

THALES

SENTINEL LDK

MIGRATION GUIDE: SENTINEL HASP TO SENTINEL LDK



All information herein is either public information or is the property of and owned solely by Thales DIS France S.A. and/or its subsidiaries or affiliates who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Thales DIS France S.A. and any of its subsidiaries and affiliates (collectively referred to herein after as "Thales") information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

- The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.
- This document shall not be posted on any network computer or broadcast in any media and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided "AS IS" without any warranty of any kind. Unless otherwise expressly agreed in writing, Thales makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Thales reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Thales hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Thales be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Thales does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Thales be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Thales products. Thales disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

Copyright © 2022 THALES. All rights reserved. Thales, the Thales logo and Sentinel are trademarks and service marks of Thales and/or its subsidiaries and affiliates and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the properties of their respective owners.

Product Version: 8.3 and later

Document Part Number: 000-000000-001, Rev. C, 2209-1

CONTENTS

| | |
|--|-----------|
| Introduction..... | 4 |
| About Sentinel LDK..... | 4 |
| About This Guide | 4 |
| About Sentinel HL Keys | 5 |
| Requirements for Run-time Environment..... | 5 |
| Available Migration Paths..... | 6 |
| Shortcut to Enhanced Protection | 6 |
| Support Contacts | 7 |
| CHAPTER 1: Migration Path 1— Sentinel LDK and Sentinel Keys Combined API Implementation | 8 |
| Stage 1: Combining Sentinel Keys with Sentinel LDK Protection..... | 9 |
| Implementing Stage 1 | 10 |
| Stage 2: Full Implementation of Advanced Sentinel LDK Functionality..... | 11 |
| Implementing Stage 2..... | 11 |
| CHAPTER 2: Migration Path 2—Gradual Migration from Sentinel Keys to Sentinel LDK Using a Launcher Application | 12 |
| Stage 1: Initial Implementation of Sentinel LDK Functionality | 13 |
| Implementing Stage 1 | 13 |
| Stage 2: Full Implementation of Sentinel LDK Functionality..... | 14 |
| Implementing Stage 2..... | 14 |
| APPENDIX A: Sentinel LDK and Sentinel Hardware Keys Comparison Tables..... | 15 |

INTRODUCTION

About Sentinel LDK

Sentinel[®] LDK is a Software Digital Rights Management (DRM) solution that delivers strong copy protection, protection for Intellectual Property, and secure and flexible licensing. Sentinel LDK is an all-in-one solution that enables you to choose a hardware- or software-based protection key, based on business considerations. Sentinel LDK software engineering and business processes are completely separate to ensure:

- > Effective and efficient product development
- > Quick time to market
- > Immediate addressing of customer and market needs
- > Comprehensive support throughout a software product's protection and licensing life cycle

The level of protection for your software is determined by the locking type you choose—hardware-based or software-based. Sentinel LDK hardware-based protection, which utilizes Sentinel HL keys, provides the safest and strongest level of protection. Sentinel LDK software-based protection, which utilizes Sentinel SL keys and software activation, provides electronic software and license distribution. Both keys are supported by the same set of tools and APIs, and the transition between them is transparent.

About This Guide

Thales provides you with a broad spectrum of DRM products. Without losing security, you can use this guide to migrate from Sentinel Hardware Keys to the Sentinel LDK product and gain the capabilities of having a licensing solution that provides strong security against piracy (by using HL keys) and the flexibility of software-based licensing (SL keys) within the same implementation.

The primary factors for migrating from Sentinel Hardware Keys to Sentinel LDK are:

- > Business logic is more flexible using Sentinel LDK-EMS.
- > The same implementation of Sentinel LDK provides access to both software-based (SL) and hardware-based (HL) license protection.
- > No loss of license protection security in moving from Sentinel Hardware Keys to Sentinel LDK

The guide assumes that the reader has a good understanding of both the Sentinel Hardware Keys and the Sentinel LDK systems and provides the following:

- > Migration paths from Sentinel Hardware Keys to Sentinel LDK, each with an overview, guidelines, and discussion of advantages and disadvantages.
- > Procedures relating to the migration that are not documented in either the Sentinel Hardware Keys documentation or the *Sentinel LDK Software Protection and Licensing Guide* and Help documentation
- > Tables comparing Sentinel LDK and Sentinel Hardware Keys, tools, and API functions.

