Sentinel® LDK

Migration Guide
SmartKey to Sentinel LDK

gemalto
security to be free

Product Version: 7.8 and later

Document Part Number: 000-000000-001, Rev. A

Document Build: 1803-1

Release Date: April 2018

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- 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-base 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 migration guide is intended for users of SmartKeys. The guide's main focus is for users who wish to continue using a hardware-based protection solution, but want to migrate to the more comprehensive Sentinel HL key protection and advanced licensing provided by Sentinel LDK. The guide assumes that the reader has a good understanding of both the SmartKey and the Sentinel LDK systems and provides the following:

- Three migration paths from SmartKey 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 SmartKey documentation, or the *Sentinel LDK Software Protection and Licensing Guide*, *Sentinel LDK Installation Guide*, or Help documentation.
- Tables comparing Sentinel LDK and SmartKey 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 SmartKey, refer to the relevant SmartKey documentation.

The procedures and terminology employed in this guide are based on the assumption that you want to migrate from SmartKeys 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 Gemalto 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 Gemalto 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.

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

Three migration paths are available. In Migration Paths 1 and 2, the stages are not interdependent, meaning it is possible to begin at Stage 2. (Note that Stage 2 is identical in both of these migration paths.) Similarly, the time that you wait before moving from one stage to the next is entirely at your discretion.

- **Migration Path 1** provides a gradual move towards improved security for your products in a very short time by merely adding Sentinel LDK as a complementary system to your current protection, and converting to the complete Sentinel LDK protection system at your convenience.

  Using Migration Path 1, you introduce Sentinel LDK alongside your current SmartKey protection, allowing a gradual adjustment at your own pace to the enhanced functionality offered by Sentinel LDK. When you are ready, you can phase SmartKey out and fully implement the superior protection of the Sentinel LDK solution.

  For more information, see Migration Path 1—Sentinel LDK Complementing SmartKey Implementation on page 9.

- **Migration Path 2** provides a way to phase out your installation base of SmartKeys over time—without necessitating the recall and replacement of SmartKeys, and without having to continue their distribution.

  Using Migration Path 2, and creating a version of your software that recognizes both SmartKey and Sentinel HL keys, you can start distributing Sentinel HL keys to new customers while existing customers continue using their SmartKeys. You can then gradually replace your install base of SmartKeys with Sentinel HL keys.

  For more information, see Migration Path 2—Sentinel LDK and SmartKey Combined API Implementation on page 12.

  Simultaneous migration of both paths is possible, to create a three-stage solution of full Sentinel LDK implementation.

  - Implement Stage 1 of Migration Path 1 to add increased security to your current SmartKey protection using Sentinel LDK Envelope. Implementing this stage can provide an immediate solution to SmartKey emulators.
  - Implement Stage 1 of Migration Path 2 for a gradual migration that does not require the distribution of both a Sentinel protection key and a SmartKey. This migration works well in markets that are less prone to piracy.

  Implementation and distribution according to steps 1 and 2 may be performed simultaneously, depending on the requirements of your market.

  - Implement Stage 2 of Migration Path 2 to completely remove SmartKeys and to upgrade to a full implementation of Sentinel LDK protection, utilizing the strongest security and accomplishing the highest licensing flexibility.

- **Migration Path 3** enables a gradual transition from SmartKey GSS to Sentinel LDK. A SmartKey GSS-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 3—Gradual Migration from SmartKey to Sentinel* LDK on page 16.

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 SmartKey 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, Gemalto 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 Gemalto sales representative.

Obtaining Support

You can contact us using any of the following options:

Business Contacts - To find the nearest office or distributor, use the following URL:
https://sentinel.gemalto.com/contact-us-sm/

Technical Support
To obtain assistance in using Gemalto products, feel free to contact our Technical Support team:

- Customer Support Portal (preferred):
  - https://supportportal.gemalto.com/csm?id=sentinel
- Phone:
  - AMER: 800-545-6608 (US toll free), International: +1-410-931-7520
  - EMEA/APAC: https://supportportal.gemalto.com/csm?id=sentinel
    - ⇨ Click “Contact us”
- E-mail (only if you cannot submit the technical issue via the portal)
  - technical.support@gemalto.com

Downloads – To download installers and other updated components using this URL:
http://sentinel.gemalto.com/technical-support-sm/

1 Migration Path 1—Sentinel LDK Complementing SmartKey Implementation

This two-stage migration path enables you to improve your security in a very short time by implementing Sentinel LDK Envelope protection, and locking your protected application to a software-based Sentinel SL key that employs product activation. The activation process can be performed manually (using software utilities), online (using the Sentinel EMS Customer Portal), or automatically via the Sentinel Licensing API and Sentinel Activation APIs. 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.

