Secure SoC Manufacturing: Foundation for a Connected World

As mobile usage continues to permeate daily lives with increasingly sensitive data and high-value transactions, the importance of device security has become even more important. Information security begins at the point when Internet-connected devices are designed and manufactured. But today's complex global supply chains are fraught with numerous challenges that can result in both security breaches and operational inefficiency, which have a downstream impact on device security and functionality.

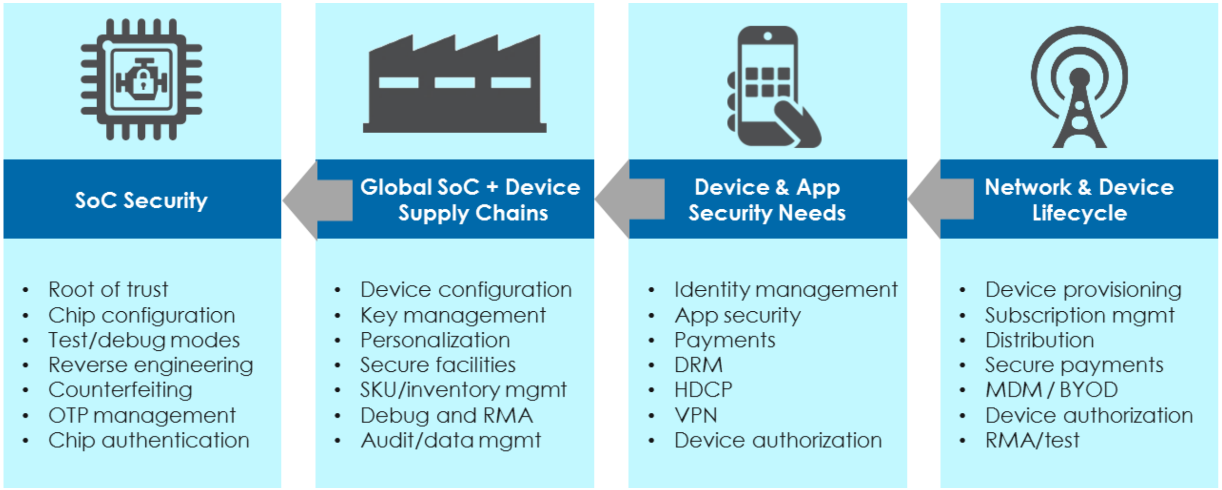
This paper will begin by examining the current state of manufacturing and the need to build security functionality into the DNA of each connected device during the first stages of design and manufacturing. The focus will then shift to the essential requirements needed to create robust endpoint security and infrastructure that enables device services for secure remote management of silicon features, cryptographic keys and delegation rights throughout a device's lifecycle.

Security Imperative for the Mobile Industry

According to a recent Gartner report, mobile phones are expected to dominate overall device shipments with 1.9 billion mobile phones projected to ship in 2014. As well, ultramobiles, which include tablets, hybrids and clamshells, are poised to take over as the main growth driver in the devices market, with an expected growth rate of 54 percent. Meanwhile the GSMA[1] estimates there will be a total of 24 billion connected devices by 2020 and that new efficiencies and services that are opening up within this global market are estimated to deliver as much as $4.5 trillion in revenue.

With the growth and functionality of mobile devices, there are increasing security concerns across the entire mobile value chain due to the diversity of new applications and ways in which mobile devices are being used (see Figure 1). As an example, new mobile devices are coming equipped with HDMI (High Definition Media Interface) along with the requirement for keys to be provisioned to the mobile device during manufacturing. The liability of leaking such keys during this process can cost millions of dollars per instance. Along these lines, the potential cost caused by a data breach is significant with one particular company estimating it lost more than $400 million in the first year after the breach. At the same time, according to information and analytics provider IHS[2], the five most prevalent types of semiconductors reported as counterfeits that have widespread commercial and military use represent $169 billion in potential annual risk for the global electronics supply chain. These combined trends drive the need for robust security which, in turn, requires that device security begins with the SoC design and subsequent manufacturing process.

