certicom™

a certicom application note

# Certicom Security for Fabless Semiconductor Design Companies

**control your outsourced manufacturing channel with a proven security solution that is based on government-approved technology**

Fabless semiconductor design companies can save millions of dollars per chip design by using low-cost foundries overseas. Unfortunately, concerns about exposure to fraud make it risky. With a new hardware-based solution built specifically for the industry, fabless design companies can make low-cost foundries as reliable as high-priced alternatives and defeat gray markets with embedded security.

## Introduction

Semiconductor companies increasingly outsource manufacturing in order to improve bottom line profitability and to remain focused on core competencies. For this reason, the fabless model has exceeded the growth of the overall semiconductor market. But this need to rely on contract manufacturers makes fabless design companies an attractive target for the growing gray market.

Since manufacturing costs make up of the largest part of chip production expenses, fabless design companies are eager to save millions of dollars per chip design by outsourcing manufacturing to low-cost providers overseas.

Unfortunately, the clearly defined cost savings is offset by the very real possibility that your IP will find its way to the gray market. The gray market costs fabless chip design companies millions of dollars in lost revenue – since a company ends up competing with low-cost versions of their own products.

According to a recent FSA poll, 84% of respondents from the fabless design industry are "very concerned" about IP protection when working with overseas foundries. It's easy to understand why. Industry research from KPMG and the Alliance for Gray Market and Counterfeit Abatement (AGMA) shows that gray market sales of IT products account for over $40 billion in revenue each year. This costs IT manufacturers up to $5 billion annually in lost profits [1] .

Gray marketing is the result of several potential areas of illegal activity. Among the most common is intentional overproduction. This is where the contract manufacturer has the opportunity to "overproduce," producing more chips than were contracted. They can then sell these chips on their own at the expense of the chip designer, creating a gray market that competes against legitimately produced silicon.

Moreover, a chip designer's intellectual property (IP) is typically exposed and vulnerable to counterfeiters because contract manufacturers, who hold the proprietary production plans from the legitimate order, can easily produce additional units on its own for gray marketers.

1 Alliance for Gray Market and Counterfeit Abatement (AGMA) http://www.agmaglobal.org/facts.html

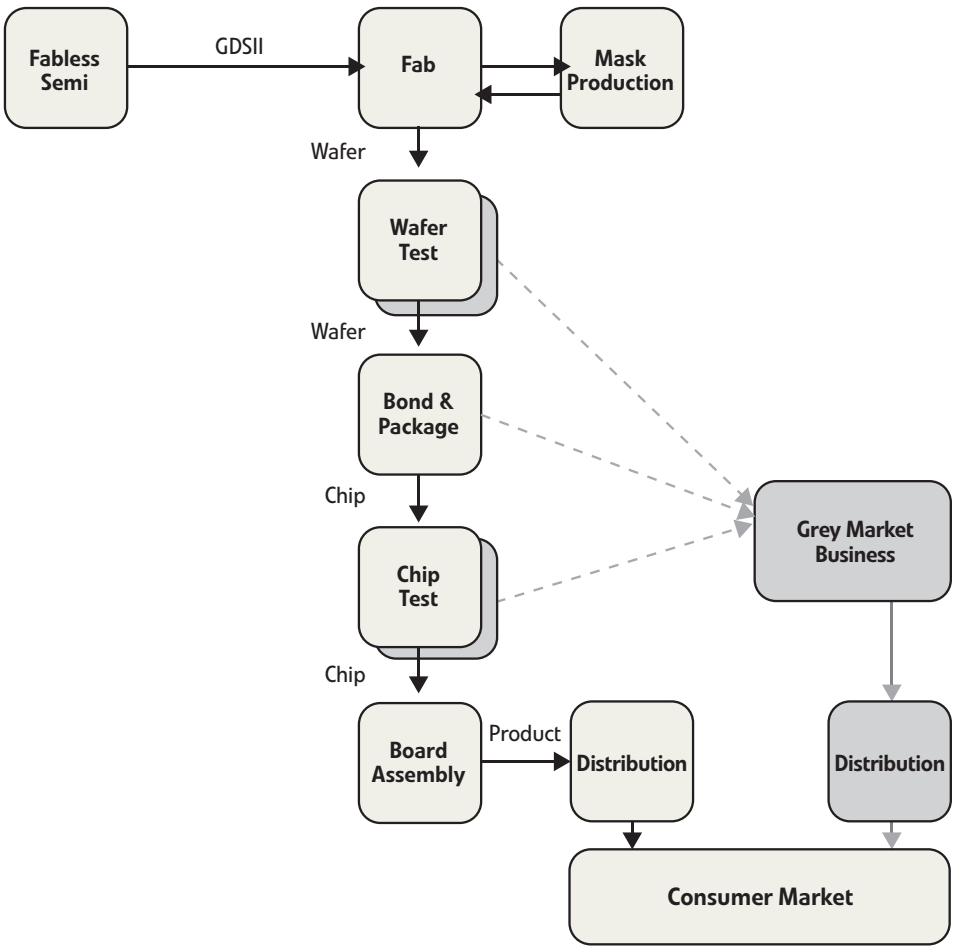


*Illustration 1: How contract manufacturers or their employees supply a gray market with working chips at the expense of the fabless design company.*

A separate problem, similar in scope and impact, is "yield misrepresentation." In this case, a contract manufacturer may operate in good faith, but its employees do not, resulting in a product being stolen right off the manufacturing line to supply a gray market.