Stage 1 presents an opportunity for you to enhance your existing SmartKey protection. While maintaining your trusted current protection, you have only to add Sentinel LDK as a complementary system. This gradual change from SmartKey to Sentinel LDK means that 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 2, which offers a much higher level of security and provides more portability. Stage 2 is ideal for new customers and/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 1 and proceed directly to Stage 2.

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

	Stage 1	Stage 2
Implementation effort	Very low	Medium
Install base	Remains SmartKey	Replace with Sentinel HL key
Keys for new customers	Sentinel SL- AdminMode and SmartKey	Sentinel HL (Driverless configuration) key
Protection process	• Keep SmartKey implementation • Protect using Sentinel LDK Envelope	• Remove SmartKey implementation • Implement Sentinel Licensing API in your code, and protect using Sentinel LDK Envelope
Security level	Improved	Very high
Flexibility level (licensing, portability)	Low	Very high
Additional benefits		Driverless deployment

Stage 1: Initial Implementation of Sentinel LDK Functionality

Stage 1 enables you to easily implement basic functionality of the Sentinel LDK system, while retaining SmartKeys as your installation base. By supplying your customers with a Sentinel SL key in addition to their SmartKey, they gain increased security and licensing capabilities.

Implementing Stage 1

The following procedure details the steps required to implement Stage 1 of the SmartKey-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 EMS and Sentinel Vendor Suite and introduce your Sentinel Vendor keys. (See the *Sentinel LDK Installation Guide*.)
2. Using Sentinel 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 SmartKey API, but do not implement GSS protection.
5. Use Sentinel LDK Envelope to protect your program.
6. Continue distributing a SmartKey to new customers with each copy of your software.
7. In Sentinel EMS, create and execute a Product Key-based entitlement for each customer. Sentinel EMS generates an email notification to each customer.
8. The customer clicks the link provided in the email notification to access the Customer Portal and activate their license for the protected application.

Steps 7 and 8 can be performed using the Sentinel Activation API.

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 HL keys.

Implementing Stage 2

The following procedure details the steps required to implement Stage 2 of the SmartKey-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 not already implemented Stage 1, perform steps 1–3 of Stage 1 in order to complete the following:
   a. Install Sentinel Vendor Suite 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.

      (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 SmartKey in the code with calls to Sentinel HL keys.
   See Table 3: *Comparison of SmartKey API Functions and Sentinel Licensing API Functions* on page 21 for a list of SmartKey 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 chapter “Distributing Sentinel LDK with your Software”).
6. Ensure that all customers who receive the Sentinel LDK-protected software also receive Sentinel HL keys.

2

Migration Path 2—Sentinel LDK and SmartKey Combined API Implementation

This two-stage migration path enables you to phase out your installation base of SmartKeys over time, without necessitating immediate recall and replacement of the SmartKeys and without having to continue their distribution. To achieve this status, you create a version of your software that is able to identify both SmartKey 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 SmartKeys.

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 2.

	Stage 1	Stage 2
Implementation effort	Medium	Medium
Install base	Remains SmartKey	Replace with Sentinel HL key
Keys for new customers	Sentinel HL (Driverless configuration) key	Sentinel HL (Driverless configuration) key
Protection process	• Leave SmartKey API implementation • Implement Sentinel Licensing API in your code • Switch between the above implementation depending on the connected key	• Remove SmartKey implementation • Implement Sentinel Licensing API in your code and protect using Sentinel LDK Envelope
Security level	Same as SmartKey API only	Very high
Flexibility level (licensing, portability)	Medium	Very high
Additional benefits		Driverless deployment

