THALES

SENTINEL LDK

MIGRATION GUIDE: HARDLOCK TO SENTINEL LDK

Trademarks, Copyrights, and Third-Party Software

Disclaimer

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.

Product Version: 8.3 and later

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

CONTENTS

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-based 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

This guide is intended for Hardlock users who wish to continue using a hardware-based protection solution, but who want to migrate to the improved Sentinel HL key protection and advanced licensing options provided by Sentinel LDK.

Note: If you want to implement Sentinel LDK software-based protection, refer to the Sentinel LDK Software Protection and Licensing Guide.

The guide assumes that the reader has a good understanding of both the Hardlock and the Sentinel LDK systems. It provides the following:

- An overview and guidelines for a two-stage migration path from Hardlock to Sentinel LDK, starting with an install base consisting only of Hardlock keys
- Procedures relating to the migration that are not documented in either the Hardlock documentation, or the *Sentinel LDK Software Protection and Licensing Guide*, and Help documentation
- Tables that list the tools and functionalities of Hardlock and their counterparts in Sentinel LDK

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

For detailed information and procedures relating to Hardlock, refer to the relevant Hardlock documentation.

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 Sentinel 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*.

Shortcut to Enhanced Protection

Sentinel SL “Unlocked Product” 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 Hardlock 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 Products, see the *Sentinel LDK Software Protection and Licensing Guide*. For pricing information for Unlocked Products, 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 Complementing Hardlock Implementation

Overview

This three-stage migration path enables you to improve your security in a very short time by protecting your applications with Sentinel LDK Envelope, and locking the application to a software-based Sentinel SL key. Two alternative methods to accomplish this locking are described in this section.

Stage 2 presents an opportunity for you to enhance your existing Hardlock protection. While maintaining your trusted current protection, you have only to add Sentinel LDK as a complementary system. With this gradual change from Hardlock to Sentinel LDK, the entire installation base is not forced to change all at once. While your customers adjust to Sentinel LDK protection, you can easily transition to Stage 3, which offers a much higher level of security and provides more portability. Stage 3 is ideal for new customers or when distributing new versions of your software.

The time that you wait before moving from one stage to the next is entirely at your discretion. You can even skip Stage 2 and proceed directly to Stage 3.

The following table summarizes the stages for Migration Path 1.

	Stage 1	Stage 2	Stage 3
Implementation effort	Very low	Very low	Medium
Install base	Remains Hardlock keys	Remains Hardlock and Sentinel HL (Hardlock configuration) keys	• Replace Hardlock keys with Sentinel HL keys • Upgrade deployed Sentinel HL (Hardlock configuration) keys to Sentinel HL (Driverless configuration) keys
Keys for new customers	Sentinel HL (Hardlock configuration) keys	HASP SL AdminMode and Sentinel HL (Hardlock configuration) keys	Sentinel HL (Driverless configuration) keys
Protection process	• No change to code. Software remains protected with Hardlock.	• Keep Hardlock implementation • Protect using Sentinel LDK Envelope	• Remove Hardlock implementation • Implement Sentinel Licensing API in your code and protect using Sentinel LDK Envelope
Security level	Hardlock security	Improved	Very high
Flexibility level (licensing, portability)	Low	Low	Very high
Additional benefits	Sentinel HL keys received by new customers will not have to be replaced at later stages.	Sentinel HL keys received by new customers will not have to be replaced at later stages.	Driverless deployment

Stage 1: Using Sentinel HL keys as Hardlock keys

Sentinel HL (Hardlock configuration) keys are fully compatible with Hardlock keys, so that your software can work with either key. At this initial stage, it is not necessary to make any changes to your software or drivers. This enables you to start to ship Sentinel HL (Hardlock configuration) keys to your customers and gradually replace your install base of Hardlock keys with Sentinel HL (Hardlock configuration) keys at your convenience.

When you decide to move to Stage 3 of the migration process and protect your software with Sentinel LDK, all the deployed Sentinel HL (Hardlock configuration) keys can easily be upgraded to Sentinel HL (Driverless configuration) keys.

