THALES

Manufacturing Process Control:

An essential guide for protecting your intellectual property and bottom line

WHITE PAPER

Peter DiToro
VP, Advanced Solutions Group
Thales e-Security

TABLE OF CONTENT

INTRODUCTION

Volatile economic conditions have driven manufacturers in all industries to reassess traditional product sourcing models. Global competition has driven the end user price of manufactured goods consistently downwards over the past decade. As a result, offshore production has become a fact of life in manufacturing today. Some telling statistics outline the macro impact of these trends. The U.S. trade deficit in goods and services widened substantially during the last decade, both in nominal terms and relative to GDP. Imports from developing countries have accounted for most—and an increasing share—of the growth in imports in recent years. From 1989 to 2000, 56 percent of the growth in non-oil imports came from developing countries; from 2000 to 2007, developing countries accounted for 70 percent of U.S. import growth. The increase from China was particularly dramatic: imports from China, which made up just 13 percent of the growth of non-oil imports from 1989 to 2000, accounted for 39 percent of the growth from 2000 to 2007[1].

Granted, by shifting production to China, India, Mexico, and other locations, U.S. manufacturers can reduce operating costs, improve return on invested capital, appease shareholders, and quickly enter and exit growing or mature markets. However, along with the obvious benefits of low wages, lack of effective worker unionization and significant financial incentives comes an increasing degree of risk to the security of intellectual property. The illegal production of counterfeit, off-brand, or gray market products by unscrupulous manufacturers has become a significant problem that can have a potentially devastating effect on a manufacturer's bottom line. Outsourcing in China, for example, has become one of the biggest threats in the realm of product piracy. Illicit phones comprise a staggering 40% of Chinese firms' production, and 13% of the world's, according to iSupli, a research firm. It reckons China will produce 145M of them this year, up by almost half since 2008[2].

---

1. Susan N. Houseman, "Measuring Offshore Outsourcing and Offshoring Problems for Economic Statistics", W.E. Upjohn Institute for Employment Research, January, 2009

2. "Counterfeit handsets proliferate in China: Talk is cheap", The Economist, Nov 19th 2009

Organizations such as the Alliance for Gray Market and Counterfeit Abatement (AGMA) have sprung up as outsourcing manufacturers attempt to circle the wagons to protect their bottom lines from piracy, counterfeiting, gray markets and other euphemisms for what we all know to be simple theft of intellectual property. As value has shifted from traditional "metal bashing" forms of manufacturing to high design and intellectual property content, the thrust of piracy has moved with it.

This white paper will discuss the steps that product manufacturers can take to confront the realities of product piracy. It will also explore how technology can be one of the key ingredients in the "manufacturer's self defense kit." Specifically, this paper will illustrate how the use of the Public Key Infrastructure (PKI) to create, distribute, embed, and validate cryptographically strong product identifiers is emerging as a best practice. It will show how the PKI family of technologies and products utilize strong cryptography to protect intellectual property and to identify end entities, be they people, crates of pharmaceuticals, or high tech products.

THE CHALLENGE: CONTROLLING THE OFFSHORE MANUFACTURING PROCESS

In most Western countries a web of laws and the court systems and procedures that enforce them protects intellectual property. If a Western manufacturer, for example, produces an exact knockoff of a patented or copyrighted product, the IP owner can pursue the counterfeiter in court and most likely prevail. In the West, we call this "the rule of law". In China, for example, laws are opaque and the processes for enforcing them are either nonexistent or inaccessible to the aggrieved victims of product knockoffs. In fact, the Chinese government protects its domestic knockoff industries; they are important parts of the local economy.

As a testament to the embedded nature of the product piracy business in the Chinese economy, consider the recent attempts by Western countries to encourage China to sign up for the Anti-Counterfeiting Trade Agreement. As recently noted in *The Economist*, "But in China, where 80% of the world's fake goods are thought to be produced, officials are loath to crack down on a thriving local business. China is not expected to sign ACTA (Anti-Counterfeiting Trade Agreement) — undermining it before it has even been unveiled. Perhaps China could make a just-as-good fake treaty instead."[3]

Against this backdrop, global manufacturers are trying to fight product piracy through various strategies and policies developed by both government-sponsored and industry groups. The Coalition Against Counterfeiting and Piracy, formed by business members of the U.S. Chamber of Commerce's Global Intellectual Property Center, recommends four key best practices against counterfeiting in its *Intellectual Property Protection Enforcement Manual: A Practical and Legal Guide for Protecting Your Intellectual Property*. Some brief highlights include:

- **Secure Legitimate Inputs** – Use only suppliers that are company-authorized and that are proven to source directly from OEMs or "first owners of goods."