[1] GSMA and Machina Research, *Connected Life in 2020*, Mobile World Congress, Barcelona, Spain, February 27, 2012.
[2] IHS iSuppli, April 4, 2012



SoC Security

- Root of trust
- Chip configuration
- Test/debug modes
- Reverse engineering
- Counterfeiting
- OTP management
- Chip authentication

Global SoC + Device Supply Chains

- Device configuration
- Key management
- Personalization
- Secure facilities
- SKU/inventory mgmt
- Debug and RMA
- Audit/data mgmt

Device & App Security Needs

- Identity management
- App security
- Payments
- DRM
- HDCP
- VPN
- Device authorization

Network & Device Lifecycle

- Device provisioning
- Subscription mgmt
- Distribution
- Secure payments
- MDM / BYOD
- Device authorization
- RMA/test

Figure 1. Mobile Value Chain Security

Mobile Chip Manufacturing Challenges

Today most chip manufacturers reduce manufacturing complexity and business risk by purchasing wafers through a contract wafer foundry. These fabless semiconductor companies typically have multiple suppliers around the world that manufacture chips remotely.

Some of the challenges that fabless semiconductor companies encounter span across several stakeholders:

Chief Information Officers (CIO) face growing pressures to ensure the security and integrity of sensitive information, secret keys, and technology IP across a globally distributed manufacturing supply chain. This is primarily due to offshore manufacturing sites introducing security risks commonly associated with counterfeiting, over-production, data security breaches, technology transfer, IP theft, and other forms of grey market activities. In addition, these remote factories are typically not staffed with key management or security experts, further compounding the challenge of securing the supply chain.

Operations Executives have distribution, continuous availability, monitoring, and tracking challenges related to the production of digital assets in the supply chain. These challenges worsen with multiple manufacturing touch points in disparate locations as well as the use of multiple vendors for each step, and the distribution of chips to multiple OEM customers.

Product Portfolio Managers are under pressure to offer differentiated product services, including the ability to personalize chips while also improving time-to-market. Increasingly, product portfolio managers must respond to changing market conditions without creating additional inventory management overhead.

Chief Financial Officers (CFO) and General Counsel (GC) have the problem of mitigating the risks associated with liabilities for a variety of situations, including leaked keys from third-party licensors, stolen identification credentials, unauthorized use of third-party IP, and other sensitive digital assets.

With mobile devices housing more and more sensitive data that is utilized in a wide variety of applications, chip suppliers must meet the complex security requirements for each potential use case or capability. Most security measures require the injection of secret identity data and cryptographic keys. These digital assets must be protected throughout the manufacturing process, including those functions that are outsourced in other parts of the world.

While highly-sophisticated technologies are often employed to secure information inside a device, the process of key injection during fabrication and test operations may expose valuable key data. Similarly, test/debug capabilities are often fully enabled on un-programmed chips (i.e. enabled by default), creating additional security challenges. To prevent theft of sensitive data or theft of IP, physical security measures such as barbed wire fences and armed guards may be employed but do not protect against attacks triggered within the manufacturing process. Ignoring security issues can lead to millions of dollars in liability costs for stolen keys as well as substantial risks to revenue, market share and brand loyalty.

Securing the Global Manufacturing Supply Chain

The semiconductor manufacturing supply chain involves a complex structure of contract manufactures with sites in disparate geographies. For low-cost manufacturing, any solution used to securely provision sensitive data elements during manufacturing must also be cost effective. A distributed global supply chain presents a variety of practical problems for product line and operations managers to navigate. The security solution must also be flexible enough to adapt to changing production demands across a dynamically changing manufacturing environment. Additionally, such a security solution must be continuously available without creating brownouts, downtime, or bottlenecks that would be disruptive and costly to the overall manufacturing process. Since multiple products, each with different requirements will be manufactured within a supply chain, it is important to manage the distribution of digital assets, such as pre-computed cryptographic keys, without confusion, loss or duplication of unique keys.