Unfortunately gray marketing is a problem even when the contract manufacturer is operating in good faith. Individuals or groups of employees often act on their own, stealing finished product off the production line for sale to counterfeiters.

Today's typical production process makes it impractical for fabless chip design companies to monitor or manage third-party contract manufacturers without incurring costs that reduce the financial benefits that made outsourcing attractive to begin with.

## Defeat Gray Markets: Introduce Hardware-Based Security into Your Existing Process

These challenges can be addressed without having to change existing manufacturing processes. By introducing proven hardware-based security that relies on government-approved technology, fabless chip design companies become empowered to select less costly contract manufacturers who otherwise would not be considered as business partners due to the perceived exposure to fraud.

With Certicom Security for Silicon Design Protection, fabless design companies can protect their IP at every stage of the production process – GDS2, fab, mask production, wafer test, bond and package, chip test, board assembly, and distribution – by adding a manufacturing security system with sophisticated hardware blocks to a customer's chip design.

As a result, any chip produced using Certicom security will only function if it follows the authorized production process. Chips produced without your knowledge simply won't work. Chips taken off the line by unscrupulous individuals for re-sale on the gray market won't function. Fabless design companies can prevent their IP from reaching the gray market by eliminating the profit motive.

**Control your outsourced manufacturing channel with a proven security solution that is based on government-approved technology**

In order for a counterfeit product to be manufactured, collusion among multiple disreputable contractors is necessary. This makes a gray market business harder to establish because two or more businesses must agree to operate in bad faith against their customer. In addition, it makes these illicit businesses more risky and expensive to operate. This will lower the number of individuals willing to participate and it will also raise the cost of gray market products, which make them less competitive.

## The Certicom Solution

Certicom Security for Silicon Design Protection assures legitimate silicon chip production, while effectively ending silicon chip gray market and overproduction.

Combining the proven software-based Certicom KeyInject system with a new production control hardware core, this solution forces checks and balances throughout the silicon manufacturing process and curbs the proliferation of gray markets.

