

# **Everything You Need To Know About Maximizing Security & Profitability**

March 2010



1025 West 7th Avenue  
Denver, CO 80204  
1.800.4.KEYLOK  
[www.KEYLOK.com](http://www.KEYLOK.com)

# Everything You Need To Know About Maximizing Security & Profitability

---

## *How to Implement a Dongle Solution to Improve Software Licensing Options, Eliminate Piracy and Increase Your Client's Overall Satisfaction with Your Software.*

If you are a Software Company Executive, Software Developer, or Software Manufacturer and are looking to eliminate software piracy, increase software revenues, or keep better track of how and where your software is being used, this report will show you a way that you can gain complete control over the use of your software, without creating nightmares for your clients, wasting money, or overloading your software support team.

You need to make sure you know the answers to these questions before making a decision on your anti-piracy solution.

1. **How to increase software licensing options?** Competition is fierce. Marketing and product management need flexibility to implement different licensing strategies that will meet the needs of your customers and sales channels.
2. **How to implement a dongle to actually prevent software piracy?** You need to implement a solution that will actually prevent software piracy. There are many things to consider in this evaluation and you need a provider who will act as your partner, not just a software or hardware manufacturer, to help you understand the best methods to ensure the most comprehensive security possible within your own application.
3. **How to increase your client's satisfaction with your software?** Face It. Your clients don't care about piracy. That is YOUR Problem. So, if you integrate the wrong Anti-Piracy Solution into your application and it causes disruption for your clients, they will be furious and you will lose them to the competition!

# **Profits That Lie Hidden In Your Hardware Dongle**

## **What Most People Don't Know**

### **About Hardware Dongles**

Hardware dongles provide more than just cost effective, bulletproof software piracy protection. They provide you with the ability to implement many different options for software licensing to meet the needs of marketing and product management. The user-defined memory on the dongle can be used for usage based licensing, time based licensing, component or module-based licensing, and concurrent user licensing.

## **Usage Based Software Licensing**

### **Overview**

Do you need to limit the number of times a user runs your application or a module within your application for demo purposes or pay per use? You can set a counter in the dongle's user-defined memory and modify the counter it each time the user runs the application.

### **Pay Per Use**

Software manufacturer had a license model where it would get paid for each time the software was used. To implement the model, the software company decided to use a hardware dongle. Based upon the number of uses a customer bought, a counter was set and the software and dongle were sent out to the customer. Each time the customer ran the software, the counter was decremented and the number of remaining uses was displayed to the user. When the count was less than twenty, the customer received a message to order more uses. Once the order was placed, the software manufacturer chose to send a new dongle to the customer pre-configured with the number of uses purchased. The manufacturer could have chosen to use the remote update capabilities of the dongle to update the counter in the field rather than shipping a new dongle.

### **Demo Version**

Software manufacturer needed to provide a demo version to its prospects and it wanted to maintain only one version of the software and limit the number of times the demo could be run. It decided to use a hardware dongle to implement the demo version. When the prospect ordered the demo, the software and the dongle were sent to the prospect. The prospect could evaluate the software for a set period of uses. If the prospect chose to buy the software, the manufacturer updated the dongle remotely and the software was now live. If the prospect needed more time to evaluate the software, the manufacturer updated the count to give the prospect more time to evaluate the dongle.

## **Time Based Software Licensing**

### **Overview**

Do you need to limit the length of time a user runs your application or a module within your application for demo purposes? Do you need to support a rental/subscription model? You can set a date in the dongle's user-defined memory to limit the time period.

### **Rental/Subscription Model**

Subscription based software is becoming more prevalent. A high-end printer manufacturer needed to implement a lease license option. It chose to implement a hardware dongle and set a date on the dongle when the printer was installed at the client's site. Once the expiration date was passed, the client could not use the printer. Once the lease was renewed, the date on the dongle was updated.

## **Demo Version**

Software manufacturer needed to provide a demo version to its prospects and it wanted to maintain only one version of the software and provide a 30-day evaluation period. It decided to use a hardware dongle to implement the demo version. When the prospect ordered the demo, the software and the dongle were sent to the prospect. The prospect could evaluate the software for 30 days. If the prospect chose to buy the software, the manufacturer updated the dongle remotely and the software was now live. If the prospect needed more time to evaluate the software, the manufacturer updated the expiration date to give the prospect more time to evaluate the dongle.