Proceed as follows:

1. Leave your install base with the Hardlock keys that they are currently using.
2. Start distributing Sentinel HL (Hardlock configuration) keys with new purchases. At this stage you do not need to make any changes to your software, which remains protected by Hardlock security.

Stage 2: Initial Implementation of Sentinel LDK Functionality

Stage 2 enables you to easily implement basic functionality of the Sentinel LDK system, while retaining Hardlock keys and Sentinel HL (Hardlock configuration) keys as your installation base. By supplying your customers with a Sentinel SL key with their Sentinel HL (Hardlock configuration) key, they gain increased security and licensing capabilities.

Sentinel SL Locking Alternatives

In this stage, you enhance the security of your application by protecting it with Sentinel LDK Envelope and licensing the application with a software-based Sentinel SL key.

Two methods are available to license the application, and each method provides different benefits:

> Locked Product

With this method, you lock the protected application to a Sentinel SL key that requires activation on each end user's computer. The activation process can be performed manually (using software utilities), or automatically via the Sentinel Licensing API and Sentinel LDK-EMS Web Services.

The manual approach deploys quickly since no additional code must be written. However, it may be less convenient when dealing with larger installation bases. In such cases, it may be preferable to choose automatic activation, which will require integration of the APIs.

The end result is that the protected application is a *Locked Product*; that is, the application is locked to a specific Sentinel SL key that, in turn, is locked to a specific machine.

This method is especially appropriate if your ultimate goal is to migrate to Sentinel SL protection.

> Unlocked Product

With this method, you lock the protected application to an unlocked Sentinel SL key that does not require activation.

The end result is that the protected application is an *Unlocked Product*; that is, the application is protected against disassembly by Sentinel LDK Envelope. However, licensing continues to be provided only by Hardlock.

This method is much simpler to implement than the Locked Product method; this method is especially appropriate if your ultimate goal is to migrate to Sentinel HL protection.

You may have already implemented this method for your application. For more information, see “Shortcut to Enhanced Protection” on page 7.

During this stage of the migration procedure, you choose which of the Sentinel SL locking alternatives you want to implement.

Implementing Stage 2

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

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. Using Sentinel LDK-EMS, create the following:

   a. A Feature that represents the protected application

   b. A Base Product containing the Feature you created, with licensing terms stating that the license is perpetual.

   c. A Sentinel LDK Run-time Environment (RTE) Installer

3. Integrate the Sentinel LDK RTE Installer into your application.

   (See *Sentinel LDK Software Protection and Licensing Guide*, chapter “Distributing Sentinel LDK with Your Software.”)

4. Protect your program using the Hardlock API, but do not implement Espresso Shell protection.

5. Use Sentinel LDK Envelope to protect your program.

6. Distribute a Sentinel HL (Hardlock configuration) key with each copy of your software.

7. Use one of the methods that follow to implement SL Locking. (For more information, see “Sentinel SL Locking Alternatives” on page 10.)

   Locked Product method:

   a. In Sentinel LDK-EMS, create and execute a Product Key-based entitlement for each customer. Sentinel LDK-EMS generates an email notification to each customer.

   b. The customer clicks the link provided in the email notification to access the Customer Portal and activate their license for the protected application.

   Note: Steps **a** and **b** can be performed using Sentinel LDK-EMS Web Services.

   Unlocked Product method:

   a. In the Sentinel LDK-EMS Catalog, create an Unlocked (Perpetual) Product for your protected application.

   b. In Sentinel LDK-EMS, create a bundle that contains the Unlocked Product, and then create an RTE Installer that contains the bundle.

   c. Include the RTE Installer in your application installation procedure. The Unlocked Product is installed together with the protected application.

Stage 3: Full Implementation of Advanced Sentinel LDK Functionality

Stage 3 enables you to fully implement the advanced functionalities of the Sentinel LDK system, thus gaining the benefit of its increased security and licensing capabilities. After you implement full Sentinel LDK protection, all customers using this version of your software must use Sentinel HL (Driverless configuration) keys.