For detailed information and procedures relating to Sentinel LDK, refer to the *Sentinel LDK Software Protection and Licensing Guide* or to the relevant Sentinel LDK Help documentation.

For detailed information and procedures relating to Sentinel Hardware Keys, refer to the *Sentinel Hardware Keys Developer's Guide*.

NOTE: The procedures and terminology employed in this guide are based on the assumption that you want to migrate from your Sentinel Hardware Keys to Sentinel HL keys. However, since Sentinel HL keys and Sentinel SL keys are supported by the same set of tools and APIs, the procedures for migrating to Sentinel SL keys are similar (migrating to Sentinel SL keys requires an activation process). If you want to migrate to Sentinel SL keys, refer to the *Sentinel LDK Software Protection and Licensing Guide* or contact Thales Technical Support.

About Sentinel HL Keys

The following types of Sentinel HL keys are available, replacing the HASP HL keys that were provided until now:

> Sentinel HL (Driverless configuration) keys

These keys make use of HID drivers (included in the Windows operating system) instead of Thales drivers. When used as standalone keys, these keys can be used without installing the Run-time Environment. (Network keys require the Run-time Environment.) However, these keys are not backward-compatible with applications protected with Sentinel LDK 6.1 or earlier, Sentinel HASP, HASP HL 1.x, or HASP4. To use these keys, your protected application must include the Licensing API libraries from Sentinel LDK v.7.1 or later, and you must be working with the backend from Sentinel LDK v.7.1 or later.

> Sentinel HL (HASP configuration) keys

These keys are fully compatible with existing HASP HL keys and with older generations of HASP keys (and with Hardlock/HASP4 keys). These keys can work with your existing API libraries and Run-time Environment, and you can work with your current backend environment. These keys can be upgraded at the customer site to Sentinel HL (Driverless configuration) keys and can thus provide all the benefits provided by the Driverless-configuration keys.

NOTE: Occurrences of the term **Sentinel HL key** in this guide generally refer to the Sentinel HL (Driverless configuration) key.

Requirements for Run-time Environment

You are required to install the Sentinel LDK Run-time Environment on at least some of your machines for the following types of Sentinel protection keys:

- > Sentinel SL-AdminMode keys (the type of Sentinel SL key recommended for one of the migration paths in this book).
- > Sentinel HL (HASP configuration) standalone keys. The Run-time Environment is required on the computer where the protected application is executed and the key is attached.

> Sentinel HL network keys.

This includes the following keys:

- Sentinel HL Net and NetTime (HASP configuration) keys
- Sentinel HL Net and NetTime (Driverless configuration) keys
- Any Sentinel HL (Driverless configuration) key (other than Basic) with a concurrency license

The Sentinel HL network key is connected to any computer in the network.

The Run-time Environment is required on the computer where the network key is attached. The protected application can execute on different computers in the network.

The standalone Sentinel HL (Driverless configuration) keys do not require the Run-time Environment.

For more information, see “Protection Keys That Require Sentinel LDK Run-time Environment” in the *Sentinel LDK Software Protection and Licensing Guide*.

Available Migration Paths

Both migration paths contain two stages; each designed to facilitate your move from Sentinel Hardware Keys to the protection and licensing functionalities of Sentinel LDK.

The stages are not interdependent, meaning that it is possible to begin at Stage 2. Similarly, the time that you wait before moving from one stage to the next is entirely at your discretion.

Migration Path 1 provides a way to phase out your installation base of Sentinel keys over time—without necessitating the recall and replacement of Sentinel keys, and without having to continue their distribution.

Using Migration Path 1, and creating a version of your software that recognizes both Sentinel and Sentinel HL keys, you can start distributing Sentinel HL keys to new customers while existing customers continue using their Sentinel keys. You can then gradually replace your install base of Sentinel keys with Sentinel HL keys.

Migration Path 2 enables a gradual transition from Sentinel Keys to Sentinel LDK. A Sentinel Keys-protected version and a Sentinel LDK-protected version of your software are distributed, together with a launcher application. The launcher detects whether a Sentinel protection key is connected to the computer and launches the appropriate version of the program. For more information, see *Migration Path 2—Gradual Migration from Sentinel Keys to Sentinel LDK* on page 11.