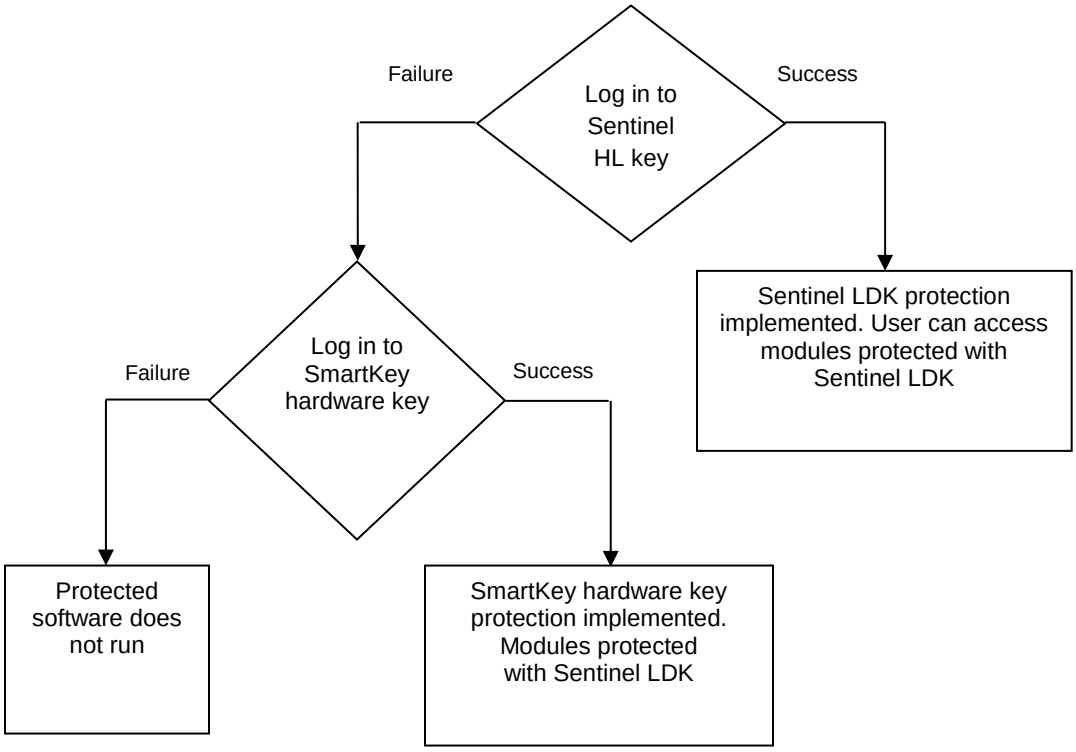
Stage 1: Combining SmartKey with Sentinel LDK Protection

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 SmartKey. If a SmartKey is detected, SmartKey protection is used.

In order to maximize security and implement the higher level of protection provided by Sentinel LDK Envelope, concurrently with the SmartKey protection of your software, you can protect SmartKey-protected files or modules using the Sentinel Licensing API. Consider also using Sentinel LDK Envelope to protect any individual files that are not protected by SmartKey. Applications that are protected solely by Sentinel LDK can only be executed using a Sentinel HL key.

Sentinel LDK-protected applications have greater security than those protected by SmartKey alone. If a SmartKey is used, modules protected with SmartKey will continue to 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:



The above diagram is relevant to all SmartKeys.

Implementing Stage 1

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

To implement both Sentinel LDK and SmartKey functionality:

1. If you have not already done so, install Sentinel Vendor Suite 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. 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 customized Sentinel Licensing API header files in your project. Do **not** remove included SmartKey headers.

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

4. To enable your software to work with SmartKey or Sentinel LDK protection, implement the decision tree on page 13 of this document, as follows:

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

      (See *Sentinel LDK Software Protection and Licensing Guide*, chapter “Sentinel Licensing API Protection,” and online help for Sentinel Licensing API.)

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

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

You can optionally enhance the security of selected items in your application by protecting them using Sentinel LDK Envelope. 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.

Important: For binaries that implement licensing APIs for SmartKey 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 SmartKeys with Sentinel HL keys, at your convenience.

Stage 2: Full Implementation of Sentinel LDK Functionality

Stage 2 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 keys.

Implementing Stage 2

The following procedure details the steps required to implement Stage 2 of the SmartKey-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 not already implemented Stage 1, perform steps 1-3 of Stage 1 in order to complete the following:
   a. Install Sentinel Vendor Suite 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.

      (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 SmartKey in the code with calls to Sentinel HL keys.
   See Table 3: *Comparison of SmartKey API Functions and Sentinel Licensing API Functions* on page 21 for a list of SmartKey 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.

