WIDEVINE

OEMCrypto State Diagrams

November 12, 2019

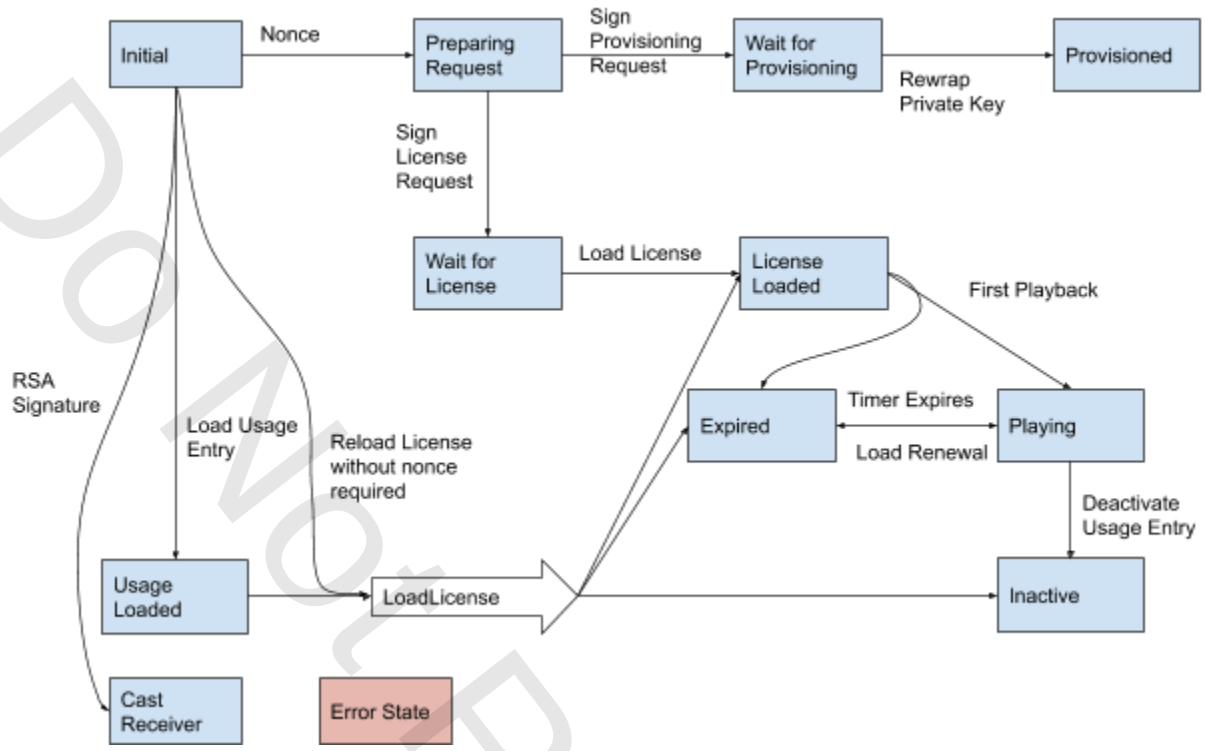
Document Status: Shared externally with partners who have signed the Widevine MDA. This document is being distributed as part of the OEMCrypto v16 design.

Overview

To understand proper usage of OEMCrypto functions, it is helpful to think of an OEMCrypto session as a state machine. OEMCrypto implementers are not required to use a state machine. For v16, Widevine does have the following requirements.

1. Only one of OEMCrypto_LoadLicense can be called in each session, and that function can only be called once in each session.
2. Only one of OEMCrypto_LoadUsageEntry and OEMCrypto_CreateUsageEntry can be called in each session, and that function can only be called once in each session.
3. OEMCrypto_GenerateNonce can only be called once in each session, and it must be called before signing either a provisioning request or a license request.

The diagram below shows the possible transitions among each state:



The states for an OEMCrypto Session are:

- **Initial** - when a new session is opened, it starts in the initial state.
- **Preparing_Request** - After a successful call to OEMCrypto_GenerateNonce, the session is being used to prepare a message to a server.
- **Wait_For_Provisioning** - After a successful call to SignProvisioningRequest, the session is waiting for a provisioning response.
- **Provisioned -** After a successful call to LoadProvisioning, the session is provisioned.
- **Wait_For_License** - After a successful call to PrepAndSignLicenseRequest, the session is waiting for a license response.
- **License_Loaded -** After a successful call to LoadLicense, the session is waiting for playback to begin.
- **Playing -** The session moves to the playing state when the first playback is attempted. If license durations have not expired, the session moves to the playing state.
- **Expired** - After the playback timer expires, the session is in the expired.
- **Inactive** - After a call to DeactivateUsageEntry, the session is holding a license that cannot be used for playback. It may still be used to report usage.
- **Usage_Loaded** - After a successful call to LoadUsageEntry, the session is ready to reload a license or clean up the usage table.
- **Cast_Receiver -** After a call to GenerateRSASignature, the session may only be used to sign cast receiver messages.
- **Error_State** - If any Sign*Request, LoadLicense, LoadKeys, or RewrapDevice* function fails, the session is in an error state. SImilarly, if an attempt is made to call a function in

the wrong state, the session transitions to the error state. The session may only be closed when in this state. This does not include “buffer too small” errors, where a recall to the function is expected.