Shortcut to Enhanced Protection

Sentinel SL “Unlocked License” is a mechanism by which the protection applied to an application can be significantly enhanced without affecting the current protection and licensing process.

You use Sentinel LDK Envelope to apply a sophisticated protection wrapper over any existing Sentinel Hardware Keys protection and licensing scheme. This wrapper protects your application against reverse engineering and theft of intellectual property.

You can apply this protection immediately as a short-term or long-term solution while you develop your process to migrate to Sentinel HL keys. For maximum security, Thales recommends that you obtain a batch code for this purpose that is different from the batch code that you will use for your Sentinel HL keys.

For more information regarding Unlocked Licenses, see the *Sentinel LDK Software Protection and Licensing Guide*. For pricing information for Unlocked Licenses, contact your Thales sales representative.

Support Contacts

You can contact us using any of the following options:

Business Contacts

To find the nearest office or distributor, go to:

<https://cpl.thalesgroup.com/software-monetization/contact-us>

Support

To obtain assistance in using Sentinel products (<https://cpl.thalesgroup.com/software-monetization/all-products>), feel free to contact our Thales Support team:

- > **Customer Support Portal** (preferred): <https://supportportal.thalesgroup.com/csm?id=sentinel>
- > **Support Essentials** (contact details, support plans, and policies):
https://supportportal.thalesgroup.com/csm?id=support_essentials
- > **For Issues Related to Using the Portal:** portal.support.DIS@thalesgroup.com
- > **Phone:**
 - In North America, call 800-545-6608 (US toll free).
 - Internationally, call +1-410-931-7520.
 - For a list of regional numbers, go to: <https://supportportal.thalesgroup.com/csm?id=sentinel>
→ Click **Contact Us** in the top-right corner of the page.

Downloads

You can download installers and other updated components from:

<https://cpl.thalesgroup.com/software-monetization/sentinel-drivers>

CHAPTER 1: Migration Path 1— Sentinel LDK and Sentinel Keys Combined API Implementation

This two-stage migration path enables you to phase out your installation base of Sentinel Keys over time, without necessitating immediate recall and replacement of the Sentinel keys and without having to continue their distribution. To achieve this status, you create a version of your software that is able to identify both Sentinel keys and Sentinel HL keys. This could be a completely new version of your software or the current version (with just the migration path changes implemented), with the ability to work with a Sentinel HL key. You can then start distributing Sentinel HL keys to all new customers, while existing users continue to use the Sentinel keys.

The time that you wait before moving from one stage to the next is entirely at your discretion. You can even skip Stage 1 and proceed directly to Stage 2.

The following table summarizes the two stages for Migration Path 1.