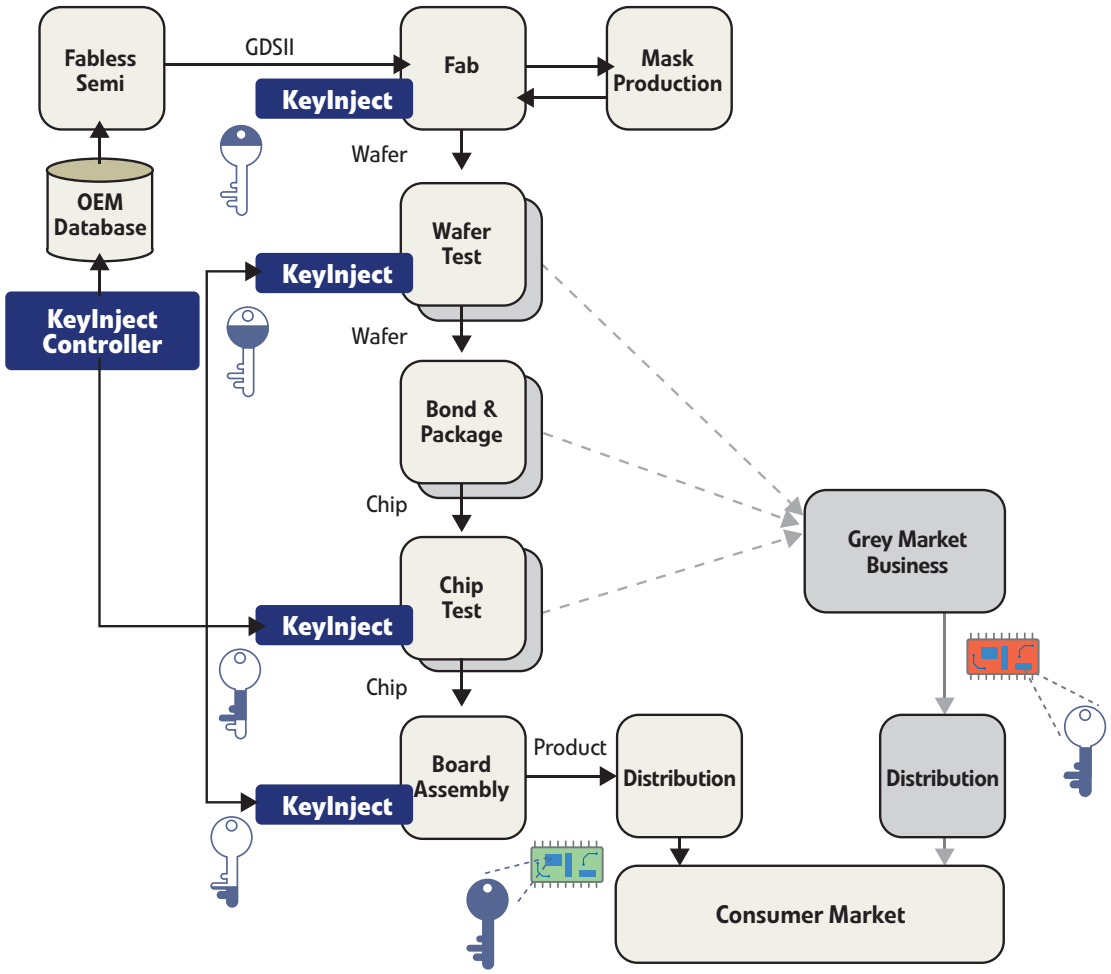


*Illustration 2: This description reflects the most secure version of KeyInject with IP Cores. You can choose which touch points are needed to secure the chip production process.*

Chips manufactured outside this secure process – as a result of overproduction or misrepresentation – are rendered unusable. As a result, companies can now lower their chip production costs by working with less expensive contract manufacturers because they will know that Certicom is protecting their products' market viability.

**Increase bottom-line profitability by securing your most cost-effective fabs without worrying about your IP reaching the gray market.**

The combination of Certicom KeyInject and production control cores ensures the injection of cryptographic keying material into One-Time-Programmable (OTP) memory at multiple stages in the manufacturing process and across multiple sub-contractors– from mask production and manufacturing of silicon wafer to testing and packaging.

The IP core, which is added to the ASIC design, verifies the keying material and at the end of the process derives a new hardware protected key to "unlock" the critical functionality in the ASIC. The KeyInject manufacturing infrastructure also enables fables design companies to control and track remote production by metering the required cryptographic keys and producing traceable audit trails from each sub-contractor.

Through this approach, chips produced following an established path through authorized manufacturing channels result in fully functioning chips. Partially completed chips that are stolen at some point during the manufacturing process that do not follow the defined path are left crippled and unusable.

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 silicon chip—the authenticated chip is dependably secure. During the operation of the device itself (for example, at power-on reset), the chip's inbuilt authentication 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.

And since Certicom uses government-rated, tamper-resistant Hardware Security Modules (HSMs) to protect key and logging data every step of the way, your designs are protected even in the most hostile environments. In fact, the core security routines actually run inside the HSM. This makes the Certicom KeyInject systems themselves safe from tampering when fielded. Any attempt to circumvent KeyInject system security – through operating system or physical attack – will result in a KeyInject server self-destruct. The equipment is not damaged, but the server will lose its identity and ability to activate chips on its intended manufacturing line. If this ever occurs, the manufacturing line can switch to a backup. And a forensic analysis of the KeyInject system can take place afterwards to enable a clear understanding of why a backup was required.

## The Outcome

Fabless chip design companies increase bottom-line profitability by using the least expensive manufacturers. Certicom enables you to protect the investment you've made in your IP, and gain control over your outsourced manufacturing channel while putting a stranglehold on gray market.

By combining the software-based KeyInject system with a hardware-based production control core, security is extended right into the silicon. As a result, fabless design companies no longer need to be concerned about design flaws or worry about keys being exposed during the manufacturing process.

Designed specifically to enable fabless semiconductor companies to choose the least expensive source of silicon, Certicom makes it virtually impossible for bad faith contractors to produce additional chips – based on your IP – without your knowledge. As a result, only authentic chips reach the market.

In addition, Certicom significantly reduces keying errors and catches irregularities before the chips leave the packaging house. And if a testing house reports a failure rate that is above expectations, you'll have an ability to track whether the issue lies with the foundry that produced the chips or the testing house itself because you will now essentially have a serial number for each chip. As a result, you'll be able to identify each faulty chip for auditing, trace which fab was responsible for the manufacturing, and generate reports that enable you to monitor yield.

By embedding Certicom security into your design, you will increase bottom-line profitability by using the least expensive contract manufacturers and you will potentially improve revenue by keeping your IP out of the gray markets.

## about certicom

**Certicom protects the value of content, software, and devices with open, standards-based security technology that has been adopted by the National Security Agency (NSA) for classified and sensitive government communications. With over 350 patents and patents pending worldwide covering key aspects of Elliptic Curve Cryptography (ECC), Certicom enables developers to quickly address the security requirements of government agencies, smart device manufacturers, service providers, and enterprise software while delivering the most security per bit of any known public-key scheme. Certicom security offerings are currently licensed by leading global companies – including General Dynamics, Motorola, Intel, Oracle, Unisys, nCipher, and Research in Motion. Founded in 1985, Certicom corporate offices are in Mississauga, Canada with worldwide Sales and Marketing headquarters in Reston, VA and other offices across the US, Canada and Europe.**

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™