Defending Against Grey-market Fraud

protecting your business and your brand

THE CHALLENGE

According to a recent KPMG white paper titled *Managing the Risks of Counterfeiting in the Information Technology Industry*, approximately 10 percent of all the technology products sold around the world today are counterfeit.

It's a troubling statistic—not only because those illegal sales amount to hundreds of billions of dollars, but also because counterfeit products jeopardize the brand integrity and reputations of companies whose goods have been copied. As KPMG states it:

> **Counterfeits not only compete with authentic products for revenue, [but] they can also harm a brand's marketplace equity, leaving the brand-holder with the problem of diminishing demand and rising product support costs.**

The issue of counterfeiting is even more problematic for producers of devices used in conditional access and digital rights management schemes such as digital transmission content protection (DTCP), high-bandwidth digital content protection (HDCP), and content protection for recordable media. That's because such devices operate within a larger, protected content-delivery system where the security of the whole system depends on the security of each individual part. In such cases, counterfeit devices pose a serious threat to the entire business structure.

The two most obvious questions emerging from this are:

1. **How do products become susceptible to counterfeiting?**
2. **More importantly, how can counterfeiting be prevented?**

As the following scenario reveals, there are several points throughout the manufacturing process at which products become vulnerable to counterfeiting. Fortunately, Certicom KeyInject™ provides an elegant and streamlined solution that addresses the full range of risks and restores control to the original device creator.

THE RISK SCENARIO

For the sake of illustration, consider a fabless semiconductor manufacturer whose chipset—after being produced by an offshore fabricator—is used in an OEM's satellite radio units. There are essentially four steps in the manufacturing process: fabrication, wafer testing, packaging and assembly, and, eventually, integration into the satellite radios.

As the following shows, opportunities arise at virtually every one of these steps for counterfeiters to skim off legitimate products and route them through to the grey market:

- **Excess chipsets produced through overruns at the fabricator stage can be secreted away to grey-market wafer test facilities and streamed through to a grey-market OEM, embedding the fabless manufacturer's technology in an illegal satellite radio product.**

- **Misreported yields at the wafer test stage can lead to similar leakage: the tester reports a lower number of chipsets passing inspection and diverts the balance to a grey-market packaging and assembly operation.**

- **A similar scenario plays out if the counterfeiting scheme begins further down the line at the packaging and assembly stage, with diversion of product directly to the grey-market OEM.**

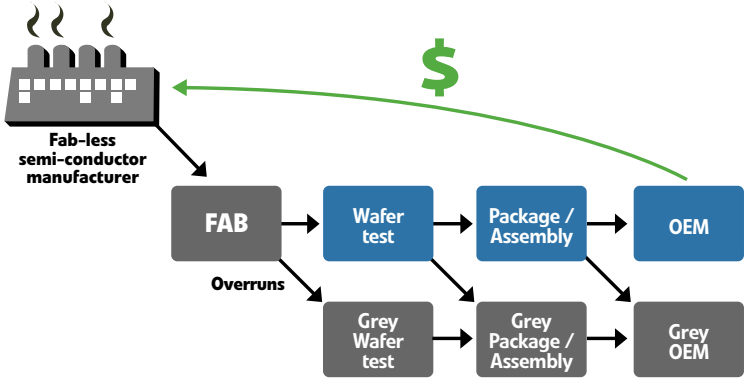

FIGURE 1. Opportunities arise at every step of the manufacturing process for counterfeiting.

In each case, it is not only the technology that is being siphoned off, but also the *security* built into each chipset. This is because each contains a legitimate electronic key that is intended to identify, protect and authenticate the end-user device in a unique way. There is no way to deny service to a counterfeit device that contains a legitimate key—and so the security of the overall content-management system is compromised.

THE SOLUTION

According to KPMG, one of the first steps toward ensuring security is to "design in and employ copy-resistant and anticounterfeit technologies on all products." Core functions relating to this include secure boot, service lockdown mechanisms, remote provisioning and service-activation capabilities—all of which are built-in processes or capabilities to protect the device, the data it stores, and the content it is (or is not) entitled to access. Securing the boot process ensures that rogue software does not compromise or overtake device systems on startup. Service lockdown mechanisms come into effect automatically if the device falls prey to malicious attack, cutting off access to protected content and services. Remote provisioning and service-activation capabilities ensure the authenticity and validity of downloaded code—firmware upgrades and the like.

To project trust from the hardware trusted platform upwards through the boot process requires a chain of hardware and software authentication for each of these components. This demands a fairly complex boot logic. Software is required to access protected memory, and to analyze firmware stored in flash with respect to code-signature locations and the actions to take when code fails the integrity check. Essential to the whole configuration is the inclusion of tamperproof encryption keys embedded in the device silicon.

