Minimizing the Quality Risks of Outsourcing

PROTECTING YOUR BUSINESS AND YOUR BRAND

Studies in Self-Defense:
A Certicom Application Note Series

October 2008

THE CHALLENGE

The need for quality control in manufacturing is so well-established these days that it really goes without saying. The same is true of the relationship between quality and brand integrity: a company's reputation among consumers—and among its business partners—is every bit as valuable as its products or services. Yet with increasing dependence on outsourced (and often offshore) manufacturing, the challenge of maintaining quality control is intensifying.

This is doubly true when security enters into the mix. Manufacturers producing components or devices for use in security-sensitive market environments such as digital transmission content protection (DTCP) or high-bandwidth digital content protection (HDCP) schemes must ensure that their products never jeopardize the security of the overarching business structure. Beyond the ire of customers whose devices fail to access paid-for content—and beyond the wrath of business partners whose revenues are at risk—companies responsible for breached security also face the costly threat of legal liability from digital content- protection licensing authorities.

So where and how do quality-related security risks arise? The chief point of vulnerability is at the packaging and assembly stage of semiconductor manufacturing. Key-injection errors or duplications can cause 'collisions' between devices out in the marketplace, and can also expose products to counterfeiting and other so-called 'grey-market' risks.

As the following scenario reveals, Certicom KeyInject™ provides an elegant and streamlined solution that addresses these perils and restores quality control to the original device creator.

THE RISK SCENARIO

Imagine a consumer electronics company that manufactures high-definition PVRs (personal video recorders). This company has distribution arrangements with high-definition cable-television service providers throughout regional markets in North America. Through these exclusive arrangements, the company's PVR units are sold or leased to all HDTV customers in those markets. As a result, the devices must be able to enforce each service provider's content-access rules—ensuring that only legitimate users are able to view the HD content they purchase on a monthly basis.

The chipsets that provide the intelligence inside these units are produced by a third-party fabless semiconductor manufacturer. Contractually, the PVR manufacturer is responsible to its cable company partners for ensuring the quality and security of the manufacturing process.

Further complicating the process is the fact that the PVR maker is obligated (again, by virtue of its contracts with the HD service providers) to purchase batches of keys from a licensing agency; these keys must be transported and stored securely until they are injected into each individual device.
Obviously, there is considerable pressure on the PVR manufacturer to ensure that the key-injection process is error-free. As the recent KPMG white paper *Managing the Risks of Counterfeiting in the Information Technology* Industry explains:

> **… the issue is preventing key injection mistakes. For example, if the same key is inserted into more than one chip by mistake, when the OEM assembles the system and tries to bind the key to the device serial number, the manufacturing process gets interrupted when the same key appears more than once. This would result in a brand quality control hit…**

As mentioned previously, that quality control 'hit' manifests through collisions when two devices are detected to have the same keys. The question arises as to which is the 'legitimate' device—for there is always the chance that one may be a grey-market product. Whatever the circumstances, one or both devices must be retired and replaced—an expensive prospect if key-injection errors are widespread, and one that is accompanied by no small amount of customer-service intervention on the part of the HD service providers.

The following illustration shows where key-injection errors enter into the manufacturing stream.

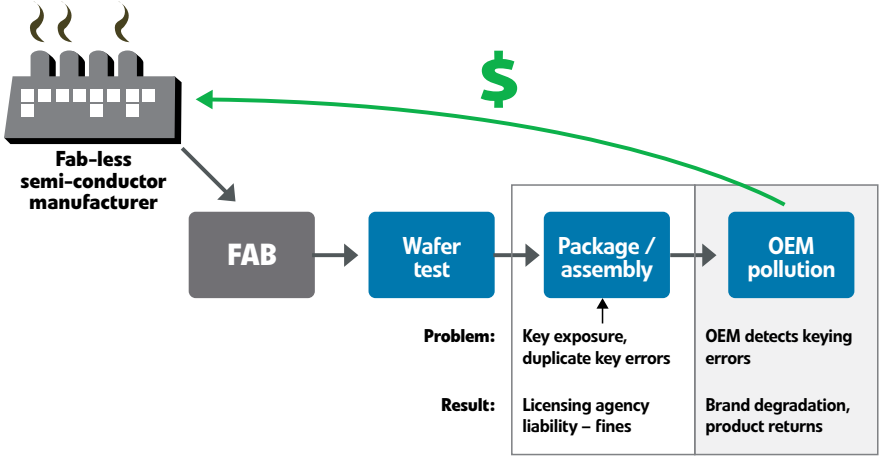

FIGURE 1. Keying errors and their consequnces.

THE SOLUTION

Incorporating a cryptographically wrapped key-injection system allows device vendors to retain control over keying material and detect key-injection errors, without impeding the necessary distribution of data throughout manufacturing. It is important to ensure that not only the keying material itself but also the channels for transporting and delivering the keying material are securely managed.

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 imported from a third-party source or 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 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, which are secured all the way back to head office and cannot be tampered with, are essential to preventing—and discovering—key injection errors or duplications.

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, the 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 automation of the system reduces operational and supervisory costs.

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 PVR 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 virtually eliminates keying errors—and any that do occur are caught before leaving the packaging house. At the same time, Certicom KeyInject prevents the leakage of wafers or parts into the grey market.

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. Certicom products and services are currently licensed to more than 300 customers including Motorola, Oracle, Research In Motion, Terayon, Texas Instruments and XM Radio. Founded in 1985, Certicom is headquartered in Mississauga, ON, Canada, with offices in Ottawa, ON; Reston, VA; San Mateo, CA; and London, England.