Sentinel® LDK

Migration Guide
HASP HL to Sentinel LDK

gemalto
security to be free

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 Software DRM 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 the 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.

The backward compatibility of Sentinel HL (HASP configuration) keys to HASP HL 1.x protection enables you to move to Sentinel LDK in stages.

About This Guide

This guide is intended for HASP HL 1.x users who wish to continue using a hardware-based protection solution, and who want to take advantage of the supreme strength of Sentinel HL key protection and of the advanced licensing options provided by Sentinel LDK.

> 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 HASP HL and the Sentinel LDK systems.

The guide provides the following:

- An overview and guidelines for a three-stage migration path from HASP HL 1.x to Sentinel LDK, starting with an install base that includes only HASP HL keys with Firmware version 2.16 or later.

- Migration procedures.

- Tables that list the tools and functionalities of HASP HL 1.x and their counterparts in Sentinel LDK.

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 HASP HL legacy functionality, refer to the *HASP HL Software Protection and Licensing Guide v.1.30* or to the relevant HASP HL Help documentation.

Terminology

The following terms are used in this guide:

Legacy HASP HL keys	HASP HL keys with Firmware version 2.16
HASP HL keys	HASP HL keys with Firmware version 3.25
HASP HL 1.x (protection)	Protection that was applied using HASP HL 1.x API and/or Envelope
Sentinel LDK (protection)	Protection that was applied using Sentinel LDK v.7.1 Licensing API and/or Envelope

> You can see the Firmware version of a HASP HL key in the **Sentinel Keys** screen in Sentinel Admin Control Center. Examine the **Version** column for the relevant HASP HL key.

Migration Use Cases

The table below lists various use cases that can be implemented using the procedures in this migration guide.

	Existing Installed Hardware Base	Existing Protection Implementation	Planned Hardware	Planned Protection Implementation	Planned Backend	Notes
1	Legacy HASP HL key or HASP HL key	HASP HL 1.x protection	HASP HL key (since already deployed) or SHL(HASP) key	Sentinel LDK	Sentinel EMS	Provides better backend, better security
2	Basic key: Legacy HASP HL key or HASP HL key	HASP HL 1.x protection	HASP HL Basic key	Sentinel LDK	None	Provides better security
3	Legacy HASP HL key or HASP HL key	HASP HL 1.x protection	SHL(HASP) key	Sentinel LDK	Sentinel EMS	Provides better backend, better security. No backward compatibility in LDK
4	Basic key: Legacy HASP HL key or HASP HL key	HASP HL 1.x protection	SHL(HASP) Basic key	Sentinel LDK	None	Provides better security
5	Legacy HASP HL key or HASP HL key	HASP HL 1.x protection	SHL(Driverless) key	Sentinel LDK	Sentinel EMS	Provides better backend, better security. Increased Features memory. No backward compatibility

	Existing Installed Hardware Base	Existing Protection Implementa-tion	Planned Hardware	Planned Protection Implementa-tion	Planned Backend	Notes
6	Basic key: Legacy HASP HL key or HASP HL key	HASP HL 1.x protection	SHL(Driverless) Basic key	Sentinel LDK	None	Provides better security No backward compatibility

> ✎ Legacy HASP HL keys are changed to HASP HL keys by upgrading the Firmware on the key. No hardware change is required.

Table Legend:

SHL(HASP)   Sentinel HL (HASP configuration) protection key

SHL(Driverless)   Sentinel HL (Driverless configuration) protection key

Compatibility With HASP HL 1.x Protection

Sentinel HL (HASP configuration) keys are fully backward compatible with HASP HL 1.x protection. This means that deployed applications currently protected by HASP HL 1.x protection software can work with Sentinel HL keys without the need to update software or drivers.

You can begin supplying Sentinel HL (HASP configuration) keys to new customers immediately, with no change to your existing software. When you decide to migrate your entire customer base to Sentinel HL (Driverless configuration) keys, it will not be necessary to replace the Sentinel HL (HASP configuration) keys that have already been deployed. These keys can be upgraded to Sentinel HL (Driverless configuration) keys at the customer site.

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*.

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 HASP HL 1.x 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
Three Stage Migration Path

The three-stage migration path is designed to facilitate a gradual move towards improved security for your products, implementing the protection and licensing functionalities of Sentinel LDK. The stages are not interdependent, and it is possible to skip Stage 1 and go directly to Stage 2. Similarly, the time that you wait before moving from one stage to the next is entirely at your discretion. The following table summarizes the three-stage migration path.

