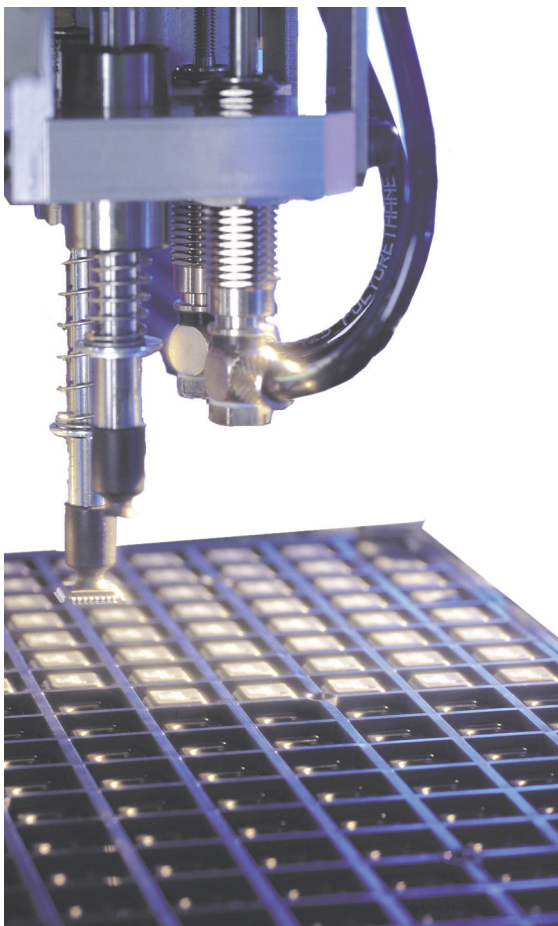


Micronas Secures Production with Certicom KeyInject®



Micronas needed a secure system for transporting and embedding keys into silicon chips for use in consumer electronics. Certicom deployed AMS KeyInject, a fully integrated secure platform, which successfully met Micronas' needs and helped secure their production.

Controlling keys during the manufacturing process is a challenge faced by many manufacturers. Certicom has produced AMS KeyInject – a product that enables you to easily manage keys and report on their usage, thus increasing the security of your operations.

KeyInject is a key component of Certicom's Asset Management System (AMS). KeyInject makes it possible to track the production of devices by contract manufacturers by controlling access to keying information, which is done using industry-standard protocols and techniques based on Elliptic Curve Cryptography (ECC) and Advanced Encryption Standard (AES). KeyInject allows your organization to monitor the use of HDCP (High-bandwidth Digital Content Protection) and other emerging standards through automated metering, with results reported back to authorized overseers.

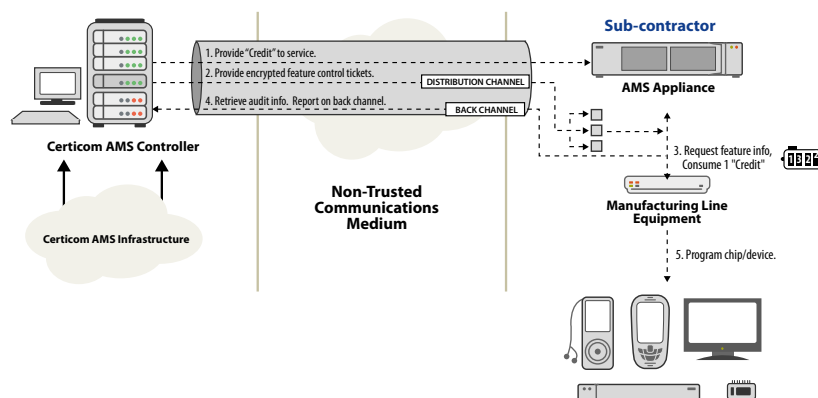
THE MICRONAS BUSINESS CHALLENGE

A semiconductor designer and manufacturer with worldwide operations, Micronas is a leading supplier of cutting-edge IC and sensor system solutions for consumer and automotive electronics. Micronas was seeking a secure and automated solution that protected its licensed keys during the manufacturing process, including situations where those keys are outsourced to global manufacturing sites. Micronas fabricated and packaged HDCP silicon in several plants and was facing two dilemmas: keys must never be used twice and they must be kept secure, even when the keys reside at 3rd party sites.