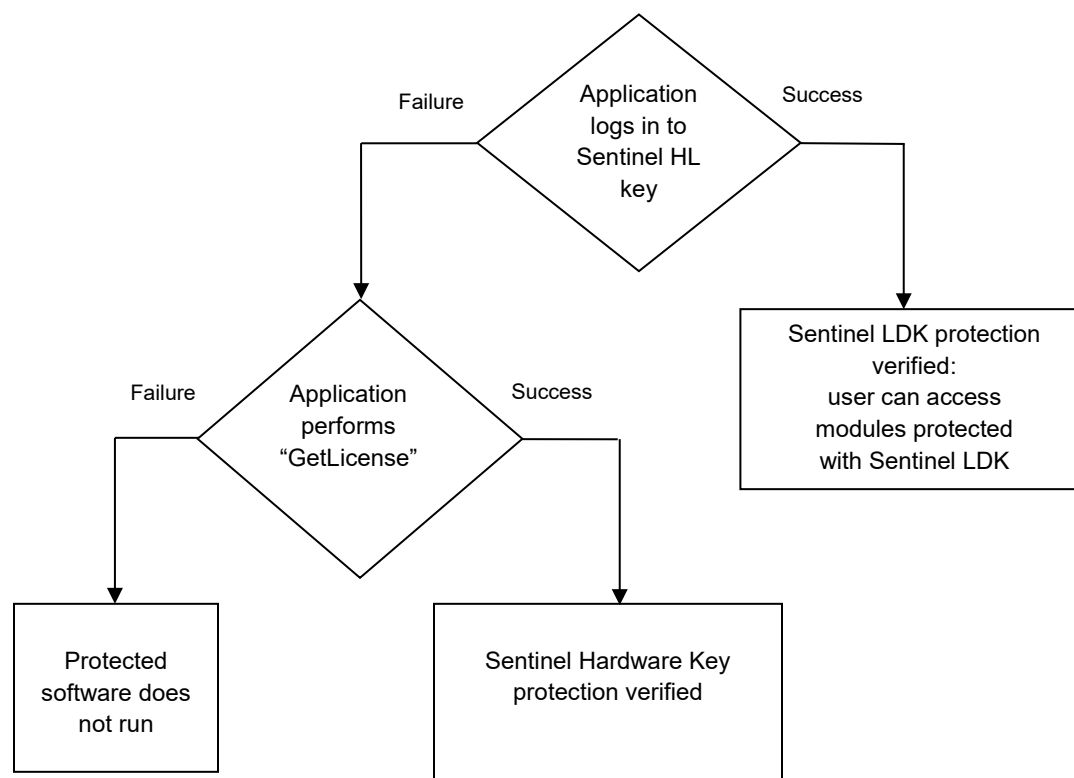
| | Stage 1 | Stage 2 |
|---|---|--|
| Implementation effort | Medium | Medium |
| Install base | Remains Sentinel Hardware Keys | Replace with Sentinel HL key |
| Keys for new customers | Sentinel HL (Driverless configuration) key | Sentinel HL (Driverless configuration) key |
| Protection process | <ul style="list-style-type: none"> • Leave Sentinel Keys API implementation • Implement Sentinel Licensing API in your code • Switch between the above implementation depending on the connected key | <ul style="list-style-type: none"> • Remove Sentinel Keys implementation • Implement Sentinel Licensing API in your code and protect using Sentinel LDK Envelope |
| Security level | Medium (due to API-only implementation) | Very high |
| Flexibility level (licensing, portability) | Medium | Very high |
| Additional benefits | Driverless deployment | Driverless deployment |

Stage 1: Combining Sentinel Keys with Sentinel LDK Protection

When your software runs, it attempts to log in to a Sentinel HL key. If a Sentinel HL key is detected, Sentinel LDK protection is used. If a Sentinel HL key is not detected, the software attempts to log in to a Sentinel key. If a Sentinel key is detected, Sentinel Keys protection is used.

During the period that your application supports both Sentinel Hardware Keys and Sentinel LDK, you are imposing an additional workload on your development and support departments. Therefore, an important objective during this stage is to provide incentive for your customers to switch from Sentinel Hardware Keys to Sentinel LDK. One way of accomplishing this is to protect new features in your application using only Sentinel HL keys. Customers that want to use the new features will be required to switch to Sentinel HL keys.

The following flowchart shows the sequential flow when the protected software executes in Stage 1:



Implementing Stage 1

The following procedure details the steps required to implement Stage 1 of the Sentinel Keys-to-Sentinel LDK migration process. Where relevant, you are pointed to additional information in the *Sentinel LDK Software Protection and Licensing Guide*.

To implement both Sentinel LDK and Sentinel Keys functionality:

1. If you have not already done so, install Sentinel Vendor Suite and Sentinel LDK-EMS, and introduce your Sentinel Vendor keys. As part of the Vendor key introduction process, Sentinel LDK generates customized Sentinel Licensing API libraries for your Vendor Code.
(For more information, see the *Sentinel LDK Installation Guide*.)
2. For customers who will receive a Sentinel HL network key: Prepare a Sentinel LDK RTE Installer. Your customers must install the Run-time Environment on the computer where they connect the Sentinel HL network key.
(See *Sentinel LDK Software Protection and Licensing Guide*, chapter “Distributing Sentinel LDK with your Software”.)
3. Include your Sentinel Licensing API header files in your project. Do **not** remove included Sentinel Keys headers.
(See *Sentinel LDK Software Protection and Licensing Guide*, chapter “Sentinel Licensing API Protection.”)
4. To enable your software to work with Sentinel Keys or Sentinel LDK protection, implement the decision tree on page 9 of this document, as follows:
 - a. Use the Sentinel Licensing API to log in to a Sentinel protection key. If the login is successful, Sentinel LDK protection is invoked.
(For information on Licensing API functions, see the online help for Sentinel Licensing API.)
 - b. If the login to Sentinel LDK fails, log in using Sentinel Keys functionality. If the Sentinel Keys login is successful, Sentinel Keys protection is invoked.
 - c. If the Sentinel Keys “GetLicense” call fails, the behavior of the application when no key is detected is invoked.