	Stage 1	Stage 2	Stage 3
Implementation effort	-	+	+ +
Install base	Remains Legacy HASP HL keys and HASP HL keys	Legacy HASP HL keys, HASP HL keys, and Sentinel HL (HASP configuration) keys	• Replace Legacy HASP HL keys (if any) and HASP HL keys with Sentinel HL (Driverless configuration) keys. • Upgrade Sentinel HL (HASP configuration) keys to Sentinel HL (Driverless configuration) keys.
Keys for new customers	Sentinel HL (HASP configuration) keys	Sentinel HL (HASP configuration) keys	• Sentinel HL (Driverless configuration) key
Protection process	No change to code. Software remains protected with HASP HL 1.x	• Update Firmware for Legacy HASP keys to v.3.56 • Perform full or partial transition of protected application to LDK protection.	• Perform complete transition of protected application to LDK protection (if not done earlier). • Eliminate use of the HASP_FILEID_MAIN and HASP_FILEID_LICENSE memory files (if not done earlier)
Security level	+	+ +	+ + + +
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

2

Stage 1: Using Sentinel HL keys as Legacy HASP HL Keys

Sentinel HL (HASP configuration) keys are fully backward compatible with HASP HL 1.x protection, so that your software can work with either the Sentinel HL (HASP configuration) keys or the Legacy HASP HL keys. 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 (HASP configuration) keys to your customers and gradually replace your install base of Legacy HASP HL keys and current HASP HL keys with Sentinel HL (HASP configuration) keys at your convenience. When you decide to move to Stage 2 or 3 of the migration process and protect your software with Sentinel LDK, you will already have deployed Sentinel HL keys.

Since Sentinel HL (HASP configuration) keys can be upgraded to Sentinel HL (Driverless configuration) keys on the end user machine, it will not be necessary to replace these keys at the later stage of the migration process.

Proceed as follows:

1. Leave your install base with the HASP HL keys and Legacy HASP HL keys that they are currently using.

2. Start distributing Sentinel HL (HASP configuration) keys with new purchases. At this stage you do not need to make any changes to your software, which remains protected by HASP HL 1.x security.

3

Stage 2: Implementing Sentinel LDK Protection

In this stage, you create a version of your software that partially or completely replaces HASP HL 1.x protection with Sentinel LDK protection. This stage is usually implemented with a new release of the protected application.

Sentinel Protection Keys

When you move from HASP HL 1.x to Sentinel LDK, there is no need to recall or replace your install base of HASP HL keys. You only need to update existing Legacy HASP HL keys to Firmware v.3.25, using the Sentinel LDK Firmware Update utility.

New customers should receive Sentinel HL (HASP configuration) keys.

Sentinel Vendor Keys

The Sentinel LDK Starter kit includes two new Sentinel Vendor keys that replace your HASP HL Master key:

- Sentinel Master key, used in the licensing and production process

- Sentinel Developer key, used in the software protection process

These keys are associated with your existing Batch Code, but contain a new Vendor Code for use with Sentinel LDK.

Transition Options

It is highly recommended that you implement a complete transition of your software protection from HASP HL to Sentinel LDK, although it is possible to maintain the legacy HASP HL 1.x protection simultaneously with added Sentinel LDK protection at this stage.

- The complete transition path is described in "Complete Transition to Sentinel LDK" on page 13.

- The path to combine Sentinel LDK and HASP HL 1.x protection is described in "Combining Sentinel LDK and HASP HL 1.x Protection" on page 16.

Complete Transition to Sentinel LDK

This section describes the process for complete transition from HASP HL 1.x to Sentinel LDK, including the adaptation of all HASP HL 1.x code segments in your software to Sentinel LDK. Where relevant, you are pointed to additional information in the *Sentinel LDK Software Protection and Licensing Guide.*

1. **Installing Sentinel LDK and Introducing your Vendor Keys**

    If you have not already done so, install Sentinel Vendor Suite and Sentinel 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. **Defining Feature IDs**

    In Sentinel EMS, define new Feature IDs to replace the program numbers used in HASP HL.

    (See *Sentinel LDK Software Protection and Licensing Guide*, chapter "Implementing Your Sentinel LDK Licensing Plan.")

    📝   Feature ID 0 is predefined as a default feature.

    ---

3. **Linking to Sentinel Licensing API Libraries**

    Replace the links in your software to the HASP HL 1.x customized libraries with links to your customized Sentinel Licensing API libraries.