Certicom KeyInject was introduced to provide a key management solution. Micronas chose KeyInject to manage and secure their highly valuable HDCP keys during the chip manufacturing process, and to ensure that key inventories are always available to their contract manufacturing plants, to avoid manufacturing interruptions.

“Certicom’s solution is not only ideal as an automated process, but also as a trusted and proven source of dependable security and key management operations.”

– Stefan Rössel, Director IT at Micronas



Micronas Secures Production with Certicom KeyInject®

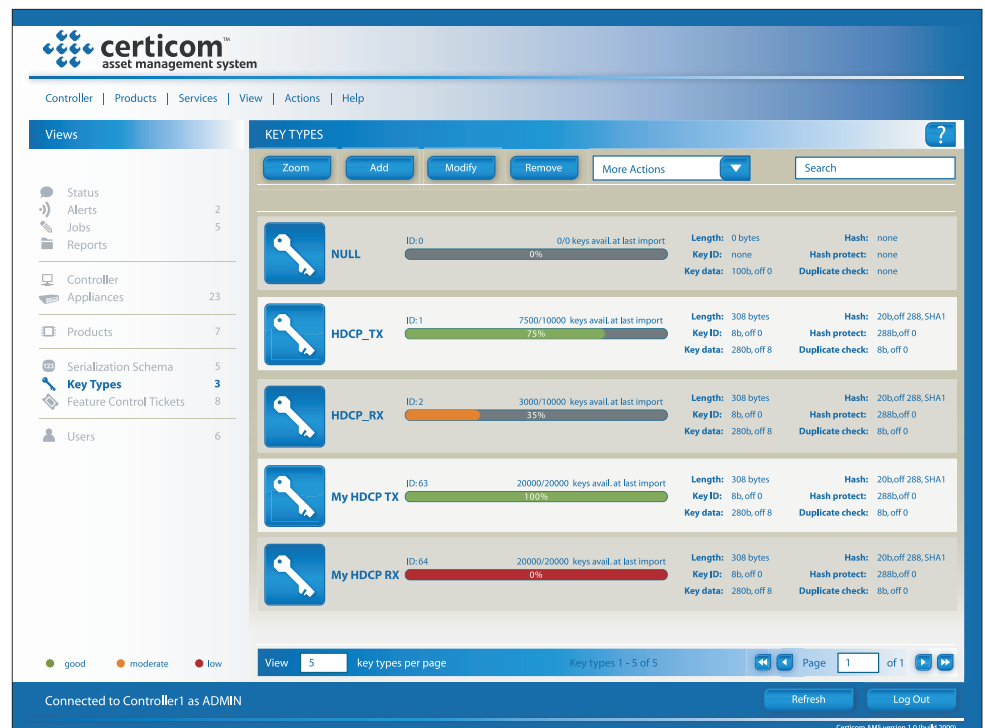


SOLUTION

Certicom security consultants were tasked with designing and building a customized KeyInject solution to mitigate the principle security threats of device cloning and managing key inventories at a Micronas production site in Germany and at a contract manufacturing site located in Singapore. The key deliverables of the solution included:

- AMS KeyInject Controller, which is a trusted key management and reporting system. This was delivered to Micronas in Germany.
- Four Certicom AMS KeyInject Appliances, which were delivered to Micronas and the vendor in Asia. The appliances are key injection and metering systems running on CentOS, installed with OS hardening tools to further enhance the overall security of the systems and decrease their susceptibility to compromise.
- The KeyAgent API interface, which acts as facilitator between KeyInject appliances and manufacturing-line equipment to request keys and push key logs. Certicom provided Micronas a toolkit that is integrated into the tester or programming environment. The toolkit enables applications to perform security and reporting tasks while abstracting the details.
- Hardware Security Modules (HSMs) that reside in the KeyInject Controller and KeyInject Appliances. The KeyInject firmware runs on an HSM, which is a piece of tamper-protected PCI hardware that has FIPS 140-2 Level 3 validated. The HSM provides high performance secure cryptographic processing in server systems and supports applications that require high-performance symmetric and asymmetric cryptographic operations. The HSM residing in the KeyInject Controller is used to protect decryption keys and force usage reports, since it the controller has been programmed to implement a metering sub-system. The metering system provides usage reports to Micronas from their manufacturers, in exchange for "credit" to continue device production.

Certicom configured a key distribution dashboard tailored to the needs of Micronas (similar to the GUI interface below). The GUI provided Micronas with a dynamic overview of all their fabrication/test locations, allowing its staff to adjust the key-credits of each Appliance, monitor key consumption, and dynamically configure (and even disable) Appliances.



Micronas Secures Production with Certicom KeyInject®



The AMS KeyInject controller resides at Micronas, and is the main repository for the keys. On the factory floors there are two sets of redundant servers (KeyInject Appliances), which communicate with many instances of the tester agents. These agents program the keys into the chips. All communication between the Controller, Appliances and tester agents is encrypted, and is also logged to allow tracing of each key to each chip.

DEPLOYMENT & IMPLEMENTATION

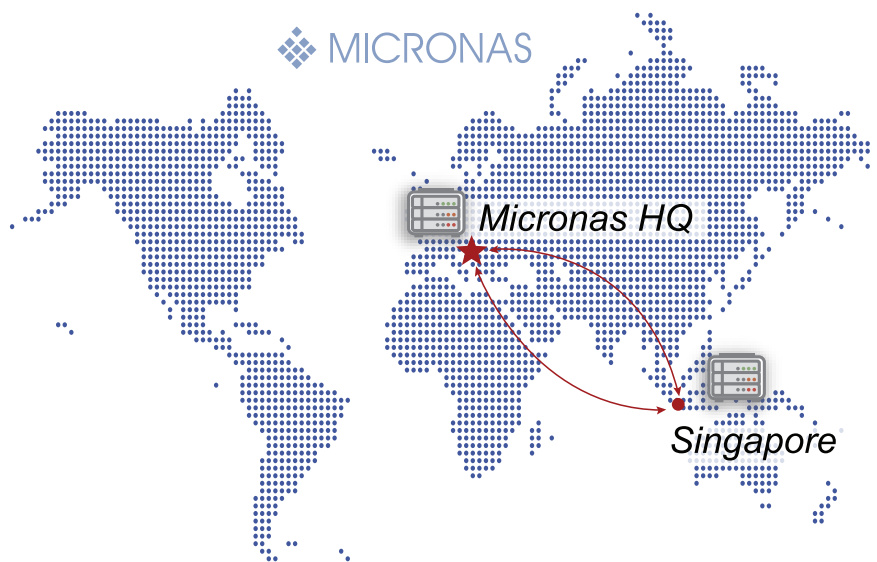
Certicom security consultants assembled and deployed the AMS KeyInject Controller and two AMS KeyInject Appliances at the Micronas production facility in Germany. Given the high level of security in the solution, key exchange and provisioning requests/responses between the AMS KeyInject Appliances and the Controller were initiated to setup communication between them.

Certicom consultants trained Micronas staff on using the KeyInject system as part of the deployment. This included instructions on defining key types, loading keys, requesting key usage logs and configuring KeyInject appliances to communicate with specific tester machines using the KeyAgent API that was integrated into the tester agent environment. Several simulated trial runs were performed to demonstrate how the AMS KeyInject Controller contacts AMS KeyInject Appliances to request key logs or to send more keys if required.