3

Migration Path 3—Gradual Migration from SmartKey to Sentinel LDK Using a Launcher Application

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

The migration is achieved by creating two versions of your software—one protected using SmartKey GSS, 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 SmartKey GSS-protected version of your software is launched.

This migration path enables you to support existing users who already have SmartKeys, 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 diagram summarizes the two stages for Migration Path 3.

	Stage 1	Stage 2
Implementation effort	Low	Medium
Install base	Remains SmartKey	Replace with Sentinel HL key
Keys for new customers	Sentinel HL (Driverless configuration) key	Sentinel HL (Driverless configuration) key
Protection process	• Create two binaries – one protected using SmartKey GSS, the other using Sentinel LDK Envelope • Create a launcher application using the Sentinel Licensing API to search for a Sentinel LDK protection key • Switch between above binaries , depending on connected key	• Remove SmartKey implementation • Implement Sentinel Licensing API in your code and protect using Sentinel LDK Envelope
Security level	Same as SmartKey GSS only	Very high
Flexibility level (licensing, portability)	Medium-high	Very high
Additional benefits		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 SmartKey GSS, 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

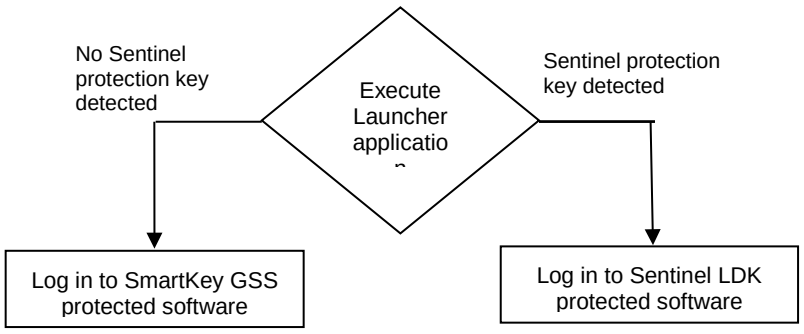
The following procedure details the steps required to implement the SmartKey GSS-to-Sentinel LDK migration process. Where relevant, you are pointed to additional information in the Sentinel LDK documentation.

To implement Sentinel LDK functionality:

1. If you have not already done so, install Sentinel Vendor Suite and Sentinel EMS, and introduce your Sentinel Vendor keys. (See the *Sentinel LDK Installation Guide*.)
2. Create a version of your software (for example, `program_smartkey.exe`) and implement SmartKey GSS protection using SmartKey GSS and/or the SmartKey API.
3. 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.
4. Create a launcher application using the Sentinel Licensing API that will detect whether a Sentinel LDK protection key is accessible. Program the following behavior:
   c. If a Sentinel LDK protection key is detected, the launcher launches `program_haspsrm.exe`.
   d. If a Sentinel LDK protection key is not detected, the launcher launches `program_smartkey.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 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 increased security and licensing capabilities. After you implement full Sentinel LDK protection, all customers using this version of your software must use Sentinel LDK protection keys.

Implementing Stage 2

The following procedure details the steps required to implement Stage 2 of the SmartKey-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 SmartKey API, replace all calls to SmartKey in the code with calls to Sentinel LDK protection keys.

   See Table 3: *Comparison of SmartKey API Functions and Sentinel Licensing API Functions* on page 21 for a list of SmartKey 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 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 SmartKey Comparison Tables

Table 1: Comparison of Sentinel HL Keys and SmartKeys

Model Type	Sentinel HL	SmartKey
Basic ♦ No read/write memory functionality ♦ Perpetual license ♦ Locally connected key	Sentinel HL (Driverless configuration) Basic	SmartKey FX
Memory ♦ Read/write and read-only memory ♦ Locally connected key	Sentinel HL (Driverless configuration) Pro ♦ 112 bytes R/W + 112 bytes ROM Sentinel HL (Driverless configuration) Max ♦ 4 KB R/W + 2 KB ROM	SmartKey PR ♦ 64/128 bytes R/W SmartKey EP ♦ 64/128 bytes R/W SmartKey SP ♦ 896 bytes R/W
Time ♦ Real-time clock ♦ Read/write and read-only memory ♦ Locally connected key	Sentinel HL (Driverless configuration) Time ♦ RTC ♦ 4 KB R/W + 2 KB ROM	None
Net ♦ Read/write and read-only memory ♦ Network-based licensing	Sentinel HL (Driverless configuration) Net ♦ 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.	SmartKey NET ♦ 896 bytes R/W ♦ Max no. of concurrent users: 254
Net and Time ♦ Real-time clock ♦ Read/write and read-only memory ♦ Network-based licensing	Sentinel HL (Driverless configuration) NetTime ♦ RTC ♦ 4 KB R/W + 2 KB ROM ♦ Max no. of concurrent users: 10, 50, 250 Sentinel HL (Driverless configuration) Time with concurrency license ♦ RTC ♦ 4 KB R/W + 2 KB ROM	None