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

4. **Adapting HASP HL Code in Your Software**

    All HASP HL 1.x code segments must be adapted to Sentinel LDK as follows:

    a. Replace the HASP HL Vendor Code used in `hasp_login()` calls with the new Vendor Code. In Sentinel LDK, Vendor Codes are saved in the following directory:

    %UserProfile%/My Documents\Gemalto\Sentinel LDK [*version*]\VendorCodes

    For Windows Vista (and later) users, the directory path is
    %UserProfile%\Documents\Gemalto\Sentinel LDK [*version*]

    b. Replace the HASP HL program number used in the `hasp_login()` call with the appropriate Feature ID that you defined in Sentinel EMS.

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

5. **Encrypting Data**

    In HASP HL 1.x, all program numbers use the same encryption key. Sentinel LDK applies a unique encryption key for each Feature ID, providing much stronger protection. In order to implement this protection, you must replace all data that was encrypted using HASP HL with data that is encrypted using Sentinel LDK as follows:

    a. Decrypt the data using HASP HL 1.x, or locate the original unencrypted data.

    b. Ensure that you are using your new Vendor Code. Encrypt the data using Sentinel LDK, using the Feature ID relevant to that data segment.

    c. Ensure that the `hasp_login()` call for the data segment is defined with the same Feature ID that you used to encrypt the data. Replace the HASP HL-encrypted data in your code with the Sentinel LDK-encrypted data.

    (See *Sentinel LDK Software Protection and Licensing Guide*, chapter "Protection Strategies.")

> To maintain backward compatibility, the encryption key assigned to Sentinel LDK Feature ID 0 and associated with your Batch Code is identical to the encryption key that was used in HASP HL 1.x with your Batch Code for all Program Numbers. This enables you to decrypt data that was encrypted with HASP HL 1.x, using Sentinel LDK.

6. **Writing Data to the Legacy HASP HL Key**

   The backward compatibility of Sentinel LDK with HASP HL 1.x enables you to continue writing data to the key with the `HASP_FILEID_MAIN` and `HASP_FILEID_LICENSE` memory files.

   However, it is highly recommended that you take advantage of the secure communication channel that Sentinel LDK adds to the Legacy HASP HL key. To do this, write your existing data, which is already saved on the key with `HASP_FILEID_MAIN` and `HASP_FILEID_LICENSE` memory files, to one of the following Sentinel protection key memory files:

   - Data in the `HASP_FILEID_RW` memory file enables you to write to, or read from, a key's memory during run-time.

   - Data in the `HASP_FILEID_RO` memory file enables you to read from a key's memory during run-time. Data may be written to the key either during key production or when updating the key.

   (See *Sentinel LDK Software Protection and Licensing Guide*, chapters "Implementing Your Sentinel LDK Licensing Plan" and "Sentinel Remote Update System.")

7. **Wrapping Your Software with Sentinel LDK Envelope**

   Ensure that you use your new Vendor Code, and wrap the software using Sentinel LDK Envelope.

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

8. **Replacing HASP HL 1.x Drivers with Sentinel LDK Run-time Environment**

   Replace the HASP HL 1.x drivers that are included in your application setup with Sentinel LDK Run-time Environment.

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

9. **Updating Legacy HASP HL Keys to Firmware v.3.25**

   When you move to Sentinel LDK, you need to update your install base of Legacy HASP HL keys, and any keys that you have in stock, from firmware v.2.16 to v.3.25. You can update the firmware independently or as part of a software update, as follows:

   - To run the firmware update independently:

   Download the latest version of the GUI-driven HASP HL Firmware Update utility as described below. Distribute the utility to your end users.

   - To run the firmware update as part of your software update:

   Download the latest version of the HASP HL Firmware Update V2C file as described below. Incorporate this file into your code using the Sentinel Licensing API `hasp_update()` function.

   OR

   Navigate to **%ProgramFiles(x86)%\Gemalto Sentinel\Sentinel LDK\Redistribute\FirmwareUpdate** and incorporate `firmware_update_325.v2c` into your code. (Under Windows x86, navigate to **%ProgramFiles%\...**).

To download the firmware upgrade utility or firmware update V2C file:

a. Go to the Sentinel download page.

b. In the **Type** list, select **Firmware Updates**. Click **Search**.

c. Select the HASP HL Firmware Update utility or HASP HL Firmware Update V2C file.

10. **Using Legacy HASP HL Net Keys**

When Sentinel LDK is fully implemented, you do not need to install the HASP License Manager or the Aladdin Monitor on the server machine to which the Legacy HASP HL Net key is attached. Sentinel LDK Run-time Environment automatically installs Sentinel Admin Control Center, including Sentinel License Manager, which manages Legacy HASP HL Net and HASP HL NetTime keys.

