Microsemi

Securing Your Supply Chain Life Cycle

Introduction Paper

Everyone wants his or her new embedded system design to be wildly successful. It is particularly disappointing when copying, counterfeiting, overbuilding, or outright theft derails a design from achieving market success. To protect a design from these threats it is critical to secure a design throughout the entire life cycle—from device fabrication, to system decommissioning. It is convenient to separate the component supply chain life cycle (the development, manufacture, and distribution of key components), from the embedded system life cycle (the development, manufacturing, deployment, and eventual decommissioning of the system). This article will cover the supply chain and a companion article"Securing Your Embedded System Life Cycle Paper and Video", will cover the embedded system, so that the complete secure life cycle of an embedded system can be described in sufficient detail.

Security Throughout the Component Life Cycle

Any component undergoes several stages in its life cycle. as illustrated in Figure 1 below. It starts with the design and fabrication by the original equipment manufacturer (OCM). Wafers are tested and working devices are passed to assembly. Devices are then tested against various speed and power criteria and 'binned' according to the grading requirements. Devices are marked and then passed to distribution for sale.

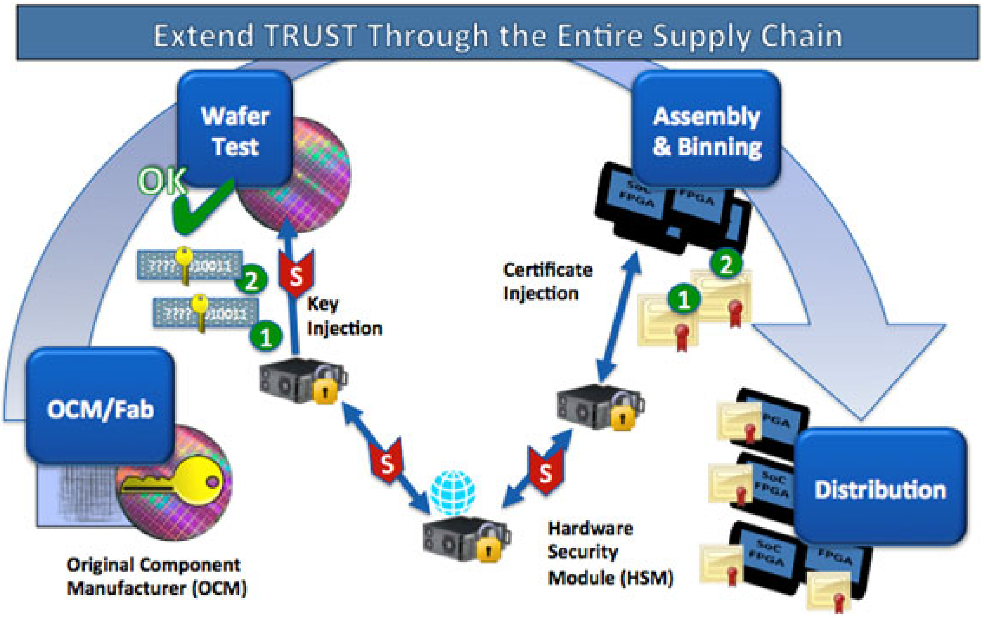
Extend TRUST Through the Entire Supply Chain
Wafer Test
OK
Key Injection
Assembly & Binning
SoC FPGA
FPGA
Certificate Injection
1
2
OCM/Fab
Original Component Manufacturer (OCM)
S
Hardware Security Module (HSM)
Distribution

Figure 1: **Implementing a Secure Supply Chain**

Requirements for Securing the Entire Device Supply Chain

The design and fabrication of the device is the most trusted part of the process. Wafer test, assembly and binning without strong anti-counterfeiting solutions are less so, and distribution channels, especially those not authorized, are fraught with risk. The aim is to build on the trust available in the earlier stages and extend the trust in these stages further and further down the chain so that ultimately counterfeit devices cannot be injected into the supply chain and end up in an electronic system. Using a secure Device Identification technique can be the starting point for trust in a secure process.

Device Identification

The critical elements of the identification technique used must be controlled, since if it becomes available to counterfeiters it could be defeated. An intelligent IC that has at least some of the following characteristics can apply the strongest known control techniques:

- Embedded nonvolatile memory
- Implement cryptographic algorithms in real-time
- Digital communication interfaces for data interchange
- Built-in hardware-level security

A device identification technology, whose security rests on cryptography and these well-proven controls, is very strong compared to any other process-based or technical identification technology. SmartFusion®2 SoC FPGAs and IGLOO®2 FPGAs from Microsemi can be used as the basis for creating a strong technical anti-counterfeit solution because they possess all of the above characteristics. They also have additional features that further enhance their overall security:

- Cryptographic device certificates that identify legitimate devices individually
- Extremely strong, tamper-resistant, and hard-to-spoof
- National Institute of Standards and Technology’s FIPS PUB 140-2 Level 3 cryptographic controls are installed in Microsemi facilities (a level appropriate to protect very high-value assets, up to and including state secrets)

Hardware Security Module

In addition to a secure identification capability for an intelligent IC, another key requirement of the protection process is the use of a hardware security module (HSM) during device manufacture. A HSM is a tamper resistant, tamper evident, security-hardened computer that is used to perform the wafer authentication, key injection, and certificate signing functions at a remote wafer test or assembly location.