Model Type	Sentinel HL	SmartKey
Drive ♦ Read/write and read-only memory ♦ Extended mass storage	Sentinel HL (Driverless configuration) Drive ♦ 4 KB R/W + 2 KB ROM ♦ 2 GB or 4 GB USB mass storage drive	SmartPico ♦ 896 bytes R/W ♦ from 256 Mb to 4 GB USB mass storage drive

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

Table 2: SmartKey and Sentinel LDK Tool Equivalents

SmartKey Tools	Sentinel LDK Tools
SmartKey Programming Central (SPC) – Setting label and password. ID code is programmed at production site.	Keys are pre-encoded at the Gemalto production site. Use your unique Vendor Code (stored in the Sentinel Vendor keys)
Global Security Setting (GSS)	Sentinel LDK Envelope (part of Sentinel Vendor Suite)
SPC - Programming keys	Sentinel EMS (part of Sentinel Vendor Suite)
SPC (for function execution only)–Code samples provided in the SDK for the most common languages	Sentinel LDK ToolBox (part of Sentinel Vendor Suite)
SmartKey Driver Installation (SDI)	Sentinel LDK Run-time Environment installer
SPCinfo and Skeymon (server monitor)	Sentinel Admin Control Center (part of the Sentinel LDK Run-time Environment)
	Sentinel Remote Update System (RUS)
Serial number	HASP ID

Table 3: Comparison of SmartKey API Functions and Sentinel Licensing API Functions

SmartKey API Function*	Sentinel Licensing API Function
Locating mode msclink(), "L" command	Performed automatically by `hasp_login()`
Scrambling mode msclink(),smartlink(), "S" command	Use `hasp_encrypt()` and `hasp_decrypt()` to perform encryption on data buffer
Reading mode msclink(),smartlink(), "R" command	Use `hasp_read()` to read Sentinel key memory
Writing mode msclink(),smartlink(), "W" command	Use `hasp_write()` to write Sentinel key memory
Block Reading mode msclink(),smartlink(), "BR" command	Use `hasp_read()` to read Sentinel key memory and set offset and length
Block Writing mode msclink(),smartlink(), "BW" command	Use `hasp_write()` to read Sentinel key memory and set offset and length
Fixing Msclink(), "F" command	Use the ROM memory of the Sentinel key instead of fixing the memory
Programming Msclink(), "P" command	Not required in Sentinel LDK. Login data is automatically managed.
Comparing Msclink(), "C" command	Performed automatically by `hasp_login()`
Model Reading msclink(),smartlink(), "M" command	`hasp_get_sessioninfo()`
Serial Number Reading msclink(),smartlink(), "N" command	`hasp_get_sessioninfo()`
Ext Model Reading msclink(),smartlink(), "M" command	`hasp_get_sessioninfo()`
Fix Reading msclink(),smartlink(), "X" command	Not present in Sentinel LDK
Fail Counter Reading msclink(),smartlink(), "A" command	Not present in Sentinel LDK
AES Set Msclink(), "G" command	Keys are pre-encoded at the Gemalto production site
AES Scramble msclink(),smartlink(), "O" command	Performed automatically by `hasp_login()`
Open Mode smartlink(), "O" NET_command	Performed automatically by `hasp_login()` Logging in to a specific connected key is possible using `hasp_login_scope()`

SmartKey API Function*	Sentinel Licensing API Function
`Access Mode` `smartlink(), “A” NET_command`	Not required in Sentinel LDK
`User Number Mode` `smartlink(), “U” NET_command`	`hasp_get_sessioninfo()`
`Close Mode` `smartlink(), “C” NET_command`	`hasp_logout ()`