3. "Knock-offs catch on", The Economist, Mar 4, 2010

- **Verify Legitimacy of Customers and Distributors** – Educate the sales force to be alert to customer actions that are suspicious, such as an unusually large order for the customer's needs.
- **Manage Waste and Inventory** – Deter the theft of damaged or inferior products by having them destroyed, and having a factory account for all unused raw materials.
- **Ensure Legitimacy of Purchased Products** – Educate buyers on how to recognize a legitimate product. In the shipping process, verify that packaging, case markings, and pallet configurations are authentic. Also, use bar coding or Radio Frequency Identification (RFID) for tracing and tracking.

In the private sector, the Alliance for Gray Market and Counterfeit Abatement (AGMA), a non-profit organization dedicated to dealing with the gray marketing and counterfeiting of technology products around the globe, recommends similar strategies. AGMA also promotes the use of a serial number tracking program with the goal of increasing the visibility of the flow of products all the way from the manufacturer to the end user. Best practices for product returns and replacements and warranty claims, as well as reseller audits and accurate record keeping are also recommended to combat product pirates in the gray market.

While these and other recognized methods might reduce counterfeiting over time, they can't adequately protect a company's brand and profits from counterfeits and gray markets. To be effective against counterfeiters, some global manufacturers are pursuing a radically different approach to manufacturing process control. The solution: encrypted digital certificates and signatures.

The same technology solution used to secure Internet banking connections and modern electronic passports can enable companies to identify and validate the authenticity of components throughout the manufacturing process anywhere in the world. Encryption technology is one of the key ingredients in the "manufacturer's self defense kit" against product piracy. Specifically, the use of the Public Key Infrastructure (PKI) to create, distribute, embed, and validate cryptographically strong product identifiers is becoming increasingly common. The PKI describes a family of technologies and products that utilize strong cryptography to protect intellectual property and to identify end entities, whether they are people, crates of pharmaceuticals, or high tech products.

REGAINING CONTROL WITH A PUBLIC KEY INFRASTRUCTURE

Just a decade ago, deploying a PKI to protect valuable IP from the world's counterfeiters was a project for the technically expert, not one for the faint of heart. Given its complexity and immaturity, simple solutions that could be deployed in developing country manufacturing operations were expensive and complex, often beyond the capabilities of the average product development organization. This is no longer the case. The technology has matured, standards are in place, and expertise is readily available, as are the components of the PKI. For example, Microsoft includes the core Certificate Services with its Server 2008 products at no additional charge, removing a cost from the deployment of a production quality PKI.

As we enter the second decade of the 21st century, there are fewer constraints than ever on the use of advanced cryptographic technology in protecting the interests of manufacturers offshoring to developing countries where piracy is endemic. The concepts are simple:

1. Determine the range of goods and corresponding quantities to be produced in a given manufacturing run. Generate a digital marker (a digital certificate in PKI terminology) for each unit based on a unique identifier. This should be generated in the home country.

2. Encrypt the data that defines the product run, also completed in the home country.

3. Put a trusted computing device, one that cannot be hacked, into the outsourced manufacturing environment. Program it so that it is the only device that can decrypt and manipulate the digital certificates that correspond to the contents of the production run.

4. Require your manufacturing entity to interface its shop floor system to the instructions output from the trusted device. This is a relatively simple procedure.

5. Ship the manufacturing instructions and unique product identifiers via encrypted communications channel to the remote site where the goods will be produced.
6. Insert a digital certificate into each corresponding device during manufacture.
7. Audit the production run to make sure they are not making duplicates.
8. Use each device's digital certificate to authenticate the product once it is put into service. Each device can present its certificate to your customer service portal (or other authentication mechanism). Those devices with a genuine certificate can be serviced; those with duplicates or without certificates are fakes.

The ability to validate digital certificates over time is a key component of the PKI. While intended for use by people (as in signing electronic contracts) it works every bit as well for devices. This is the same technology behind the U.S. Government Common Access Card (CAC) and the European standard for electronic passports as established by the Brussels Interoperability Group (BIG). In addition, it is commonly used in cable set top boxes to control digital downloads. It can, in addition, be used to check and balance the tendency of offshore manufacturers to pirate copies of products while manufacturing them.

TECHNOLOGY COMPONENTS

To put the process into practice, organizations will need to install and integrate a number of core components. These include:

Manufacturing Device Certificate (MDC) issuing sub-system

This sub-system is responsible for initial generation of all the RSA key pairs used by the key delivery system and would typically be deployed in the company's "home" facility, for this example let's assume it is in the U.S. This is the heart of the PKI, where unique identifiers are created, starting the chain of digital track and trace. In this example, the MAC address of the product (a unique identifier built into all devices that must access a network) is used as the unique identifier for each unit.