Implementing Stage 3

The following procedure details the steps required to implement Stage 3 of the Sentinel Hardlock-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 2, perform steps 1–3 of Stage 2 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 that is 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 Hardlock in the code with calls to Sentinel HL keys.
   For a list of Hardlock functions and their Sentinel LDK equivalents, see Table 4: Comparison of Hardlock API and Sentinel Licensing API Functions on page 25.

   (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. Generate a Sentinel LDK Hardlock-to-Driverless Upgrade Tool. This tool will upgrade Sentinel HL (Hardlock configuration) keys at the customer site to Sentinel HL (Driverless configuration) keys. For more information, see the readme file in your Sentinel LDK installation, in the directory:

   %ProgramFiles(x86)%\Thales\Sentinel LDK\Vendor Tools\Utilities\Sentinel HL Hardlock to Driverless Upgrade Tool

   (For x86 machines: **%ProgramFiles%\...)**
6. 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.”)

7. Ensure that all customers who receive the Sentinel LDK-protected software also receive Sentinel HL (Driverless configuration) keys.

CHAPTER 2: Migration Path 2— Gradual Migration from Hardlock to Sentinel LDK

This two-stage migration path enables you to improve your security and expand your licensing options by gradually implementing Sentinel LDK capabilities. The time that you wait before moving from one stage to the next is entirely at your discretion. You can also proceed directly to Stage 2.

The following table summarizes the two-stage migration path.

	Stage 1	Stage 2
Implementation effort	Low	Medium
Install base	Remains Hardlock	• Replace with Sentinel HL (Driverless configuration) keys
Keys for new customers	• Sentinel HL (Driverless configuration) keys	• Sentinel HL (Driverless configuration) keys
Protection process	• Retain Hardlock API • Add Sentinel Licensing API in your code	• Implement the Sentinel Licensing API in your code and protect using Sentinel LDK Envelope
Security level	Same as Hardlock only	Very high
Additional benefits	Sentinel HL keys received by new customers will not have to be replaced at later stages.	Driverless deployment

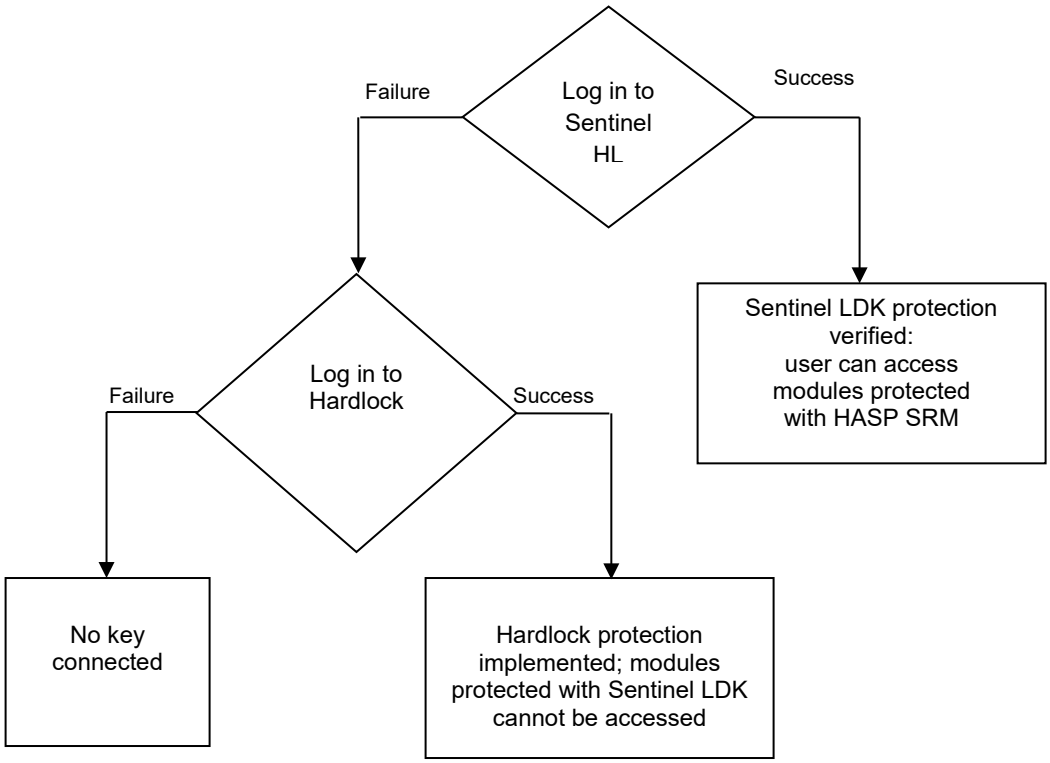
Stage 1: Combining Hardlock Protection with Sentinel LDK Protection

