cpl.thalesgroup.com

Software Protection Best Practices

Deepening the Secure Bond between the Hardware Key and Your Application with AppOnChip

One of the biggest issues software publishers face is how to prevent unauthorized use of their software without creating unnecessary obstacles for customers who wish to legitimately purchase and use it. Software piracy stunts revenue potential and negatively impacts paying customers, who ultimately bear the cost of illegal product use. This is where Sentinel LDK's Envelope comes in—providing proven and easy-to-use techniques for protecting your IP, revenue, and reputation.

Sentinel Envelope wraps your application to provide robust IP protection against reverse engineering through file encryption, code obfuscation, and system-level anti-debugging. It then creates multiple, random layers of protection for each file, making it extremely complex and time-consuming for hackers to remove, ensuring that your software code is safe from exposure while en route to its end-user destination.

AppOnChip—The Most Secure Way to Protect Your Software

The AppOnChip feature of Sentinel Envelope facilitates an inseparable binding of the Sentinel hardware key to the application, providing software publishers with the most secure software protection solution available.

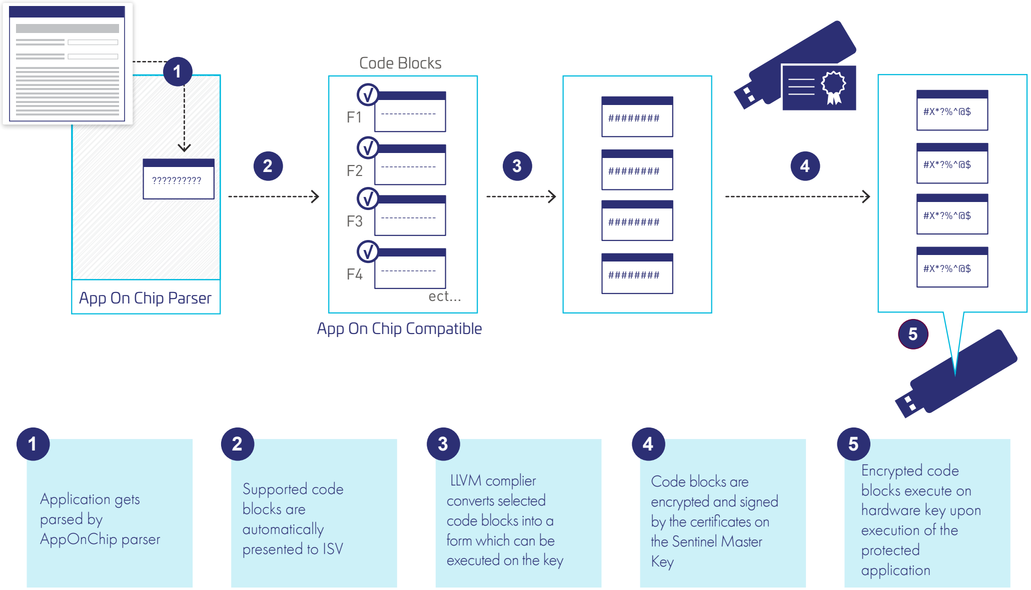
This fully automated process presents software vendors with a list of functions from their application that contain code blocks that are compatible with the AppOnChip feature. The protected code blocks, encrypted and signed, can then be loaded and executed on the hardware key itself. This additional security measure makes it the most secure software licensing implementation in the market. Moreover, this AppOnChip feature can be used to protect both 32-bit and 64-bit native binaries (EXE and DLL files).

Features and Benefits

- **Stronger Security**–AppOnChip provides stronger protection from unauthorized software use by requiring the token to be present for the application to execute.
- **Easy Implementation**–The process of binding the software to the hardware key, analyzing which code can be executed on the token, and converting code into token-executable form is entirely automated—no engineering efforts are required.
- **Maximum Licensing Flexibility**–The protected code blocks do not utilize any of the storage space of the hardware key, ensuring that the ISV has maximum memory available for license storage.
- **End User Transparency**–AppOnChip functionality has no impact on application performance and has no impact on the end user experience.
- **No Operational Burden**–No additional requirements to update the keys in the field if a new version of the software is released.

How it Works—Protection and Execution

Protection-Once the AppOnChip feature is enabled within Sentinel LDK, the unprotected application will get parsed by AppOnChip to analyze all the supported functions. Code blocks from all or several functions, based on ISV selection, get converted to a form that can then be executed on the key. These converted code blocks are encrypted and signed for security.



1 Application gets parsed by AppOnChip parser

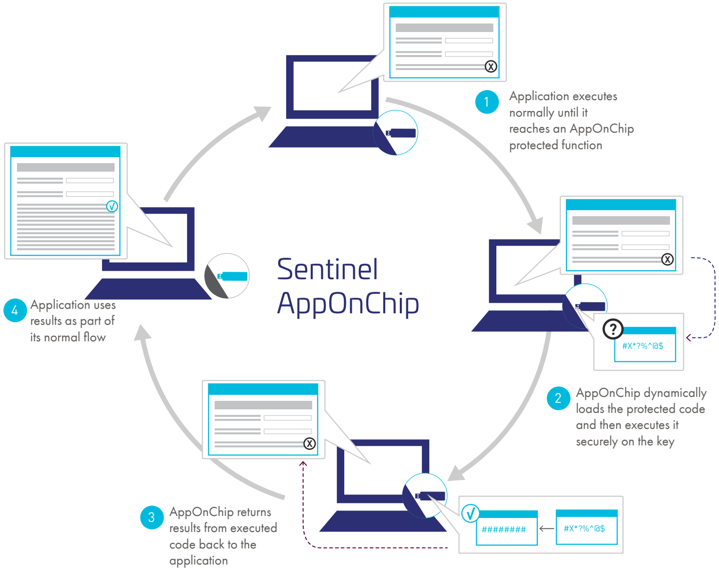
2 Supported code blocks are automatically presented to ISV

3 LLVM complier converts selected code blocks into a form which can be executed on the key

4 Code blocks are encrypted and signed by the certificates on the Sentinel Master Key

5 Encrypted code blocks execute on hardware key upon execution of the protected application

Execution–When an end user attempts to use the software, the execution phase kicks in. The protected software executes normally until it reaches the function protected by the AppOnChip feature of Sentinel LDK. The code flow in the application transfers to the key. AppOnChip dynamically loads and then executes the protected code securely on the key. The results from the executed code are returned back to the application and normal flow continues.



1 Application executes normally until it reaches an AppOnChip protected function

2 AppOnChip dynamically loads the protected code and then executes it securely on the key

3 AppOnChip returns results from executed code back to the application

4 Application uses results as part of its normal flow

Activating the AppOnChip Feature—A Simple 5-Click Process

For Sentinel LDK users, taking advantage of the AppOnChip software protection feature is a simple, 5-click process. Once in the LDK management console, the user will simply:

1. Choose the application to apply the feature to.
2. Select the **AppOnChip** tab.
3. Select the **Enable AppOnChip** check box.
4. Select the software command to apply the feature to. When you enable the feature, LDK will automatically generate a list of compatible commands for you to choose from.
5. Click **Protect** to complete the process.

Visit sentinel.gemalto.com/software-monetization/apponchip/ for more information on the solution or to request a free trial today!

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.