There are three components in this sub-system: certification authority (CA) module, MDC module and MAC authorization module:

- **Certification Authority Module**: This module is deployed in the "home" facility and its sole purpose is to interact with the MDC module to issue manufacture device certificates (MDCs). A hardware security module (HSM) is used to host the issuing CA's private signing key. This device is the "master controller" for the solution.

- **MDC module**: This module is also deployed in the U.S. facility, and its purpose is to verify the signed MAC address list submitted by the MAC authorization module. Once the digital signature on the MAC address list is successfully validated, the MDC module will generate the required number of RSA key pairs along with their corresponding certificate signing requests. All RSA private key objects will be generated and stored in a pre-configured secure key management system (KMS).

- **MAC Authorization module**: This module can also be regarded as the CA's registration authority, the means by which devices are "registered" with the system so that they can subsequently be issued digital certificates. The module will be deployed in the offshore manufacturing facility, and the production control

function is responsible for authorizing the submission of the MAC address list to the MDC module deployed in the home office facility. One employee or a number of trusted employees must manage the MAC authorization module in the manufacturing facility. It is considered best practice to use the built in access controls of the RA to enforce separation of duties at this phase in the process. A signing key hosted by a HSM is assigned to the trusted employees. The access to the signing key is controlled by smart card-based, two-factor authentication along with a quorum to ensure maximum security. All MAC address lists submitted to the MDC module must carry a valid digital signature created by the signing key.

MDC secure transfer sub-system

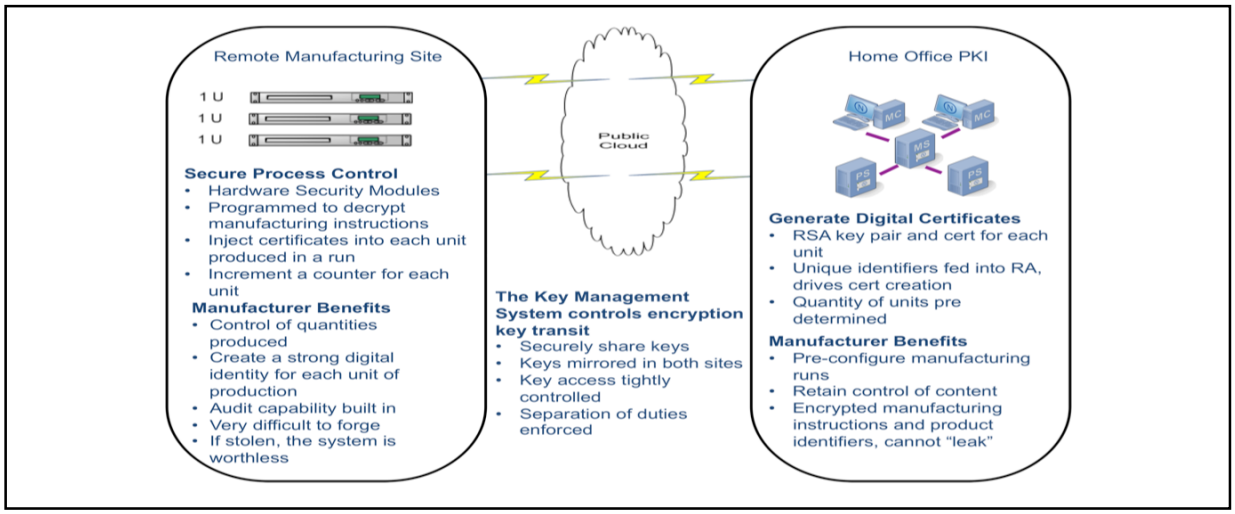
This sub-system is responsible for securely transferring all the MDCs along with their corresponding private keys from the home facility to the manufacturing facility. The methodology used by the sub-system to manage key transfer should be based on a robust KMS so integrity of encryption keys is maintained while access to them at the appropriate place in the process is assured.

The KMS should be capable of configuring a shared key store that can be accessed from both the home office and the remote manufacturing facility. The single KMS logical structure will enable any cryptographic key generated by the system to be used at either location. Based on this model, the transfer of MDCs and their private key objects can be viewed as simple as file transfers between the two locations. During the transfer, all private key objects will remain encrypted and will not need to be exported outside of the KMS logical structure.