NOTE: You can optionally enhance the security of selected items in your application by protecting them using Sentinel LDK Envelope and using the encryption functions available in the Sentinel Licensing API. For maximum security, any file you choose to protect using the Sentinel Licensing API, including a DLL, should also be protected using Sentinel LDK Envelope. You can also protect code snippets and other data using the API. These protected items will only be accessible when a Sentinel HL key is connected. (By protecting new functionality with Sentinel LDK only, you can provide incentive to existing customers to switch to Sentinel HL keys.)

IMPORTANT: For binaries that implement licensing APIs for Sentinel Hardware Keys and Sentinel HL keys, do not use Envelope protection, as this type of protection loads first, and only works with Sentinel HL keys.

5. Supply all new customers with Sentinel HL keys. Only these customers can access modules protected with Sentinel LDK.
6. Gradually replace your install base of Sentinel keys with Sentinel HL keys, at your convenience.

Stage 2: Full Implementation of Advanced Sentinel LDK Functionality

Stage 2 enables you to fully implement the functionalities of the Sentinel LDK system, thus gaining the benefit of its advanced business logic. After you implement full Sentinel LDK protection, all customers using this version of your software must use Sentinel HL keys.

Implementing Stage 2

The following procedure details the steps required to implement Stage 2 of the Sentinel Keys-to-Sentinel LDK migration process. Where relevant, you are pointed to additional information in the *Sentinel LDK Software Protection and Licensing Guide*.

To implement advanced Sentinel LDK functionality:

1. If you have not already implemented Stage 1, perform steps 1-3 of Stage 1 in order to complete the following:
 - a. Install Sentinel Vendor Suite and Sentinel LDK-EMS, and introduce your Sentinel Vendor keys. As part of the Sentinel Vendor key introduction process, Sentinel LDK generates customized Sentinel Licensing API libraries for your Vendor Code.
(For more information, see the *Sentinel LDK Installation Guide*.)
 - b. Link the Sentinel Licensing API library to the application to be protected.
2. For customers who will receive a Sentinel HL network key: Prepare a Sentinel LDK RTE Installer. Your customers must install the Run-time Environment on the computer where they connect the Sentinel HL network key.
(See *Sentinel LDK Software Protection and Licensing Guide*, chapter “Distributing Sentinel LDK with your Software”.)
3. Replace all calls to Sentinel Keys in the code with calls to Sentinel HL keys.
See “Table 3: Comparison of Sentinel Hardware Key API Functions and Sentinel Licensing API Functions” on page 17 for a list of Sentinel Keys functions and their Sentinel LDK equivalents.
(For information on Licensing API functions, see the online help for Sentinel Licensing API.)
4. Protect your software using Sentinel LDK Envelope.
(See *Sentinel LDK Software Protection and Licensing Guide*, chapter “Sentinel LDK Envelope Protection.”)
5. Follow the instructions in the *Sentinel LDK Software Protection and Licensing Guide* to distribute your software.
(See *Sentinel LDK Software Protection and Licensing Guide*, chapter “Distributing Sentinel LDK with Your Software.”)
6. Ensure that all customers who receive the Sentinel LDK-protected software also receive Sentinel HL keys.

CHAPTER 2: Migration Path 2—Gradual Migration from Sentinel Keys to Sentinel LDK Using a Launcher Application

This migration path enables you to phase out your installation base of Sentinel Hardware Keys—without necessitating the recall and replacement of the keys, and without having to continue their distribution.

The migration is achieved by creating two versions of your software—one protected using Sentinel Keys, and the other protected using Sentinel LDK Envelope. The two versions of the software are bundled with a launcher application. If the launcher detects that a Sentinel HL key is accessed, the Sentinel LDK Envelope-protected version of your software is launched. If a Sentinel HL key is not detected, the Sentinel Keys-protected version of your software is launched.

This migration path enables you to support existing users who already have Sentinel Keys, and to provide new users with the added protection available with Sentinel protection keys.

When you are ready to fully switch to Sentinel LDK protection and licensing functionality, many of your users will already be using Sentinel protection keys.