The following functions may only be called in some states. Functions that cause a transition are in bold.

OEMCrypto_OpenSession - puts session in Initial_State.

OEMCrypto_GenerateNonce - May only be called in Initial state. The session transitions to Preparing_Request state.

OEMCrypto_GenerateDerivedKeys - May only be called in Wait_For_Provisioning state.

OEMCrypto_DeriveKeysFromSessionKey - May only be called in Wait_For_Provisioning or Wait_For_License state.

OEMCrypto_PrepAndSignLicenseRequest - May only be called in Preparing_Request state. The session transitions to Wait_For_License state.

OEMCrypto_PrepAndSignProvisionRequestt - May only be called in Preparing_Request state. The session transitions to Wait_For_Provisioning state.

OEMCrypto_PrepAndSignRenewalRequest - May only be called in License_Loaded, Expired or Playing states.

OEMCrypto_LoadKeys - May only be called once. The session transitions to LIcense_Loaded state.

OEMCrypto_LoadLicense - May only be called once. The session transitions to LIcense_Loaded state.

OEMCrypto_LoadOEMPrivateKey - May only be called in Preparing_Request.

OEMCrypto_LoadProvisioning - May only be called in Wait_For_Provisioning. The session transitions to Provisioned.

OEMCrypto_LoadPrivateDRMKey - May only be called in Preparing_Request state.

OEMCrypto_GenerateRSASignature - May only be called in Initial state. The session transitions to Cast_Receiver state.

OEMCrypto_CreateNewUsageEntry - May only be called in Wait_For_License state. It may only be called once.

OEMCrypto_LoadUsageEntry - May only be called in Initial state. The session transitions to Usage_Loaded state.

The following functions may be called in License_Loaded, Expired, Playing or Inactive states:

OEMCrypto_LoadEntitledContentKeys

OEMCrypto_SelectKey

OEMCrypto_QueryKeyControl

OEMCrypto_DeactivateUsageEntry - The session and usage entry transitions to Inactive state.

LoadRenewal - May only be called in License_Loaded, Expired, or Playing state. If the state was expired and the timer has been restarted, the session transitions to Playing state.

The following functions may be called in License_Loaded or Playing state: OEMCrypto_DecryptCENC, OEMCrypto_Generic_Encrypt, OEMCrypto_Generic_Decrypt, OEMCrypto_Generic_Sign, OEMCrypto_Generic_Verify. When called from License_Loaded state, the call is treated as a first decrypt for the session. The session transitions to either Playing or Expired depending on the state of the session's timers.

OEMCrypto_MoveEntry - May only be called in Usage_Loaded state.

The following functions may be called in any state in which a usage entry has been loaded or create:
OEMCrypto_ReportUsage
OEMCrypto_UpdateUsageEntry

The following functions may be called in any state:
OEMCrypto_CopyBuffer
OEMCrypto_LoadSRM
OEMCrypto_GetKeyData
OEMCrypto_GetDeviceID
OEMCrypto_GetProvisioningMethod
OEMCrypto_APIVersion
OEMCrypto_BuildInformation
OEMCrypto_Security_Patch_Level
OEMCrypto_SecurityLevel
OEMCrypto_GetHDCPCapability
OEMCrypto_SupportsUsageTable
OEMCrypto_IsAntiRollbackHwPresent
OEMCrypto_GetNumberOfOpenSessions
OEMCrypto_GetMaxNumberOfSessions
OEMCrypto_SupportedCertificates
OEMCrypto_IsSRMUpdateSupported
OEMCrypto_GetCurrentSRMVersion
OEMCrypto_GetAnalogOutputFlags
OEMCrypto_ResourceRatingTier
OEMCrypto_CloseSession

The following functions are special:
OEMCrypto_SetSandbox -- only called on system initialization.
OEMCrypto_Initialize -- only called on system initialization.
OEMCrypto_Terminate -- only called on system termination.
OEMCrypto_WrapKeyboxOrOEMCert - only called in the factory.
OEMCrypto_InstallKeyboxOrOEMCert -- only called on system initialization.
OEMCrypto_LoadTestKeybox -- only called on system initialization.

OEMCrypto_IsKeyboxOrOEMCertValid -- only called on system initialization.
OEMCrypto_LoadTestRSAKey -- only called on system initialization.
OEMCrypto_CreateUsageTableHeader -- not a session function.
OEMCrypto_LoadUsageTableHeader -- not a session function.
OEMCrypto_DeleteOldUsageTable -- not a session function.
OEMCrypto_CopyOldUsageEntry -- only called on system initialization
OEMCrypto_ShrinkUsageTableHeader -- not a session function.
OEMCrypto_GetOEMPublicCertificate - modified version is not a session function.

The following functions are obsolete:
OEMCrypto_GenerateSignature - replaced.
OEMCrypto_RefreshKeys - replaced.
OEMCrypto_RewrapDeviceRSAKey30 - replaced,
OEMCrypto_RewrapDeviceRSAKey - replaced.
OEMCrypto_LoadDeviceRSAKey - replaced.