**Turning the Tables on Product Counterfeiters with Encryption Technology**

By Peter DiToro

Vice President, Advanced Solutions Group

Thales e-Security

Offshore production is a fact of life in manufacturing today. However, with offshore 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.

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 20081.

How can U.S. manufacturers fight back? One company that is doing just that is Polycom, Inc., a California-based global provider of telepresence, video, and voice solutions, and the creator of the iconic triangular-shaped conference phone. Polycom wanted to find an easier and more robust alternative to traditional passwords for authenticating and identifying their VoIP phones on customer and service provider networks. Another reason for the change – a password-based process offers little protection against phone manufacturers making counterfeit devices. If VoIP phones could be “forged”, customers were at risk of incurring fraudulently placed and inaccurately billed calls by unauthorized users on the network. Obviously, that could mean lost business and a damaged brand reputation.

The security challenge for Polycom, and any manufacturer, always begins on the offshore production line. Overcoming the threat of losing market share to product counterfeiting by hostile offshore manufacturers was the company’s primary goal. Taking a groundbreaking step, Polycom wanted to develop a secure end-to-end manufacturing process using encrypted digital certificates.

**The best defence: encrypted digital certificates**

To date, manufacturers have defended themselves by pursuing some key best practices against counterfeiting: secure legitimate inputs, verify legitimacy of customers and distributors, manage waste and inventory, and ensure legitimacy of purchased products. Unfortunately, these recognized methods can't provide adequate protection unless they are supported by technology and a process that enables audit and control of the supply chain. The best defence for U.S. manufacturers today: encrypted digital certificates and signatures.

Using encrypted digital certificates and signatures is a radically different approach to manufacturing process control, and one that is proven to work. They leverage the same technology solution used to secure Internet banking connections and can also be found in modern electronic passports. As such, they enable companies to identify and validate the authenticity of components throughout the manufacturing process anywhere in the world.
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.

Just a decade ago, deploying a PKI to protect valuable IP from the world’s counterfeiters was an expensive and complex project even for the technology savvy. This is no longer the case. PKI technology has matured, standards are in place, and expertise is readily available, as are the components of the PKI.

**New best practices for fighting counterfeiters**

Today, there are fewer constraints than ever on the use of advanced cryptographic technology for protecting the interests of manufacturer’s offshoring to developing countries where piracy is widespread. The best practices of using this technology are simple, but can have powerful results for offshore manufacturers:

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.

Polycom’s decision makers chose digital certificates and encryption keys generated and secured by Thales hardware security modules (HSMs). 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 as part of the manufacturing process.

Overall, deploying a PKI solution to protect intellectual property has made the manufacturing and distribution processes safer for Polycom, thereby reducing the risk of counterfeit VoIP phones. In addition, Polycom’s customers enjoy a higher level of confidence in the VoIP products they purchase, and that has resulted in increased sales opportunities for Polycom. Like Polycom, any manufacturer can achieve these benefits by using PKI in offshore manufacturing processes to:

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

The battle against offshore counterfeiting can be won – but only if manufacturers move beyond traditional marketing, labelling, loss prevention, and channel management methods to a sophisticated PKI solution within the manufacturing process. By ensuring the authenticity of all components throughout the manufacturing process, product manufacturers can effectively turn the tables on counterfeiters and gray markets and protect their intellectual property and bottom line.

**About the Author**

At Thales e-Security ([www.thalesgroup.com](http://www.thalesgroup.com)) 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.

*1 “Counterfeit handsets proliferate in China: Talk is cheap”, The Economist, Nov 19th 2009*