

Frequently Asked Questions: Sentinel Hardware Keys

What are Sentinel Hardware Keys?

Sentinel Hardware Keys are physical hardware tokens that protect software applications from piracy: unauthorized use and distribution.

How do Sentinel Hardware Keys work?

Sentinel Keys are integrated into a software application through use of a software development toolkit. The key is then distributed along with the software application to the end user. The protected application checks for the presence of the key during runtime to ensure that the software usage is authorized and the parameters of the license agreement are enforced.

Why Use Sentinel Hardware Keys?

1. To protect the intellectual property and revenues of software vendors.
 - Sentinel Keys ensure that your organization receives revenue it deserves for its software development.
2. To allow software vendors to market effectively by offering customers flexible, user-friendly licensing.
 - Sentinel Keys offer a variety of licensing models for software vendors to select from in order to deliver their products to their end-users.

Why Are Sentinel Keys Superior to other Software Protection Tokens?

1. Unmatched Security

Superior Protection

Sentinel Keys secure communications between the key and the protected application through use of public key cryptography and 128-bit AES encryption. A unique encryption key is used for every communication session between the application and the hardware token, making brute force attacks virtually impossible. The keys also include internal authentication to prevent cloning.

Additional Layers of Protection for Further Security

Sentinel Keys offer additional protection layers with the Sentinel Shell to prevent memory dumping and make reverse engineering more difficult. Without the additional layer of protection from the Sentinel Shell, the source code is exposed to these threats. The Sentinel Shell enables developers to embed licensing and protect software applications in minutes, even without access to source code.

2. Ease-Of-Use

Easier Integration

Sentinel Keys reduce and simplify programming steps, enabling a secure and easy integration. With Sentinel Business Layer APIs, developers can obtain the highest level of security and control over sophisticated license designs without spending time on lower-level programming. Business Layer APIs are pre-configured, higher level APIs for popular license models such as subscription, evaluation and

pay-per-use. These tools typically reduce the programming time required to secure a new application by up to 60% or more compared to other hardware key solutions.

Agility in Delivering License Updates

Software vendors are able to send and manage remote updates or additional licenses to keys in the field in a secure, controlled manner. As license requirements change, license configuration can be altered remotely without further development changes. Updates are sent using the same high level of security as communications between the hardware token and software application.

Multiple Application Protection

Sentinel Keys are flexible enough to protect multiple applications with a single token. Protection for other applications can be added at a later date without altering the existing security structure.

3. Business Enablement

Trusted Distributor Model

Only Sentinel Hardware Keys allow for control and regulation over distribution channels through the use of Distributor Keys. Developers can assign and securely embed encryption keys during the manufacturing process in order to control the creation of licenses through distribution channels. For example, developers can limit the number of licenses generated by distributors or allow for the creation of trial licenses only.

Reliable Time-Based Licensing

The Sentinel V-Clock allows developers to reliably and securely offer time-based license models such as trial, demo or subscription. Sentinel V-Clock resists time tampering and requires no on-board battery, enabling secure time-based licensing without added costs. The V-Clock checks and stores the system time in the hardware key; then checks repeatedly to verify consistency. If the system time ever differs significantly from the last known date and time, the application can be disabled or run in a restricted mode.

Available with a Real Time Clock (RTC)

With Sentinel's RTC, developers can meet unique customer needs for flexible time-based licensing, while protecting their own revenue streams. The RTC also allows end users to place time and date stamps on the output of an application for definitive time recording purposes. To ensure reliability, the battery which powers the internal clock has a life expectancy of four to six years.

Ability to Licensing Across Networks

Sentinel Keys allow for multiple licenses of an application to be stored on one key throughout the network to track and manage license usage on the network.

4. Leading Provider in Software Protection

Popular Development Environment and Platform Support

As the leading innovator in information security, SafeNet is the first to respond to emerging technologies. You can be assured that your software protection products will provide support for the latest platforms and technologies in the industry. Sentinel Keys provide sample code for the most popular development environments, including Microsoft Visual C++, Microsoft Visual Basic and Microsoft .NET. With Sentinel, applications can be supported on multiple operating platforms with a single development effort, further reducing development time and cost.

Superior Technical Support

The SafeNet Technical Services organization provides worldwide telephone, email and Internet-based support to customers 24 hours a day, 5 days a week. The Sentinel Integration Center provides online resources to assist development staff through the implementation process.

Market Leadership and Longevity

Over 40 million licenses worldwide are protected by SafeNet Sentinel hardware keys. Sentinel has been setting the standard for software protection since 1984 and secures more clients worldwide than any other key. At SafeNet, we provide complete rights management solutions to protect the assets of software vendors throughout the entire product lifecycle – from development, delivery and management of software, to monitoring and mitigation of piracy. We are the quickest to respond to emerging technologies, providing software vendors the features they need in order to enable the best protection for their valuable software products.

What types of license models are supported?

Sentinel Keys support a variety of license models. Vendors can base licenses on time, number of executions, or a determined expiration date. License models include: evaluation, pay-per-use, standalone, network and more.

With the Sentinel V-Clock, vendors can securely offer license models, such as trial, demo or subscription. The V-Clock stores the system time in the key and checks repeatedly to verify consistency of the time. If the system time ever differs significantly from the last checked time and date, the application can be disabled or run in a restricted mode. When an evaluation license expires, the key can be updated remotely with an additional trial license or upgraded to a fully functioning application. The Sentinel V-Clock comes standard, at no additional cost.