Stage 1 enables you to phase out your install base of Hardlock keys over a period of time, without necessitating immediate recall and replacement of the Hardlock keys. To achieve this, you create a version of your software that is able to identify both Hardlock and Sentinel HL keys. This could be a new version of your software, or the current version, 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 Hardlock keys.

When the software runs, it tries to log into a Sentinel HL key. If a Sentinel HL key is found, Sentinel LDK protection is implemented. If no Sentinel HL key is found, the software then tries to log into a Hardlock key. If a Hardlock key is found, Hardlock protection is implemented.

In order to maximize security and implement the higher level of protection provided by Sentinel LDK concurrently with Hardlock protection of your software, you can protect selected files or modules with Sentinel LDK. Sentinel LDK-protected items will have greater security than those only protected by Hardlock. The Sentinel LDK-protected items can only be activated with a Sentinel HL key. In this case, if a Hardlock key is used, the modules protected with Hardlock will function, but modules protected with Sentinel LDK will not run.

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



Implementing Stage 1

The following procedure details the steps you take in order to implement Stage 1 of the Hardlock-to-Sentinel LDK migration process. Where relevant, you are pointed to additional information in the Sentinel LDK documentation.

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.

   (See the *Sentinel LDK Installation Guide*.)

2. Integrate the Sentinel LDK Run-time Environment as part of your application setup.

   (See Sentinel LDK Software Protection and Licensing Guide, chapter Distributing Sentinel LDK with Your Software.)

3. Link the customized Sentinel Run-time API libraries to the protected files as follows:

   - If you link to your customized Sentinel Licensing API `.lib` files, remove the existing link to the Hardlock library files. The Sentinel Licensing API `.lib` files contain both Sentinel LDK and Hardlock functionalities.
   - The legacy Hardlock API files are not required for static linkage (LIB). However, for dynamic linkage, the legacy Hardlock DLL files are still required. (The DLL of the Licensing API in Sentinel LDK v.7.1 does *not* contain backwards compatibility to Hardlock functions.)
   - If you link to your customized Sentinel Licensing API `.dll` files, do **not** remove the link to the Hardlock library files.
   - Include your customized Sentinel Licensing API header files in your project. Do **not** remove included Hardlock headers.

   (See Sentinel LDK Software Protection and Licensing Guide, chapter Sentinel Licensing API Protection.)

4. To enable your software to work with Hardlock or Sentinel LDK protection, implement the decision tree on page 15 of this document, as follows:

   a. Use the Sentinel Licensing API to log in to a key. If the login is successful, Sentinel LDK protection is invoked.

      (See Sentinel LDK Software Protection and Licensing Guide, chapter Sentinel Licensing API Protection.)

   b. If the login to Sentinel LDK fails, log in using Hardlock functionality. If the Hardlock login is successful, Hardlock protection is invoked.

   c. If the login to Hardlock fails, the behavior of the application when no key is connected is invoked.

   Note: You can optionally enhance the security of selected items in your software by protecting them with Sentinel LDK. You can protect individual files using Sentinel LDK Envelope or Sentinel Licensing API. You can protect code snippets and other data using the Sentinel Licensing API. These protected items are only accessible when a Sentinel HL key is connected.