MDC certificate injection sub-system

This sub-system is responsible for the final MDC/key delivery from the secure repository to the production unit device. To secure the end point, which is by definition to be deployed in a hostile environment, a programmable HSM can be configured then signed and encrypted by keys managed by the master HSM. The programs in the remote HSM will only execute in an HSM that has the proper KMS configuration. The HSM needs to be installed either at the secure repository server or a separate workstation that will function as a key

delivery server. The server running the MDC certificate injection system must have an HSM installed and pre-configured to share the same KMS used by other sub-systems.



The interoperable units that comprise the KMS make generations of unique identifiers and corresponding digital certificates for production runs simple and secure. The HSM executes instructions inside of a tamper proof device that is rated by NIST as adhering to the most stringent cryptographic standards. One of these devices can be placed in the contract manufacturing facility with full knowledge that the process and intellectual property it contains is impervious to tampering even by the most diligent forgers. Experts can help to design, configure and deploy the solution relieving organizations of the need to acquire specialist cryptographic skills.

Polycom protects VoIP devices with digital certificates

Polycom, Inc., a California-based global leader in telepresence, video, and voice solutions, wanted to find an easier and more robust alternative to passwords for authenticating and identifying their VoIP phones on customer and service provider networks. Another reason for the change – a password-based process did not protect against phone manufacturers making counterfeit devices. If VoIP phones can be "forged," Polycom's customers were at risk of incurring fraudulently placed and inaccurately billed calls by unauthorized users on the network.

Polycom's decision makers chose digital certificates and encryption keys generated and secured by Thales hardware security modules. The digital certificates are issued as part of the manufacturing process. Thales developed a solution that generates encryption keys secured by Thales hardware security modules (HSMs) and uses a Microsoft certificate authority (CA) to sign digital certificates at Polycom's data center in North America. Then the keys and certificates are transferred to the Thales HSM in Polycom's manufacturing facility in Thailand. There, the keys and certificates are stored encrypted until they are placed in a newly manufactured VoIP phone.

The bottom-line benefits: reduced risk of counterfeits and increased sales opportunities as Polycom can confidently deliver a higher level of security with more ease of setup and use of their VoIP devices.

CONCLUSION

While today's recommended best practices for overseas manufacturing have made great strides in protecting against product piracy and gray market sales, they are only as effective as the diligence of the people who follow them. Using encryption technology and digital certificates in a PKI throughout the manufacturing and distribution processes enables the products and components to literally protect themselves automatically.

Deploying a PKI to protect intellectual property not only makes the manufacturing and distribution processes safer, but also brings consumers a higher level of confidence in the products they purchase. At Thales, we have found that our customers have benefited from our nCipher encryption key solutions in the following ways:

- Stopped gray markets by validating the source and authenticity of products at the time of manufacture
- Enforced licensing and validity by enforcing license validity periods with digital signatures
- Detected counterfeits by identifying counterfeited products or components when connected to other enabled products or the Internet
- Ensured trusted operation of the product by verifying the authenticity of networked or connected products to meet customer expectations

In these ways, product manufacturers can move beyond traditional marketing, labeling, loss prevention, and channel management to a more sophisticated and ironclad technology approach. By having this greater control over the manufacturing process, organizations can better safeguard the integrity of their products, while also protecting their profit margins, sales channels, and customer trust.

FOR MORE INFORMATION

For more details on Thales security solutions for manufacturers, please contact manufacturing@thalesesec.com or visit www.thalesesec.com/mfgpr

About the Author

At Thales e-Security Mr. DiToro manages a team of more than 40 technical and support sales professionals for the delivery of complex cryptographic solutions to the Fortune 1000. Prior to joining Thales, Mr. DiToro was the founder of the Professional Services team at nCipher, which was acquired by Thales in October 2008.

About Thales

Thales is a global technology leader for the Aerospace and Space, Defense, Security and Transportation markets. In 2009, the company generated revenues of 12.9 billion Euros with 68,000 employees in 50 countries. With its 25,000 engineers and researchers, Thales has a unique capability to design, develop and deploy equipment, systems and services that meet the most complex security requirements. Thales has an exceptional international footprint, with operations around the world working with customers as local partners. www.thalesgroup.com

The Information Technology Security activities of Thales

Thales is a leading global provider of data encryption solutions to the financial services, high technology manufacturing, government and technology sectors. With a 40-year track record of protecting corporate and government information, Thales solutions are used by four of the five largest energy and aerospace companies, 22 NATO countries, and they secure more than 70 percent of worldwide payment transactions. Thales e-Security has offices in France, Hong Kong, Norway, United States and the United Kingdom. For more information, visit www.thalesgroup.com/iss.