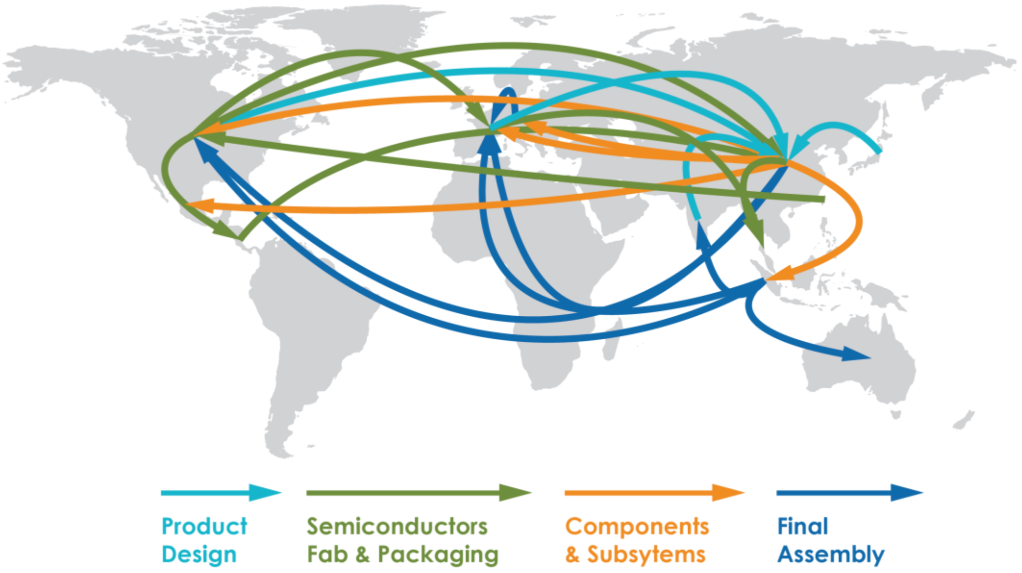


Figure 2. Distributed Manufacturing Flow

As illustrated in Figure 2, a security solution must be able to provision sensitive materials at different stages of the manufacturing process. For example, a chip may be serialized and identity information may need to be provisioned at wafer test as part of the fabrication of the chip in the first stages of production. Keys, chip-level modes, and features may then be provisioned at final test after the chip has been assembled and packaged.

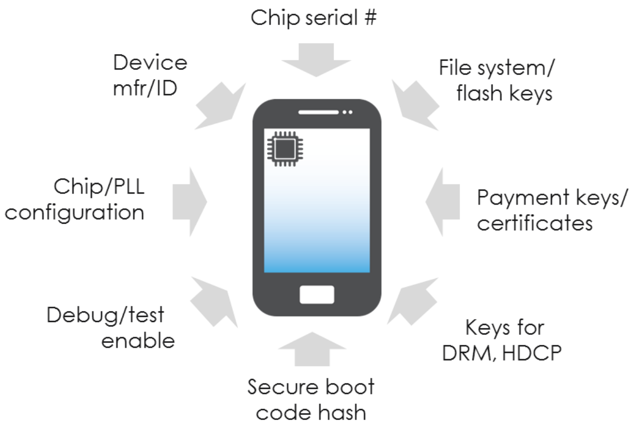


Figure 3. New Capabilities Bring New Security Requirements

Currently, sensitive SoC configuration information such as cryptographic keys is provisioned in the open without encryption on test equipment which is operated by third party contract manufacturers. These current provisioning methods expose chip manufacturers to liability and risks for any security breach that occurs within their supply chain. Additionally, this exposure opens up vulnerabilities in the supply chain and the ability to transfer technology and engage in grey market activity. Specifically, the vulnerability for cryptographic keys to be leaked and used improperly presents a serious problem given the expanded role of keys in the lifecycle of contemporary mobile devices. In today's smart mobile devices, an ever-increasing proportion of the features are Internet-related services that must be personalized and managed securely. As shown in Figure 3, these

SoCs are required to protect and manage vital data, including identification credentials, serial numbers, boot codes, device/feature configuration, and cryptographic keys. These keys are used for secure mobile applications and services such as mobile payments, digital rights management, and identity services, to name a few.

The leaking of cryptographic keys can expose all of these applications and lead to piracy of the valuable content and services. Conversely, the ability to securely personalize and provision mobile application services and content presents an enormous opportunity for adding value within the global supply chain.

Mitigating System Security Risks

This next section examines the requirements and elements needed to mitigate system security risks from cryptographic key injection throughout the fabrication, assembly and test/debug operations within the global manufacturing supply chain.