   Important: For binaries that implement licensing APIs for Hardlock 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 (Driverless configuration) keys. Only customers with Sentinel HL keys can access modules protected with Sentinel LDK.

6. Gradually replace your install base of Hardlock keys with Sentinel HL keys, at your convenience.

Stage 2: Full Implementation of Advanced Sentinel LDK Functionality

This stage enables you to fully implement the advanced functionalities of the Sentinel LDK system, and gain the benefit of its increased security and licensing capabilities. After you implement full Sentinel LDK protection, all customers using this version of your software must use Sentinel HL keys.

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

Implementing Stage 2

Fully implement the advanced Sentinel Licensing API by integrating Sentinel LDK functionalities into your code.

1. If you have not carried out Stage 1, implement steps 1-3 of Stage 1 in order to complete the following:
   a. Install Sentinel Vendor Suite and Sentinel LDK-EMS, and introduce your Vendor keys.
   b. Link the Sentinel Licensing API library to the protected files.
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 in the code to Hardlock with calls to Sentinel LDK. Refer to Table 4: Comparison of Hardlock API and Sentinel Licensing API Functions on page 25 for a list of Hardlock functions and their Sentinel LDK counterparts.
4. Protect the 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 the chapter Distributing Sentinel LDK with Your Software).
6. Ensure that all customers who receive the Sentinel LDK-protected software also receive Sentinel HL (Driverless configuration) keys.

CHAPTER 3: Migration Path 3— Gradual Migration from Hardlock to Sentinel LDK Using a Launcher Application

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

The migration is achieved by creating two versions of your software—one protected using Hardlock Espresso, 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 protection key is accessed, the Sentinel LDK Envelope-protected version of your software is launched. If a Sentinel protection key is not detected, the Hardlock Espresso-protected version of your software is launched.

This migration path enables you to support existing users who already have Hardlock 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 3.

	Stage 1	Stage 2
Implementation effort	Low	Medium
Install base	Remains Hardlock	• Replace with Sentinel HL (Driverless configuration) keys
Keys for new customers	• Sentinel HL (Driverless configuration) key	• Sentinel HL (Driverless configuration) keys
Protection process	• Create two binaries – one protected using Hardlock Espresso, 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.	• Remove Hardlock implementation. • Implement the Sentinel Licensing API in your code and protect using Sentinel LDK Envelope.
Security level	Same as Hardlock Express only	Very high
Flexibility level	Medium-high	Very high
Additional benefits	Sentinel HL keys received by new customers will not have to be replaced at later stages.	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 Hardlock Espresso, 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 Hardlock Espresso-to-Sentinel LDK migration process. Where relevant, you are pointed to additional information in the Sentinel LDK documentation.

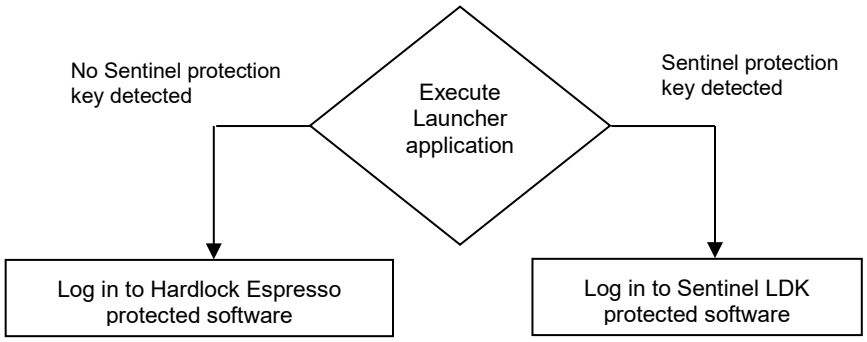
To implement Sentinel LDK functionality:

1. If you have not already done so, install Sentinel Vendor Suite and Sentinel LDK-EMS, and introduce your Sentinel Vendor keys.

   (See the Sentinel LDK Installation Guide.)