Where is the return on an investment in Sentinel Keys?

In 2006, nearly \$40 billion in software was pirated worldwide, according to the Business Software Association. Sentinel Hardware Keys ensure that software vendors are able to protect their markets and intellectual property from loss due to piracy.

In addition to preventing piracy, the flexible licensing provided by Sentinel allows your company to reach new markets, providing an opportunity for increasing their revenues. Sentinel Keys also help decrease development costs with features such as Business Layer APIs™ that speed implementation time compared to other protection solutions.

How do I implement Sentinel Keys?

The best implementation of any protection scheme should include complete integration into your application through APIs. Sentinel Business Layer APIs™ are pre-configured, higher level APIs for popular license models such as subscription, evaluation and pay-per-use. By using Sentinel Business Layer APIs, vendors can obtain the highest level of security and control over sophisticated license designs without spending time on lower-level programming. These tools typically reduce the programming time required to secure a new application by up to 60% or more compared to other hardware key solutions.

The Sentinel Shell offers a way to quickly implement additional protection to your application without requiring any alteration to the source code. When used in conjunction with API level integrations, the Shell greatly enhances overall security.

Will implementation of Sentinel Keys delay my product launch?

At SafeNet, we are the industry leader in software protection. We build our products so they are quick and easy to use to ensure maximum information security in the marketplace. The time it takes to implement Sentinel Keys varies, depending on the type of license models that you plan to implement and the number of applications you need to protect.

By using Sentinel Business Layer APIs™, you can obtain the highest level of security and control over sophisticated license designs without spending time on lower level programming. Business Layer APIs are pre-configured, higher level APIs for popular license models such as subscription, evaluation and pay-per-use. These tools typically reduce the programming time required to secure a new application by up to 60% or more compared to other hardware key solutions.

The Sentinel Shell enhances overall security when used in conjunction with API level integrations and requires only minutes to implement.

Can I update keys that have been deployed?

Sentinel technology enables ISVs to send updates or additional licenses to keys in the field in a secure, controlled manner. Updates are sent using the same high level of security as communications between the hardware token and the software application.

How do I enable my distributors to fulfill licenses?

Sentinel Hardware Keys allow you to securely control your distribution channels through the use of Distributor Keys. You can assign and securely embed encryption keys during the manufacturing process in order to control the creation of licenses through your

channels. Distributor Keys can enforce limits such as a maximum number of licenses or the creation of trial versions only.

Are end-users able to control license usage?

Network administrators can cancel licenses in order to redistribute among users or revoke idle licenses. This provides administrators with the ability to control optimal license use across the enterprise.

How can I get started with Sentinel Keys?

We offer a Software Development Kit that you can use to test the creation and implementation of software protection with a Sentinel Hardware Key. Our starter pack includes the software and 10 keys.

Why should I choose SafeNet?

Only SafeNet offers a complete suite of services and products for your entire software lifecycle. With SafeNet, you can protect and enable revenue, automate fulfillment and ongoing management, and monitor and mitigate piracy threats. SafeNet also offers superior worldwide technical support via telephone, email and Internet. Our SafeNet Service Guarantee ensures that you consistently receive the highest level of service. SafeNet is the industry leader in software protection, securing over 40 million licenses. We understand emerging technologies, including the features you want in order to enable the best protection for your software products.

Sentinel Hardware Keys v1.2

What is integrated license fulfillment?

Integrated license fulfillment allows customers to integrate SHK into their fulfillment process through the use of back office APIs. This provides the customer the ability to integrate software-based security licensing into their products without interruption to their existing business model. APIs allow vendors to expose functionality without providing an actual application. Back office APIs allow vendors to create applications to program the SHK. They are termed “back office” because the information stored in a token defines how the software application behaves.

What is the benefit of back office APIs (also referred to as integrated license fulfillment)?

Today, software publishers program SHKs using the application provided by SafeNet. This requires them to manually program each SHK. When dealing with mass quantities of keys, manual programming can be costly and inefficient, not to mention inconvenient. Back office APIs allow software publishers to program SHKs using their own internal applications, providing them more independence and flexibility. This facilitates automation and a greater degree of autonomy with their internal manufacturing and delivery systems.

What is a secure remote update?

Software publishers distribute keys out in the field to be used with their products. Over time, customers' security implementations may change, or they may need to distribute new updates to their products. These changes may require the software publisher to update the deployed SHK. The process of updating SHKs remotely means software publishers are not required to recall keys or send new keys every time their security implementations require change. The remote updates are secured to ensure only the intended key is updated.

What is a bi-directional update?

A bi-directional update involves the end-user providing unique information about the Sentinel Hardware Key, which can be used by the developer to provide an update specifically for that key. This means updates cannot be used by any key other than one for which it was intended. Additionally, bi-directional updates can only be used once. Vendors may use a bi-directional update to extend an expiration date or implement a counter to restrict usage. Essentially, it allows you to limit features to avoid misuse.

What is a broadcast update?

A broadcast update can be used to update one or more keys without any information from the end-user. A broadcast update can be targeted toward multiple keys or towards a specific key. These updates can also be reapplied. In turn, they should be limited to features which are not affected by re-use. This refers to data fields stored in a key which do not change, such as an algorithm used for security. An additional benefit of a broadcast update is the ability to ship out blank keys and then program them at a later date out in the field, and in mass quantities.