The following table summarizes the two stages for Migration Path 2.

| | Stage1 | Stage 2 |
|---|---|--|
| Implementation effort | Low | Medium |
| Install base | Remains Sentinel Hardware Keys | Replace with Sentinel HL key |
| Keys for new customers | Sentinel HL (Driverless configuration) key | Sentinel HL (Driverless configuration) key |
| Protection process | <ul style="list-style-type: none"> • Create two binaries – one protected using Sentinel Keys, the other using Sentinel LDK Envelope • Create a launcher application using the Sentinel Licensing API to search for a Sentinel protection key • Switch between above binaries, depending on connected key | <ul style="list-style-type: none"> • Remove Sentinel Keys implementation • Implement Sentinel Licensing API in your code and protect using Sentinel LDK Envelope |
| Security level | Same as Sentinel Keys only | Very high |
| Flexibility level (licensing, portability) | Medium | Very high |
| Additional benefits | Driverless deployment | Driverless deployment |

Stage 1: Initial Implementation of Sentinel LDK Functionality

During Stage 1 of the migration process, you create two versions of your software—one protected using Sentinel Keys, and the other protected using Sentinel LDK Envelope. The two versions of the software are bundled with a launcher application. The launcher application detects which version of your software to use.

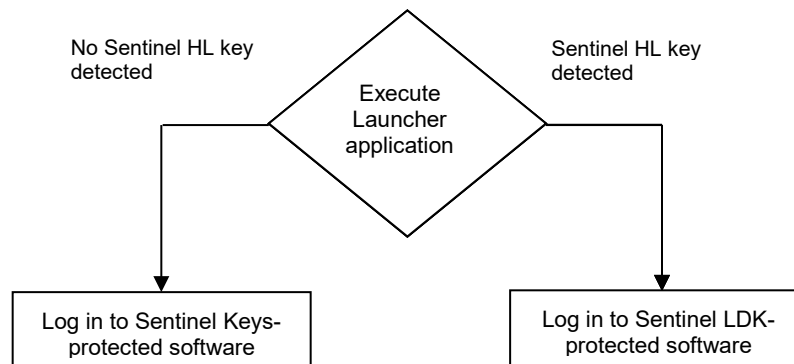
Implementing Stage 1

The following procedure details the steps required to implement the Sentinel Keys-to-Sentinel LDK migration process. Where relevant, you are pointed to additional information in the Sentinel LDK documentation.

To implement Sentinel LDK functionality:

1. If you have not already done so, install Sentinel Vendor Suite and Sentinel LDK-EMS, and introduce your Sentinel Vendor keys.
(For more information, see the *Sentinel LDK Installation Guide*.)
2. Create a version of your software (for example, `program_shk.exe`) and implement Sentinel Keys protection using the Sentinel Shell, Sentinel API, or both.
3. Create a version of your software (for example, `program_hasp.exe`) and implement Sentinel LDK protection, using Sentinel LDK Envelope, Sentinel Licensing API, or both.
4. Create a launcher application using the Sentinel Licensing API that will detect whether a Sentinel protection key is accessible. Program the following behavior:
 - a. If a Sentinel protection key is detected, the launcher launches `program_hasp.exe`.
 - b. If a Sentinel protection key is not detected, the launcher launches `program_shk.exe`.
5. Package both versions of the software with the launcher application.
6. For customers who will receive a Sentinel HL network key: Prepare a Sentinel LDK RTE Installer. Your customers must install the Run-time Environment on the computer where they connect the Sentinel HL network key.
(See *Sentinel LDK Software Protection and Licensing Guide*, chapter “Distributing Sentinel LDK with your Software”.)
7. Follow the instructions in the *Sentinel LDK Software Protection and Licensing Guide* to distribute your software.
(See *Sentinel LDK Software Protection and Licensing Guide*, chapter “Distributing Sentinel LDK with Your Software.”)
8. Ensure that all customers who receive the Sentinel LDK-protected software also receive Sentinel HL keys.

The following flowchart shows the flow when the application launcher executes:



Stage 2: Full Implementation of Sentinel LDK Functionality

Stage 2 enables you to fully implement the functionalities of the Sentinel LDK system, thus gaining the benefit of its advanced business logic. After you implement full Sentinel LDK protection, all customers using this version of your software must use Sentinel protection keys.