The CryptoManager™ Platform is a secure key and feature management platform for SoC manufacturers and smart mobile device manufacturers (see Figure 4 below). Leveraging a hardware root-of-trust, configuration of the device may be provisioned securely over the Internet via operations called device services; this includes details such as the features and sensitive security information, i.e. the digital security assets. Digital security assets may be defined as pre-computed digital data elements such as identity credentials, cryptographic keys, tokens, codes, hashes, and, in general, any other information used to assure integrity and protect sensitive information. In support of a global supply chain that encompasses both the SoC manufacturer and its OEM device customers, the CryptoManager solution provides the capability for downstream OEM device customers to securely provision SoC devices used in their products. The CryptoManager platform is comprised of two primary aspects: 1) the Security Engine, a soft silicon IP core embedded in the SoC design; and 2) the Infrastructure, an information technology framework consisting of specialized server hardware, security hardware, embedded firmware, and software. Infrastructure components include the **Service** (head-end master control center located in customer's datacenter), the **Appliance** (remote security appliance located in the offshore manufacturing location), and the **Client Library** (specialized software that runs on manufacturing test equipment in the remote manufacturing location).

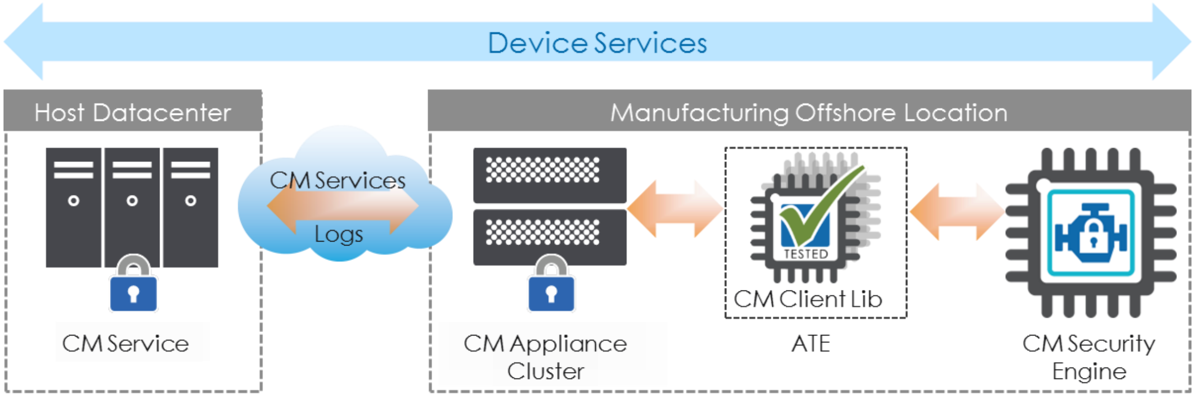


Figure 4. CryptoManager Platform

The **CryptoManager Security Engine** is a silicon core integrated into a SoC, providing a hardware root-of-trust for on-chip processes. The Security Engine provides a secure "nervous system" for the SoC to address fundamental security tasks during chip and device manufacturing. For example, the Security Engine performs secure operations inside the SoC such as cryptographic key and secure boot provisioning as well as configuration of debug modes and debug/test access ports.

Within the **CryptoManager Infrastructure**, the Service acts as a central operations control center that manages the overall Infrastructure configuration, digital security assets, and all authorized device services. The Service also includes monitors and alerts to assure prompt notification for any irregularities in the operations of the Infrastructure. The Service includes a Management Console that provides a common user interface for system administrators and operators. The Appliance is configured in clusters for redundancy and performance scalability and located in the datacenter of remote contract manufacturing sites. Appliances are needed to establish a secure communication channel between the Service and the Security Engine in the target SoC device to enable end-to-end protection of digital security assets and feature controls during the manufacturing process. This is achieved via the Client Lib running on the test equipment. Appliances are also needed to store digital security assets locally for performance reasons. The provisioning of sensitive data such as keys must be performed rapidly to ensure no unnecessary bottlenecks are introduced into the production line.