2. Create a version of your software (for example, `program_hardlock.exe`) and implement protection using Hardlock Espresso and/or the Hardlock API.
3. Integrate the Sentinel LDK Run-time Environment as part of your application setup. (The Run-time Environment is only required if customers will be using Sentinel HL network keys.
4. Create a version of your software (for example, `program_haspsrm.exe`) and implement Sentinel LDK protection, using Sentinel LDK Envelope and/or the Sentinel Licensing API.
5. Create a launcher application using the Sentinel Licensing API that will detect whether a Sentinel LDK protection key is accessible. Program the following behavior:
   - If a Sentinel protection key is detected, the launcher launches program_haspsrm.exe.
   - If a Sentinel protection key is not detected, the launcher launches program_hardlock.exe.
6. Package both versions of the software with the launcher application.
7. Follow the instructions in the Sentinel LDK Software Protection and Licensing Guide to distribute your software (see the chapter Distributing Sentinel LDK with your Software).
8. Ensure that all customers who receive the Sentinel LDK-protected software also receive Sentinel HL (Driverless configuration) 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 increased security and licensing capabilities. 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 Hardlock-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. If you have a Hardlock API, replace all calls to Hardlock in the code with calls to Sentinel protection keys. See Table 4: Comparison of Hardlock API and Sentinel Licensing API Functions on page 25 for a list of Hardlock functions and their Sentinel LDK equivalents.
2. Protect your software using Sentinel LDK Envelope.

   (See Sentinel LDK Software Protection and Licensing Guide, chapter Sentinel LDK Envelope Protection.)
3. For customers who will receive a Sentinel HL Net key or 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”.)
4. Follow the instructions in the *Sentinel LDK Software Protection and Licensing Guide* to distribute your software (see chapter “Distributing Sentinel LDK with your Software”).
5. Ensure that all customers who receive the Sentinel LDK-protected software also receive Sentinel HL (Driverless configuration) keys.

APPENDIX A: Sentinel LDK and Hardlock Comparison Tables

Table 1: Comparison of Hardlock and Sentinel HL Keys

Hardlock		Sentinel HL (LDK)	
Key Type	**Memory Size**	**Key Type**	**Memory Size**
EYE, Twin	–	Basic	–
EYE, Twin with memory	32 Bytes R/W 96 Bytes ROM	Sentinel HL Pro	112 Bytes backward-compatible memory* 112 Bytes Read/Write memory 112 Bytes ROM
		Sentinel HL Max	4 KB backward-compatible memory* 4 KB Read/Write memory 2 KB ROM
–	–	Sentinel HL Time	4 KB backward-compatible memory* 4 KB Read/Write memory 2 KB ROM
–	–	Sentinel HL Drive	2 GB / 4 GB Flash memory 4 KB backward-compatible memory* 4 KB Read/Write memory 2 KB ROM
HL-Server	32 Bytes R/W 96 Bytes ROM	Sentinel HL Net	4 KB backward-compatible memory* 4 KB Read/Write memory 2 KB ROM
		Sentinel HL (Driverless configuration) – all types except Basic	As described above
–	–	Sentinel HL NetTime	4 KB backward-compatible memory* 4 KB Read/Write memory 2 KB ROM

*Backward-compatible memory is available in HASP configuration only.

Table 2: HL-Server Keys and Equivalent Sentinel Network Keys

HL-Server	Sentinel HL Net	Sentinel HL NetTime	Sentinel HL (Driverless configuration) key
HL-Server 5	Net 10	NetTime 10	Sentinel HL (Driverless configuration) key other than Basic, with concurrency license
HL-Server 10	Net 10	NetTime 10	
HL-Server 20	Net 50	NetTime 50	
HL-Server 50	Net 50	NetTime 50	
HL-Server 250	Net 250+	NetTime 250+	