The deployment at a vendor based in Asia was similar to that done in Germany, except that the AMS KeyInject Appliances in Germany reside in a secure room on the production floor. At the vendor, the AMS KeyInject appliances communicate with the AMS KeyInject Controller over an encrypted VPN channel between the two sites. The installation of two AMS KeyInject Appliances in Singapore means that manufacturing throughput won't be affected if the active AMS KeyInject Appliance fails, as the redundant Appliance can assume the duties of the failed Appliance.

Micronas bulk encrypts device keys for transmission to the Asian vendor, where the encrypted data is stored on-site and decrypted in an automated fashion during the manufacturing process. Therefore, the device keys are protected while still under control of the AMS KeyInject system. AMS KeyInject guarantees that keys are never exposed until they are burned into the chip or device.

Toward the end of the AMS KeyInject deployment, Certicom security consultants conducted a security audit of the Singapore manufacturing plant which included a tour of facilities and interviews with upper level management, after which a security risk assessment report was generated. The security assessment report provided Micronas with a general understanding of potential physical security risks and recommendations for addressing those risks.



“Using our KeyInject system, Micronas is able to deliver their chip solutions for consumer electronics like high-definition TVs to market much faster.”

Brian Neill,
Certicom Product Manager

Micronas Secures Production with Certicom KeyInject®

CERTICOM AMS KEYINJECT FEATURES

A semiconductor designer and manufacturer with worldwide operations, Micronas is a leading supplier of cutting-edge IC and sensor system solutions for consumer and automotive electronics. Micronas was seeking a secure and automated solution that protected its licensed keys during the manufacturing process, including situations where those keys are outsourced to global manufacturing sites. Micronas fabricated and packaged HDCP silicon in several plants and was facing two dilemmas: keys must never be used twice and they must be kept secure, even when the keys reside at 3rd party sites.

Operations Support Options

24x7x365 Support Plans provide manufacturing operations teams with critical time sensitive operations support.

Support for key types other than HDCP

KeyInject natively supports most other CA and DRM keys, as well as custom key type support for proprietary keys using XML definitions. The KeyInject solution also enables you to specify which key types can be sent to specific remote factories.

Multiple Product SKU Features

Keyinject can package both HDCPTX and HDCP RX keys for the same chip. It can track multiple HDCP keys associated with the same SKU. Custom metadata can be transmitted in-band with key data to protect proprietary and secret chip configuration data.

Optional Advanced Security

KeyInject encrypts HDCP keys directly to silicon, using Certicom's Asset Control Core, part of the AMS solution family. KeyInject also supports multi-point injection – inject half of a key at wafer test and the other half at post package test. (Requires Certicom Asset Control Core).

Security Features

All keys, configuration information and logs are protected by FIPS-140 rated hardware security, implemented with government approved cryptography using ECC, AES-128 and SHA-256 based Suite-B cipher suites.

SUMMARY

Certicom's solution combined key management and security system management technologies to equip Micronas with state-of-the-art systems that control and report on the volume of keyed devices at time of manufacture, significantly reducing the risk of lost revenues due to device cloning or theft, which enabled Micronas to deliver value to market much faster than without Certicom AMS KeyInject.

About Micronas

A market leader in innovative global TV system solutions, Micronas leverages its expertise into new markets emerging through the digitization of audio and video content. Micronas also offers a variety of microcontrollers and Hall-sensors for automotive and industrial applications, such as car dashboard, body control, as well as motor management and comfort functions.

About Certicom

Certicom manages and protects the value of your content, applications and devices with security offerings based on Elliptic Curve Cryptography (ECC). Some of world's leading chip manufacturers rely on Certicom Asset Management System to reduce costs, deliver strong brand protection and provide new revenue enhancement capabilities

North America
1.800.561.6100

EMEA
+44.20.7484.5025

International
+1.905.507.4220

E-mail
info@certicom.com

www.certicom.com

