificate.

Provider DRM Provisioning

In some very specific circumstances, a content provider may operate a Widevine DRM Provisioning server for the purpose of generating DRM Device Certificates for use with its own service. This capability is restricted for use in environments where the Widevine DRM Provisioning Service is not reachable, such as airplanes. As in the case of Widevine DRM Provisioning, it uses the OEM Device Certificate as device root of trust for DRM provisioning.

Once these credentials have been obtained, the device may store them and use them indefinitely to obtain media licenses from the content provider.

Provider DRM Certificate Chain



In this scenario, the Provider requests a Provisioning Certificate from Widevine. It can then use this certificate to generate intermediate device certificates for any device types registered with Widevine, as well as DRM device certificates for use with its license server. These DRM device certificates are not valid for use with any other provider's services.
The generating provider is responsible for DRM certificate key security, and for revocation of any generated intermediate device type certificates.
Widevine provides a Provisioning SDK which implements the Widevine DRM Device Provisioning Protocol, and which providers can use to implement their own DRM provisioning services.