## **Component Based Software Licensing**

### **Overview**

Do you need to control which modules a customer has access to? You can assign a variable in the dongle's user-defined memory to determine which components a customer has access to.

### **Component Licensing**

A CRM software vendor needed to control access to certain pieces of functionality based upon what the client purchased. The software vendor chose to implement a hardware dongle and set variables in the dongle's memory to enable access to certain pieces of optional functionality.

## **Concurrent User Based Software Licensing**

### **Overview**

Do you need to support concurrent users? You can use the hardware dongle to set the maximum number of users. The application can check the number of users against the maximum number of users stored on the dongle to allow or deny access.

### **Concurrent Users Model**

A software manufacturer wanted to offer a multi-user version of its software. It chose to price its software in 20-user increments. It used the hardware dongle to set the maximum number of users. Once the customer reached the maximum number of users, the next user was denied access. If the customer decided to buy more licenses, the software manufacturer updated the dongle remotely to increase the number of users.

## **Software Piracy Prevention Strategies**

### **Which Ones Actually Work...**

**And Which Ones Are Guaranteed To Crush Your Revenues,  
Eat Up Your Profits, Overload Your Technical Support Staff, And  
Send Your Clients Running To Your Competition.**

More and more software companies are implementing security solutions to reduce losses to software piracy. There are three different methods being used; 1) software based, 2) software based using dumb hardware, and 3) software based using smart hardware.

Software based solutions use passwords and registration codes to control access to the software. Protection can be added to your software quickly and with little financial commitment. These solutions do not provide reliable software protection.

Software protection based upon dumb hardware use computer specific attributes to control access to your software. This method uses serials numbers or other attributes of hard drives, network cards, etc. and limit the use of the software to the computer on which it was installed. Protection can be implemented quickly and inexpensively and offer higher security than solely software based solutions but it is inconvenient and problematic for end-users. Any changes to the computer render the software useless and cause increased dissatisfaction from your clients.

Software protection based upon smart hardware offer reliable cost effective protection. Smart hardware, commonly referred to as security hardware dongles, has built-in intelligence and is designed specifically to integrate with your software to offer piracy protection. This solution is difficult to break and does not limit your customer's use of the software. Hardware dongles can be implemented quickly, yet still offer you maximum protection from software pirates. They can be transferred from one machine to another. Licensing and security is tied directly to the dongle, not a piece of hardware on a PC which prevents your customer from using the software on another machine without reregistering the software. Additionally, you eliminate the complicated task of continually updating and modifying software code to stay ahead of the hackers who want to steal your software. You get paid for every copy of software being used and your customers get flexibility.

If you need a software piracy prevention strategy, security hardware dongles offer the only dependable alternative. The remainder of this section will concentrate on hardware dongles. You can protect your application in two ways when using a hardware dongle: 1) Through the use of a wrapper around your executable files, commonly referred to as the Shell method, or 2) through the use of functions which are embedded directly into your application code, commonly referred to as the API method.

## Shell Method

### Overview

The Shell method offers a basic level of security. The Shell is a protective, encrypted layer that wraps the executable file or DLL. It automatically handles functions such as checking and verification by using an internal proprietary algorithm to perform periodic checks for the dongle. An application can only be run if the user has the correct hardware key.

### Benefits

It doesn't require programming skills and can be applied in a matter of minutes.

### Costs

You do not have control over the protection implementation. It provides only a single layer of protection which is more susceptible to being hacked. If the protection is broken on any software using this methodology, a generic hack can be made available and be applied to your application.

### Use

The Shell method should only be used:

- if you do not have access to the source code but need a protection method,
- as a temporary protection solution when you have delayed your software protection decision and are short of time and need to get your product shipped, or
- in conjunction with the API method.

## API Method

### Overview

The API method allows you to devise protection specific to your application. There are an infinite number of combinations of embedding functions throughout the source code of your application to configure your security. Your needs and the creativity of your developers is the only limiting factor. The more unique calls hidden within your source code, the less vulnerable you are to hackers.

### **Benefits**

You have complete control over the security protection implementation. You decide which modules or features you want to protect, how you protect them and when you want to protect them. Even if another software vendor's product is hacked, your application remains secure.

### **Costs**

This method requires development time to design and implement security protection. Typically, you need to budget 4 – 8 hours of development time for each module you want to protect.

### **Use**

The API method should always be used when you have access to the source code.