Combining Sentinel LDK and HASP HL 1.x Protection

You can maintain your legacy HASP HL 1.x protection simultaneously with the added protection and licensing capabilities of Sentinel LDK. This is possible because when the Legacy HASP HL key is updated to firmware v.3.25, the key is divided into two sectors, each of which functions as a separate key. The legacy key sector provides full HASP HL legacy functionality. The Sentinel LDK key sector provides the advanced Sentinel LDK capabilities. When you combine HASP HL 1.x and Sentinel LDK functionality, the two separate key sectors require a dual process in the production phase and at the end-user site.

Similarly, Sentinel HL (HASP configuration) keys provide both backward compatibility with HASP 1.x and advanced Sentinel LDK capabilities.

Following is a breakdown of the required steps when you choose to retain legacy HASP HL 1.x protection in your code concurrently with Sentinel LDK functionality. Where relevant, you are pointed to additional information in the *Sentinel LDK Software Protection and Licensing Guide*.

1. **Installing Sentinel LDK and Introducing your Vendor Keys**

    > **Important:** Do not uninstall HASP HL 1.x.

    If you have not already done so, install Sentinel Vendor Suite and Sentinel 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. **Enabling Legacy HASP HL Functionality**

    a. In the Sentinel Vendor Suite window, select **ToolBox**. From the Sentinel LDK ToolBox menu bar, select **Files > Settings**.

    b. In the General tab of the Settings dialog box, select the Allow access to HASP HL v.1.x check box.

    > Version 1.x refers to the legacy functionality on the HASP HL keys.

3. **Combining HASP HL 1.x and Sentinel LDK Protection**

    a. For code sections for which you want to implement Sentinel LDK protection, proceed as described in steps 2–7 of "Complete Transition to Sentinel LDK" on page 13. These code sections use the Sentinel LDK sector of the HASP HL key.

    b. For code sections for which you want to retain existing HASP HL 1.x protection, it is not necessary to make any changes, since Sentinel LDK is backward compatible with HASP HL 1.x. These code sections use the legacy HASP HL sector on the HASP HL key.

4. **Licensing, Production and End-User License Management**

    The Sentinel LDK and legacy HASP HL sectors in a HASP HL key are managed separately, and the licensing, production and updating of each sector are implemented using the relevant tools.

The following table details the tools and definitions you must use to manage each of the key sectors.

Management of...	Sentinel LDK Sector	Legacy HASP HL Sector
Program/ Feature ID	Recognizes Feature IDs in the range: `0x00000000-0x0000FFBF`	Program numbers 0-112 Recognizes Feature IDs in the range: `0xFFFF0000-0xFFFF0070`
Licensing	Sentinel EMS	HASP HL Factory
Production and Creation of Remote Update Files	Sentinel EMS	HASP HL Factory
Remote Update at End-User Site	Sentinel Remote Update System (RUS)	HASP HL Remote Update System (RUS)
Key Monitoring	Sentinel Admin Control Center	Aladdin Monitor
License Management at End-User Site	Sentinel License Manager, interfaced through the Sentinel Admin Control Center	HASP License Manager

5. **Replacing HL Drivers with Sentinel LDK Run-time Environment**

   Replace the HASP HL 1.x drivers that are included in your application setup with Sentinel LDK Run-time Environment, which is backward-compatible with HASP HL 1.x.

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

6. **Updating Legacy HASP HL Keys to Firmware v.3.25**

   Update your install base of Legacy HASP HL keys firmware v.2.16 to v.3.25 as described in step 9 of *Complete* Transition to Sentinel LDK in this document.

4

Stage 3: Migration to Driverless Keys

In this stage, you complete the migration to Sentinel HL (Driverless configuration) keys and, if not done earlier, complete the migration to Sentinel LDK protection and backend.

Legacy HASP HL keys (if any) and HASP HL keys at the customer site must be replaced by Sentinel HL (Driverless configuration) keys. Sentinel HL (HASP configuration) keys at the customer site must be upgraded to Sentinel HL (Driverless configuration) keys.

Note that the Run-time Environment is required on the machine where a Sentinel network key is connected, regardless of the configuration of the key.

Implementing Stage 3

Fully implement the migration to Driverless keys as follows:

1. Complete the transition to Sentinel LDK

   If you have not already done so in Stage 2, complete your transition to Sentinel LDK and described on page 13.

   If you have completed your transition, but are still writing data to the key with the `HASP_FILEID_MAIN` and `HASP_FILEID_LICENSE` memory files, write your data to one of the Sentinel protection key data files as described in "Writing Data to the Legacy HASP HL Key" on page 14.