Securing Wafer Test

Securing devices at the wafer test stage is the first step in creating a secure life cycle. By creating a unique device identification that is also secure, the rest of the security methodology can be built on this ‘secure foundation’. The use of the HSM is also critical at this stage so that additional identification information stored in the device is secure and complete.

The HSM initially verifies that the device and wafer being tested is the expected one using authentication features designed in at the lowest transistor and interconnect levels of the device, “baked” into the device. Then and only then does it generate a secret key that is injected into the device. This key is unique to an individual device and prevents upgrading of such components by authenticating only components with the exact parameters specified in the device certificate. All communication between the device and the HSM use standard public key cryptographic methods so the device can be validated and protected from unauthorized accesses.

Physically Unclonable Function

Creating a unique device identification that is secure requires it to be 'bound' directly to the individual device. To provide true device binding, an intrinsic physical property with a high degree of repeatability and individuality can be used. Such a behavior is known as a physically unclonable function (PUF). In an electronic circuit, any internal SRAM memories, when powered up but before being written to, will contain a random collection of 1s and 0s. This unique pattern of 1s and 0s will remain stable in each individual device and can therefore be used to identify that particular device, analogous to the way fingerprints can provide biometric identification of people. This function is illustrated in Figure 2 below, and shows the Quiddikey™ implementation used by Microsemi in select FPGA devices. This function provides one of the highest levels of security available and is a unique offering by Microsemi for FPGAs.

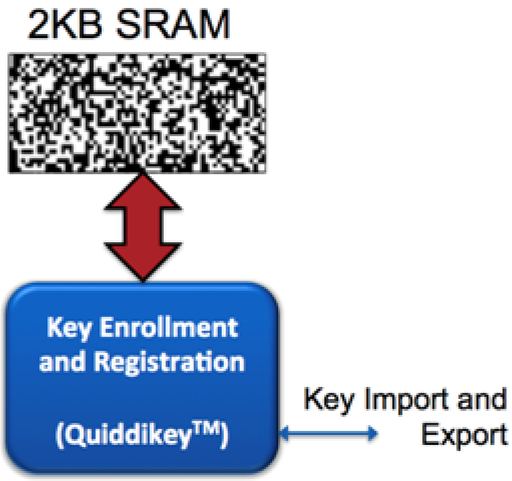

Figure 2: **Use of Quiddikey SRAM-PUF for Unique Device Identification**

Securing Assembly and Binning

Building on the secret key injected at the wafer test stage, a digital certificate is injected into the device at the assembly and binning stage. This certificate contains data fields that define key device characteristics used to distinguish the device and its operational parameters, including:

- Original Component Manufacturer (OCM) identifier—in this case, Microsemi
- Device serial number
- Model number with grading information
- Assembly date code
- Data binding the certificate with the secret key previously injected

The HSM ensures only good devices receive a certificate, which prevents the representation of failed components as good ones. The HSM securely logs each certificate so the OCM knows exactly how many have been issued. The certificate is injected after test and binning so it contains authenticated device grading information. This facilitates user detection of devices tested to a lower speed or temperature grade than indicated by package-top markings, which could potentially be fraudulent (modified by a counterfeiter).

Certificate Revocation List

As a further element of supply chain security any certificate can be invalidated by Microsemi by adding it to the appropriate certificate revocation list (CRL). The CRL describes certificates that should not be trusted any longer.

Some examples of CRL updates include:

- Inventory retest failure
- Production failure
- Field application obsolescence
- Theft of components
- Detection that a device has been tampered with

Securing the Distribution Channel

The device now contains very detailed and secure information, some of which can be securely verified at any point in the distribution channel, using the OCM’s public key to read and verify the device certificate. For example, during incoming inspection devices can be authenticated against the following:

- The certificate’s integrity and signature, using the OCMs public key
- Verifying the device knows the unique secret key stored in the device and bound to the certificate, proving the certificate is not just a copy from another device
- The certificate can be checked for listing on a certificate revocation list

Conclusion

When secure and unique device identification is used in conjunction with a hardware security module the backbone of a secure supply chain can be established. Devices with strong cryptographic and anti-tamper capabilities (like Microsemi IGLOO2 and SmartFusion2 devices) can build on the secure backbone to create additional levels of security, using digitally signed certificates and certificate revocation lists to extend trust through the entire supply chain life cycle.

Microsemi has a wide variety of security related material available on its Security website. We invite you to visit the site and in particular explore the material listed in the "To Learn More" section below to expand your knowledge of the fast growing and ever evolving security field.

To Learn More

1. Securing Your Embedded System Life Cycle Paper and Video
2. SmartFusion2 and IGLOO2 Cryptography Services
3. How Easy is it to Secure Your Designs?
4. What is Design Security in a Mainstream SoC Chalk Talk

Secure Boot

1. Overview of Secure Boot with Microsemi SmartFusion2 SoC FPGAs
2. Overview of Data Security Using Microsemi FPGAs and SoC FPGAs

Microsemi Corporate Headquarters
One Enterprise, Aliso Viejo CA 92656 USA
Within the USA: +1 (949) 380-6100
Sales: +1 (949) 380-6136
Fax: +1 (949) 215-4996

Microsemi Corporation (NASDAQ: MSCC) offers a comprehensive portfolio of semiconductor solutions for: aerospace, defense and security; enterprise and communications; and industrial and alternative energy markets. Products include high-performance, high-reliability analog and RF devices, mixed signal and RF integrated circuits, customizable SoCs, FPGAs, and complete subsystems. Microsemi is headquartered in Aliso Viejo, Calif. Learn more at **www.microsemi.com**.