## **The #1 Most Common Mistake In Implementing a Dongle**

### *A Little Goof That Cost A Software Developer His Job*

By only checking for the presence of the dongle when your application is started, you leave hackers an opportunity to break your security. You want to make your software application impenetrable. There are many ways to strengthen your security implementation and eliminate unauthorized use of your product.

# **The Top 10 Things to Do When Implementing Hardware Based Security Protection**

1. Periodic checks should be placed in your application to assure the continued presence of the dongle. This is to prevent someone from moving the dongle to another computer after your application has started in order to run multiple copies of your program using a single dongle.
2. Add code to your application to prevent the attachment of a debugger prior to running your application. Add code to check for the presence of kernel level debuggers and disassemblers.
3. The distributed application should have all meaningful function names removed from the executable. There are utilities available to 'scrub' these names from distributable files. Some compilers also have settings that reduce the amount of information (i.e. visible names) present in the final executable. It is very important that all debugging information be removed.
4. Distribute the dongle related calls within the protected application to gain a higher level of protection. If all calls are contained in a single place with consecutive lines of code, the easier it is for a hacker to understand what is happening and implement a 'solution' to bypass.
5. Delay the response to an API call. Run additional code within your application and then use a different subroutine to evaluate the results. This hides the security related code and makes it difficult for the hacker to understand what is happening.
6. Avoid a direct comparison of results to expected values. A comparison of this type with a jump to one block of code on success and a different block of code on failure is the easiest for a hacker to bypass. Use data conversion algorithms before performing comparisons. This ensures removal of the API call disables your application.
7. After you have determined there is a security violation problem, and prior to the actual 'check' in your code you should perform a series of operations that would render the operation of your program useless (e.g. reinitialize variables to invalid values, etc). The objective is to prevent a simple code change at the point of your final check to branch to the success instead of the failure block of code as a means of bypassing the security.
8. Vary the activities performed with the dongle based upon the day of the week/month/year, etc. Using this technique if someone successfully found a way to hack around the dongle today, then

the application would fail tomorrow due to the additional/different checks being performed that weren't bypassed during the original hacking operation. After several sequential encounters of this type, most hackers would eventually abandon the bypassing process.

9. Messages within your application which indicate to the hacker the proper dongle is not present should be encrypted within the distributed application in order to prevent them from being found by simply searching the file, and then working backwards from the message to alter the go/no-go switch within your program.
10. Combine the Shell and API method within your application.

## 3 Critical Characteristics To Demand From Your Dongle Manufacturer

### Does yours stack up?

Your clients do not care about software piracy. That is your problem. They do not want to encounter problems due to an anti-piracy solution you implement. They just want your application to work as advertised.

Incorporating a software anti-piracy solution into your product is a big step for you. You want the process to be hassle-free, fast and profitable. You are running a business, not trying to figure out how a dongle works. You need to make sure your software security partner makes the anti-piracy process hassle-free, fast and profitable for you and is as committed to your success as you are.

Demand these 3 critical characteristics from you software security partner to ensure your software piracy prevention implementation solves your problems and does not impact your clients.

1. **Easy to do Business With.** *Can you get your questions and issues resolved quickly without wasting your valuable time?*
2. **Guaranteed Fast Turnaround.** *How long will it take to get your order filled?*
3. **Stand Behind Their Product.** *What happens if something goes wrong with the dongle?*

## Ease of Doing Business With

You have enough to worry about. You need a hassle-free solution and partner. Make sure the partner you choose makes it easy for you in these key areas.

### Support

What happens if you have a problem? What if one of your end-users needs help? Will your manufacturer's support process force you into an email dialogue which leaves your client up the proverbial creek, or will they work immediately and directly with you and your clients to resolve the issue quickly? Make sure your questions, concerns and problems are answered quickly and accurately so you can provide your clients with the support they demand.

What about their support staff? Are they certified developers? Do they have the expertise and experience to help you and advise you with your unique integration? What kind of ongoing education and certification standards are in place? Do they have high turnover? Your clients expect you to solve their problems right the first time so make sure your manufacturer has the ability and expertise to support you and your clients.