Implementing Stage 2

The following procedure details the steps required to implement Stage 2 of the Sentinel Keys-to-Sentinel LDK migration process. Where relevant, you are pointed to additional information in the Sentinel LDK documentation.

To implement full Sentinel LDK functionality:

1. Replace all calls to Sentinel Keys in the code with calls to Sentinel HL keys.
See “Table 3: Comparison of Sentinel Hardware Key API Functions and Sentinel Licensing API Functions” on page 17 for a list of Sentinel Keys functions and their Sentinel LDK equivalents.
(For information on Licensing API functions, see the online help for Sentinel Licensing API.)
2. Protect your software using Sentinel LDK Envelope.
(See Sentinel LDK Software Protection and Licensing Guide, chapter “Sentinel LDK Envelope Protection.”)
3. Follow the instructions in the *Sentinel LDK Software Protection and Licensing Guide* to distribute your software.
(See *Sentinel LDK Software Protection and Licensing Guide*, chapter “Distributing Sentinel LDK with Your Software.”)
4. For customers who will receive a Sentinel HL network key: Prepare a Sentinel LDK RTE Installer. Your customers must install the Run-time Environment on the computer where they connect the Sentinel HL network key.
(See *Sentinel LDK Software Protection and Licensing Guide*, chapter “Distributing Sentinel LDK with your Software.”)
5. Ensure that all customers who receive the Sentinel LDK-protected software also receive Sentinel protection keys.

APPENDIX A: Sentinel LDK and Sentinel Hardware Keys Comparison Tables

Table 1: Comparison of Sentinel HL Keys and Sentinel Hardware Keys

| Model Type | Sentinel HL | Sentinel Hardware Keys |
|--|---|---|
| Basic <ul style="list-style-type: none"> ◆ No read/write memory functionality ◆ Perpetual license ◆ Locally connected key | Sentinel HL (Driverless configuration) Basic | None |
| Memory <ul style="list-style-type: none"> ◆ Read/write and read-only memory ◆ Locally connected key | Sentinel HL (Driverless configuration) Pro <ul style="list-style-type: none"> ◆ 112 bytes R/W + 112 bytes ROM Sentinel HL (Driverless configuration) Max <ul style="list-style-type: none"> ◆ 4 KB R/W + 2 KB ROM | Sentinel S <ul style="list-style-type: none"> ◆ 8 KB (1.75 KB accessible) Sentinel X <ul style="list-style-type: none"> ◆ 12 KB accessible |
| Time <ul style="list-style-type: none"> ◆ Real-time clock ◆ Read/write and read-only memory ◆ Locally connected key | Sentinel HL (Driverless configuration) Time <ul style="list-style-type: none"> ◆ RTC ◆ 4 KB R/W + 2 KB ROM | Sentinel ST <ul style="list-style-type: none"> ◆ RTC ◆ 8 KB (1.75 KB accessible) |
| Net <ul style="list-style-type: none"> ◆ Read/write and read-only memory ◆ Network-based licensing | Sentinel HL (Driverless configuration) Net <ul style="list-style-type: none"> ◆ 4 KB R/W + 2 KB ROM ◆ Max no. of concurrent users: 10, 50, 250+ Sentinel HL (Driverless configuration) key with concurrency license – any key other than Basic. | Sentinel SNT <ul style="list-style-type: none"> ◆ 8 KB (1.75 KB accessible) ◆ Max no. of concurrent users: 3, 5, 10, 25, 50, 100, 250 |
| Net and Time <ul style="list-style-type: none"> ◆ Real-time clock ◆ Read/write and read-only memory ◆ Network-based licensing | Sentinel HL (Driverless configuration) NetTime <ul style="list-style-type: none"> ◆ RTC ◆ 4 KB R/W + 2 KB ROM ◆ Max no. of concurrent users: 10, 50, 250 Sentinel HL (Driverless configuration) Time with concurrency license <ul style="list-style-type: none"> ◆ RTC 4 KB R/W + 2 KB ROM | Sentinel SN <ul style="list-style-type: none"> ◆ RTC ◆ 8 KB (1.75 KB accessible) ◆ Max no. of concurrent users: 3, 5, 10, 25, 50, 100, 250 |

| Model Type | Sentinel HL | Sentinel Hardware Keys |
|--|---|------------------------|
| Drive <ul style="list-style-type: none"> ◆ Read/write and read-only memory ◆ Extended mass storage | Sentinel HL (Driverless configuration) Drive <ul style="list-style-type: none"> ◆ 4 KB R/W + 2 KB ROM ◆ 2 GB or 4 GB USB Mass Storage drive | None |
| Vendor Site Production Key | Sentinel Master Key | Sentinel I |
| Vendor Site Development Key | Sentinel Developer Key | Sentinel I |
| Distribution Site Production Key | Channel Partner functionality in Sentinel LDK v.6.1 and later | Sentinel D |

For more specification data regarding Sentinel HL keys, see the *Sentinel HL Data Sheet*.