The Infrastructure automates the provisioning of device services across the supply chain, reducing operating costs and accelerating time-to-market. The Infrastructure has been designed to be easily integrated into any manufacturing facility without disruption to existing operations. Additionally, for ease of maintenance and management, the Appliances can be securely and remotely managed from within the enterprise datacenter.

Use Case Example: Device Personalization

The CryptoManager solution leverages a secure root-of-trust designed into the SoC as part of a framework for securely delivering SoC personalization services from a hosted Service in the cloud. These device services specific to select customers can be provisioned at any stage of manufacturing within the global supply chain. As outlined in this paper, the term "device service" describes a type of operation that may be performed on the device to affect the operation of its features, trust levels, protections, and the provisioning of IDs or keys. Specifically, the CryptoManager platform enables specific functions such as chip personalization services to be provisioned to a standard product for high-volume customers without adding Stock-Keeping Units (SKU) that would increase inventory overhead and waste. This capability brings both differentiation and cost savings to the semiconductor manufacturer supply chain while also substantially speeding time-to-market for both the semiconductor manufacturer and its customers.

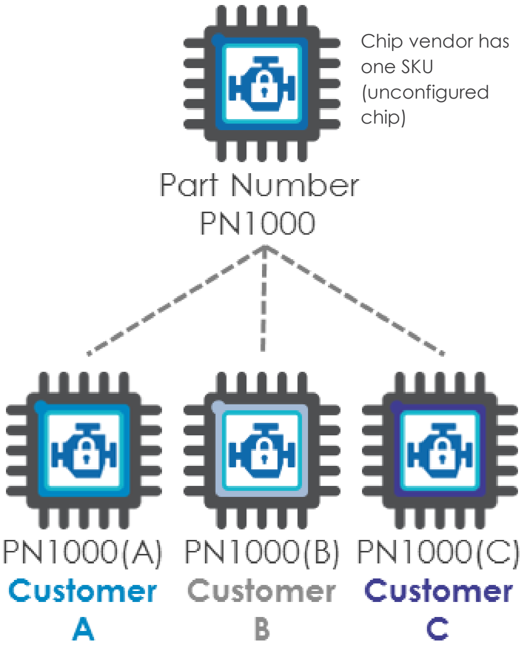


Figure 5. Device Personalization Use Case

Related to the inherent complexities and costs associated with building a brand new chip, fabless chip manufacturers are under constant pressure to improve operating efficiencies while, at the same time, satisfying OEM customer requirements (see Figure 5). As such, large OEM customers requesting personalization, customer-specific data preparation and feature customization of standard parts challenge the chip-makers ability to minimize inventory overhead and improve operating efficiencies. For example, if three OEM customers of a SoC manufacturer each request different feature configurations and/or data preparations for a standard SoC product, the SoC manufacture needs to figure out how to support three customer-specific part types without creating three different SKUs. In this case, pushing the personalization processing step to the last step in the manufacturing flow just prior to or, in some cases after delivery to the customer, mitigates the impact on inventory and operations.

By enabling chip and device makers to securely provision features and keys into their SoCs at the beginning and throughout the device lifecycle, customer-specific requirements may be satisfied while, at the same time, having the ability to streamline the manufacturing process for standard products. Additionally, these customer-specific personalization services may be accomplished with a high degree of visibility and audit tracking controls that are secured by the CryptoManager solution for each step in the manufacturing supply chain. The complexities are both automated and managed by the CryptoManager solution to minimize any incremental overhead or human error that results from supporting these value-added services.

Summary

Effective device security is intrinsic to the design and manufacturing process and rests within the DNA of the SoC; essentially, a secure, tamper-resistant hardware endpoint that forms a secure foundation for all device services. A secure hosted service that connects to security appliances in remote manufacturing locations acts in concert with this silicon root-of-trust to secure the global supply chain of the mobile ecosystem. This is accomplished by establishing a robust end-to-end communications channel from the CryptoManager Service managed by the chip manufacturer, device maker, and any additional trusted third parties with pre-authorized permissions to the root-of-trust in the SoC. Fundamentally, the CryptoManager platform provides a secure device services framework, mitigating the risks and hidden costs of insecure provisioning solutions that are not designed for mission-critical applications such as manufacturing.

For more information on the CryptoManager Key and Feature Security Platform, please visit rambus.com/cryptomanager.