2. Upgrade to Sentinel HL (Driverless Configuration) Keys

   Define an Update Product or Base Product that includes the **Upgrade to Driverless** attribute. This upgrades existing Sentinel HL (HASP configuration) keys to Sentinel HL (Driverless) keys. The attribute is ignored when applied to protection keys for which the attribute is not relevant (that is, Sentinel HL (Driverless configuration) keys). This Product should be applied to Sentinel HL keys that exist at the customer sites.

   For more information, see the appendix "How to Upgrade a Sentinel HL Key to Driverless Configuration" in the *Sentinel LDK Software Protection and Licensing Guide.*

3. Distribute Your Software

   Follow the instructions in the *Sentinel LDK Software Protection and Licensing Guide* to distribute your software (chapter "Distributing Sentinel LDK with Your Software").

4. Distribute or Upgrade End-User Keys

   Ensure that all customers who are still working with Legacy HASP HL keys (if any) or HASP HL keys, and who receive the Sentinel LDK-protected software, also receive Sentinel HL (Driverless configuration) keys.

   The Sentinel HL (HASP configuration) keys that newer customers received will be upgraded to Sentinel HL (Driverless configuration) keys by the Product that you defined in step 2 above.

APPENDIX A
Sentinel LDK and HASP HL Comparison Tables

Table 1: Memory Size in HASP HL Firmware v.3.25 Keys

Key Type	Legacy HASP HL Sector	Sentinel LDK Sector
Basic	–	–
Pro	112 bytes backward-compatible memory	112 bytes protected Read/Write memory 112 bytes ROM
Max	4 KB backward-compatible memory	4 KB protected Read/Write memory 2 KB ROM
Time	4 KB backward-compatible memory	4 KB protected Read/Write memory 2 KB ROM
Drive	4 KB backward-compatible memory	2 GB / 4 GB Flash memory 4 KB protected Read/Write memory 2 KB ROM
Net	4 KB backward-compatible memory	4 KB protected Read/Write memory 2 KB ROM
NetTime	4 KB backward-compatible memory	4 KB protected Read/Write memory 2 KB ROM

Table 2: HASP HL Tools and Functions and their Sentinel LDK Counterparts

HASP HL Application / Functionality	Sentinel LDK Application / Functionality
HASP HL Vendor Code, read from file	Vendor Code, can be read from the Sentinel EMS database or from a file
HASP HL Envelope	Sentinel LDK Envelope
HASP HL Factory	Sentinel EMS
HASP HL ToolBox	Sentinel LDK ToolBox
HASP HL Drivers	Sentinel LDK Run-time Environment
Aladdin Monitor	Sentinel Admin Control Center (part of the Sentinel LDK Run-time Environment)
Aladdin DiagnositX	Sentinel Admin Control Center (part of the Sentinel LDK Run-time Environment)
HASP HL Factory API	Sentinel EMS Web Services
HASP HL RUS	Sentinel RUS
HASP HL API	Sentinel Licensing API

HASP HL Application / Functionality	Sentinel LDK Application / Functionality
–	Sentinel Activation API
Key time set in HASP HL Factory	Key time set to UTC during production
License Manager, Monitor, DiagnostiX	
`Lmsetup.exe`	Run-time Environment Installer
LM application – `Nhsrvw32.exe`	–
LM application (service) – `Lmsrvice.exe`	Sentinel License Manager – `hasplms.exe`
Monitor Setup – `aksmon32.exe`	Run-time setup
`Nethasp.ini` – client configuration file	Sentinel Admin Control Center – from **Configuration** menu, **Access to Remote License Managers** `hasplm.ini`
`Nhsrv.ini` – LM configuration file	Sentinel Admin Control Center – from **Configuration** menu, **Access to Remote Clients** `hasplm.ini`
Aladdin Monitor	Sentinel Admin Control Center (part of the Sentinel LDK Run-time Environment)

Table 3: New Sentinel Licensing API Functions

HASP HL Function*	Sentinel LDK Function
`hasp_get_sessioninfo()`	`hasp_get_sessioninfo()` `hasp_get_info()`
`hasp_login()`	`hasp_login()` `hasp_loginscope()`
`hasp_read()`	Transfer data saved in HASP HL with `HASP_FILEID_MAIN` and `HASP_FILEID_LICENSE` memory files to Sentinel protection key HASP `HASP_FILEID_RW` or `HASP_FILEID_RO` memory files.
`hasp_write()`	
`hasp_detach()`	`hasp_transfer()`

* Only functions that differ from HASP HL are listed. For additional information about the Sentinel Licensing API functions, see the online help for Sentinel Licensing API.