Incorporating a cryptographically wrapped key-injection system allows device vendors to retain control over keying material without impeding the necessary distribution of data throughout manufacturing.

What is important to ensure is that not only the keying material itself but also the channels for transporting and delivering the keying material are secure. This requires that the security core be designed in before the mask is delivered to the fabrication facility to protect the entire chain.

The KeyInject process

Certicom experts assist with the implementation of Certicom KeyInject, recommending mask security enhancements including features capable of verifying the encryption keys that are to be injected at the fab (such as one-time programming (OTP) bits for signature storage).

Key batches are generated by the KeyInject key engine and secured by the vendor's head-office key controller. Sub-batches are then shipped periodically to the fabrication, testing or packaging locations as required; this controls the quantity of keys distributed at any one time.

Shipped-out keys are stored in a secure, remote KeyInject appliance installed at the fabrication site. This appliance works in tandem with a KeyInject software agent, that resides in the SOC Chip Tester that requests keys as needed and injects them into each wafer; it also burns in a high-strength, low bit-count signature at either the wafer test, packaging and assembly or OEM stages.

Every successful injection automatically results in a log entry that can be configured according to the vendor's needs (e.g. to include part serial number, subcontractor identifier, testing line identifier and more). These logs are secured all the way back to head office and cannot be tampered with.

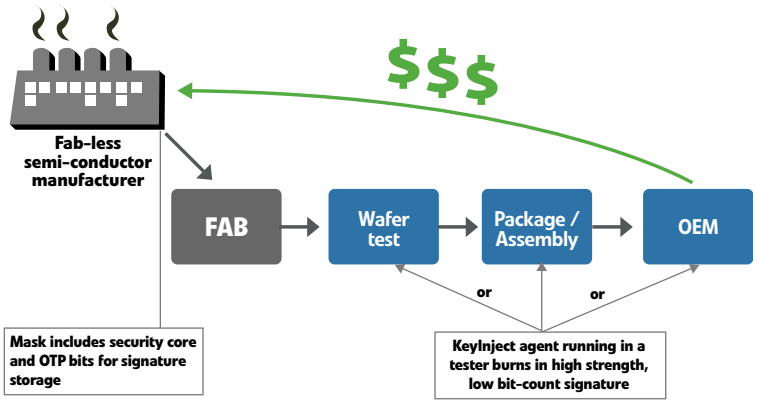

FIGURE 2. Certicom KeyInject secures the entire manufacturing process.

The key controller at head office periodically performs maintenance sessions that retrieve these logs, analyzes key usage and delivers new key batches. Alarms are triggered when manufacturing counts and key usage figures do not match, and emails to operations personnel are generated immediately.

Together, these secure logging functions allow vendors to track the distribution of keys, giving them greater control over —and insight into—the outsourced manufacturing process in addition to providing stronger security. It also integrates well into customer business models, as these various metrics can be used to determine royalty revenues.

The advantage of built-in security

With a unique, valid encryption key embedded in each chipset—and accounted for at every step of the way from point of issue to integration within the OEM satellite radio unit—the overall DRM or content-protection scheme is dependably secure. During the operation of the device itself (for example, at power-on reset), the chip's inbuilt security function verifies the key and decodes the data path that enables all other functions to operate.

Because the vendor can be certain as to whether a key is valid or not, a failure at the verification can prompt device shutdown or restrict it to baseline functions only. In other words, there is an opportunity to respond decisively and assuredly because there is no doubt or confusion about the chip's legitimacy.

THE OUTCOME

By employing Certicom KeyInject, vendors strengthen both the security of their devices and the security of the systems those devices are built to serve. Certicom's solution stops the leakage of wafers or parts into the grey market by eliminating the opportunities for it to occur—and at the same time ensures the vendor's ability to distinguish legitimate devices from illegitimate ones after they are taken up by users.

With enhancements to the security of the chip design itself, vendors are also protected against the threat of counterfeiting by means of reverse engineering. The challenges to would-be fraud perpetrators are so extreme that the cost of reverse engineering becomes prohibitive.

In the end, securing your outsourced manufacturing operations with Certicom KeyInject protects your two most precious assets: namely, your brand and your revenue.

about certicom

Certicom Corp. (TSX: CIC) is the authority for strong, efficient cryptography required by software vendors and device manufacturers to embed security in their products. Adopted by the US Government's National Security Agency (NSA), Certicom technologies for Elliptic Curve Cryptography (ECC) provide the most security per bit of any known public key scheme, making it ideal for constrained environments.

North America 1.800.561.6100
EMEA +44.20.7484.5025
International +1.905.507.4220
E-mail info@certicom.com
www.certicom.com

certicom™