Table 2: Sentinel Keys and Sentinel LDK Tool Equivalents

| Sentinel Keys Tools | Sentinel LDK Tools |
|--|--|
| Encoding Sentinel keys | Keys are pre-encoded at the Thales production site. Use your unique Vendor Code (stored in the Sentinel Vendor keys) |
| Sentinel Keys ToolKit | Sentinel Vendor Suite |
| Shell or Cover Code | Sentinel LDK Envelope (part of Sentinel Vendor Suite) |
| License Manager | Sentinel LDK-EMS (part of Sentinel Vendor Suite) |
| API Explorer | Sentinel LDK ToolBox (part of Sentinel Vendor Suite) |
| Sentinel Protection installer | Sentinel LDK Run-time Environment installer |
| Sentinel System Driver (legacy) | Sentinel LDK Run-time Environment installer |
| Sentinel Keys Server (legacy) | Sentinel LDK Run-time Environment installer |
| Sentinel Keys License Monitor (previously SuperPro Monitoring Tool and UltraPro License Monitor) | Sentinel Admin Control Center (part of the Sentinel LDK Run-time Environment) |
| SafeNet Sentinel Medic | Sentinel Admin Control Center (part of the Sentinel LDK Run-time Environment) |
| Secure Update utility | Sentinel Remote Update System (RUS) |
| Serial number | HASP ID |

Table 3: Comparison of Sentinel Hardware Key API Functions and Sentinel Licensing API Functions

| Sentinel Hardware Key API Function* | Sentinel Licensing API Function |
|--|--|
| SFNTCounterDecrement() | Not required in Sentinel LDK—performed automatically by hasp_login() when logging in to Features with execution counters. |
| SFNTDecrypt() | hasp_decrypt() |
| SFNTEncrypt() | hasp_encrypt() |
| SFNTSetContactServer() | Not required in Sentinel LDK—performed automatically by hasp_login(). Logging in to a specific server is possible using hasp_login_scope(). |
| SFNTGetLicense() | hasp_login() |
| SFNTGetFeatureInfo() | hasp_get_info() |
| SFNTGetLicenseInfo() | hasp_get_info() |
| SFNTQueryFeature() | Not required in Sentinel LDK—performed automatically by hasp_login(). Note: The SFNTQueryFeature function is implemented by a proprietary algorithm based on AES. If you want to implement a similar mechanism, you can replace the query/response table with a similar table generated using hasp_decrypt/hasp_encrypt. |
| SFNTEnumServer() | Not required in Sentinel LDK—performed automatically by hasp_login(). Logging in to a specific server is possible using hasp_login_scope(). |
| SFNTReadInteger() | hasp_read() |
| SFNTReadRawData() | hasp_read() |
| SFNTReadString() | hasp_read() |
| SFNTGetServerInfo() | hasp_get_sessioninfo() |
| SFNTReleaseLicense() | hasp_logout() |
| SFNTSetHeartbeat() | Not required in Sentinel LDK. |
| SFNTGetDeviceInfo() | hasp_get_info() or hasp_get_sessioninfo() |
| SFNTSign() | Not required in Sentinel LDK. |
| SFNTVerify() | Not required in Sentinel LDK. |
| SFNTWriteInteger() | hasp_write() |
| SFNTReadRawData() | hasp_write() |
| SFNTWriteRawData() | hasp_write() |
| SFNTWriteString() | hasp_write() |
| SFNTSetConfigFile() (added in Sentinel Hardware Keys version 1.3.0) | Run-time Environment configuration can be performed using the Admin Control Center user interface. The location of the configuration file is not modifiable. The file path is typically Program Files\Common Files\Aladdin Shared\HASP\hasplm.ini . |

* Sentinel functions that are not listed are obsolete.