### Order Fulfillment

What is the order fulfillment process? How easy does the manufacturer make it to order dongles? How long does it take to fill your order? Are there multiple shipping options available? Does the manufacturer keep you informed about the status of your order? Is there a guaranteed turnaround time? Accurate,

fast order fulfillment is important when you are waiting to ship your product to your end-user. For example, what would happen if you had an unexpected large order at the end of the month or quarter and you were out of dongles? You need them the next day so you can ship your software and recognize the revenue. Can you get them the next day or do you have to wait 3 – 5 days before you receive them so you can ship your software? Delays infuriate your client and your CFO!

## **Guaranteed Fast Turnaround**

Choosing a partner means you are now dependent upon someone else. You no longer have control. Make sure your partner is committed to your success and your client's satisfaction by guaranteeing timeframes for responses to your questions and issues and order fulfillment.

### **Customer Support**

Does the vendor guarantee a response within a certain time frame? If not, what should your client expect? You call support when you or one of your clients has a problem. Make sure you are not left waiting and wondering. Your client will not accept the "we're working on it" response. They want an answer right now. Don't put yourself in an undesirable position. You need a manufacturer who will support you and your clients in a fast, responsive way.

### **Order Fulfillment**

How long does it take to fill your order? Is there a guaranteed turnaround time? You should expect, **No Demand**, your orders be filled the day the order is placed or at least within 24 hours of placement. Fast order fulfillment means you never have to wait to ship your product to your end-user.

## **Stand Behind Their Product**

The more commitments the manufacturer makes to stand behind its product, the more confident you can be it will work right the first time. Get answers to these important questions to know how committed the manufacturer is to your success.

### **Quality Assurance Process**

What does the manufacturer do to ensure quality? What type of testing is done before the dongle is shipped to you? The quality assurance process has a direct impact on the number of dongles which fail when shipped to you or your clients, otherwise known as the field failure rate. If the dongle manufacturer has a stringent quality assurance process, you should expect a very low field failure rate.

### **Field Failure Rate**

What is the field failure rate of the type of dongle you need? What is the lifetime field failure rate of the manufacturer? The field failure rate has a direct impact on your customers. If the dongles are failing in the field, there will be significant impact on your ability to ship your software or your customer's ability to run your software. You want a very low field failure rate.

### **Warranty/Guaranty**

What type of warranty is provided? How long do you need the dongle to last? The warranty should match your expectations.

### **Replacement Policy**

What do you have to do to get a dongle replaced? What if the dongle does not work? Does the dongle manufacturer make it easy for you to get a replacement or do you have to jump through several hoops just to get it replaced? You should only have to pay for dongles which actually work. Vendors should offer a no questions asked replacement policy if they stand behind their products.

If the manufacturer thoroughly tests its product, has a very low field failure rate, you can know it is committed to you and your client's success.

# ***What Nobody Ever Tells You About Anti-Piracy Solutions!***

What do you need to know to evaluate anti-piracy solutions? It is difficult to get this information. All of the manufacturers want to tell you why their solution is right for you. At KEYLOK, we have provided you with this report to help you make the right decision.

As a review, the three key questions to answer to maximize your security and profitability when implementing anti-piracy solutions are:

1. How to increase software licensing options?
2. How to implement a solution to actually prevent software piracy?
3. How to increase your client's satisfaction with your software?

If you need to implement different licensing options or ensure your anti-piracy solution is reliable, then software based solutions utilizing smart hardware (i.e. dongles) is an alternative requiring further investigation. The user-defined memory on a dongle can be used to implement licensing options to help you grow your business and differentiate yourself from your competition. Dongles provide cost effective reliable security by combining the Shell and API methods of protection.

Client satisfaction when implementing a dongle-based solution is dependent upon choosing the right dongle manufacturer. Choosing a manufacturer who addresses the three critical characteristics ensures the impact is positive rather than negative.

If you are considering a dongle-based solution, then you need to read on.

## **How to Evaluate Hardware Dongle Solutions... The Top 15 Things to Demand of your Dongle Manufacturer**

### ***Free Dongle Evaluation Checklist***

At KEYLOK, we realize that incorporating a software anti-piracy solution into your product is a big step for you. We also know you are running a business, not trying to figure out how a dongle works. That's why we've committed ourselves to making your anti-piracy process hassle-free, fast and profitable. You are making a very important decision when choosing your software security partner and you only want to make this decision once. You do not want to make a mistake that will cost you your job. Make sure you know the answers to these questions before making a decision on your anti-piracy solution.

You can get your "*Dongle Evaluation Checklist*" at [www.KEYLOK.com](http://www.KEYLOK.com).