Table 3: Hardlock Tools and Functions and their Sentinel LDK Counterparts

Hardlock Tool / Functionality	Sentinel LDK Tool / Functionality
Encoding Hardlock keys	Keys are pre-encoded at the Thales production site. Use your unique Vendor Code (stored in the Sentinel Vendor keys)
Hardlock Bistro	Sentinel Vendor Suite
Espresso	Sentinel LDK Envelope (part of Vendor Suite)
Cappuccino	Sentinel LDK-EMS (part of Vendor Suite)
Latteccino	Sentinel LDK ToolBox (part of Vendor Suite)
Hardlock Driver	Sentinel LDK Run-time Environment
Hardlock Server	Sentinel LDK Run-time Environment
Aladdin Monitor	Sentinel Admin Control Center (part of the Sentinel LDK Run-time Environment)
Aladdin DiagnostiX	Sentinel Admin Control Center (part of the Sentinel LDK Run-time Environment)
`Hlup.exe` (Hardlock upgrade)	Sentinel LDK Remote Update System (RUS)
Read Only memory	Read Only memory
–	Sentinel key unique ID
Cappuccino	
Vendor Key manager	System uses signatures contained in Sentinel Vendor keys
Insert order	Sentinel LDK-EMS – Entitlements
Creating licenses	Sentinel LDK-EMS – Catalog > Products, Entitlements
Programming the memory	Sentinel LDK-EMS – Catalog > Products, or Sentinel LDK ToolBox
Reading the key memory	Sentinel LDK-EMS – Catalog > Products, or Sentinel LDK ToolBox
Programming licenses to a key	Sentinel LDK-EMS – Entitlements
Espresso	
Module address of Demo key	Demo key batch code is DEMOMA
Data Files node – data files filtering	Sentinel LDK Envelope – Enable data file encryption (DataHASP) check box in Protection Details pane
Data File node - data file encryption (`dfcrypt.exe`)	Sentinel LDK Envelope – Encrypt Data button in Protection Details pane
Using HL-RUS in Programs window	Sentinel LDK Envelope – Feature ID in Protection Details pane
Error Messages node	Sentinel LDK Envelope – User Messages pane
Local and network searches	Sentinel LDK Envelope – Protection Key search mode options in Protection Details pane

Hardlock Tool / Functionality	Sentinel LDK Tool / Functionality
Sentinel LDK Run-time Environment	
`hldinst.exe` (command line)	`haspdinst.exe` (command line)
`Hldrv32.exe` (GUI driven)	`HASPUserSetup.exe` (GUI driven)
Driver installation API	Sentinel LDK Run-time Environment
Server, Monitor, DiagnostiX	
`Hlsw32.exe`	Sentinel LDK Run-time Environment
LM application – `hls32.exe`	Sentinel LDK Run-time Environment
LM application (service) – `hls32svc.exe`	Sentinel LDK Run-time Environment
Monitor Setup – `aksmon32.exe`	Sentinel Admin Control Center (part of the Sentinel LDK Run-time Environment)
DiagnostiX Setup – `Diagnostix.exe`	Sentinel Admin Control Center (part of the Sentinel LDK Run-time Environment)

Table 4: Comparison of Hardlock API and Sentinel Licensing API Functions

Hardlock API Function*	Sentinel Licensing API Function
HL_LOGIN()	hasp_login() hasp_login_scope()
HL_LOGOUT()	hasp_logout()
HL_CODE()	hasp_encrypt() hasp_decrypt()
HL_MEMINFO()	hasp_get_sessioninfo() hasp_get_size()
HL_READID()	hasp_get_info()
HL_READ(); HL_READBL()	hasp_read()
HL_WRITE(); HL_WRITEBL()	hasp_write()
HL_PORTINF()	hasp_get_sessioninfo()
HL_ACCINF()	hasp_get_info()
HL_USERINF()	hasp_get_info()
HL_MAXUSER()	hasp_get_info()
HLM_WRITELICENSE()	hasp_update()
HLM_LOGIN()	In Sentinel LDK, hasp_update() does not require hasp_login() or hasp_logout()
HLM_LOGOUT()	
HLM_OCCUPYSLOT()	
HLM_FREESLOT()	
HLM_GETRUSINFO()	hasp_get_info()
HLM_CHECKCOUNTER()	hasp_get_info()
HLM_CHECKEXPDATE()	hasp_get_info()

* Hardlock functions that are not listed are obsolete.

