certicom | BlackBerry Subsidiary

SECURE CRYPTOGRAPHIC ASSET MANAGEMENT SYSTEM: AMS

MAKE YOUR SUPPLY CHAIN NOT JUST SECURE, BUT BLACKBERRY SECURE

Securely manage and distribute security assets to fight cloning, counterfeiting, and waste.

Certicom, a subsidiary of BlackBerry, is a recognized leader in public key infrastructure (PKI) security design, innovation, and delivery. Certicom offers government validated crypto libraries, PKI certificate solutions, and cryptographic asset management systems to make products, ecosystems, and manufacturing chains not just secure, but BlackBerry Secure.

With today's globalized supply chain, manufacturers have become reliant on a decentralized ecosystem of factories and testing facilities to bring their products to market. The problem is that every step represents an opportunity for cloning, counterfeiting, and waste. Certicom's solutions, such as the Asset Management System (AMS), leverage world class security methodologies to protect manufacturing supply chains to enhance revenue and profit, and protect brand equity.

Asset Management System

A major key to security is ensuring that secret keys stay secret in the manufacturing chain. That is what the AMS system is designed to do.

SECURITY AT EVERY STEP.

The modern supply chain is filled with points of attack where cloning and counterfeiting can happen.

Only an end to end secure manufacturing system using the most robust cryptographic methodologies can protect a company's brand image, revenue stream, and product safety.

IT'S PERSONAL

Security assets such as crypto keys inject personalities into products.

Certicom's Asset Management System (AMS) installs cryptographic keys and other cryptographic assets into devices such as processors, memory, and key storage ICs, among others, to ensure they are secure from tampering, counterfeiting, cloning, and other bad things that can happen. Without AMS there are multiple attack points allowing grey marketers access to valuable IP and products, particularly at the various subcontractor sites such as wafer test, bonding and packaging, and chip test.

AMS is based on a process known in the industry as "personalization" in which each device receives a unique identity by means of an inserted cryptographic key, making it possible to track and authenticate products.

Personalization prevents subcontractors from overbuilding, copying, or cloning devices, designs, or firmware.

Secure crypto keys are absolutely necessary for robust security. Private or secret keys must stay secret starting from the time that they are created and injected into the device until their usage in the application. Unique serial numbers, while not necessarily secret, are often used in authentication and other cryptographic operations.

Certicom AMS makes it possible to add Digital Rights Management (DRM) and Conditional Access System (CAS) device personalization to protect DRM and CAS keys during vulnerable (i.e. attackable) manufacturing stages. Using AMS minimizes the risk from liquidated damages clauses contained in High Definition Content Protection (HDCP), Content Protection for Recordable Media (CPRM), Digital Transmission Content Protection (DTCP), and Advanced Access Content System (AACS), and similar agreements. (Note: Certicom is the leading commercial solution for HDCP-enabled chip manufacturing.)

BENEFITS OF AMS

1 **IMPROVED SECURITY:** AMS improves manufacturing security with subcontractors, around the clock.

2 **REDUCED INVENTORY:** AMS reduces over-inventory and waste during manufacturing. SKU selection later in time reduces over-inventory.

3 **BETTER TRACEABILITY:** Tracking of all manufacturing steps across multiple subcontractors is effectuated.

4 **ENHANCED BRAND PROTECTION:** AMS lowers risk of counterfeiting and cloning.

5 **IMPROVED YIELDS AND REDUCED TEST TIMES:** Early defect detection and wafer mapping can pinpoint defects, improving yields and reducing test times.

6 **DECREASED LIABILITY:** Liability from liquidated damages clauses in IP licenses (e.g. HDCP) is lowered.

7 **FIGHTS COUNTERFEITING:** Automated SKU selection prevents counterfeiting. AMS detects grey market clones and counterfeit devices even at insecure low cost subcontractors via key injection.

8 **GUARANTEED SECURE KEY INJECTION:** KeyInject ™ tracks cryptographic keys worldwide and securely injects them into devices.

WHAT DOES AMS DO?

AMS assures visibility at every step in the supply chain to ensure product authenticity.

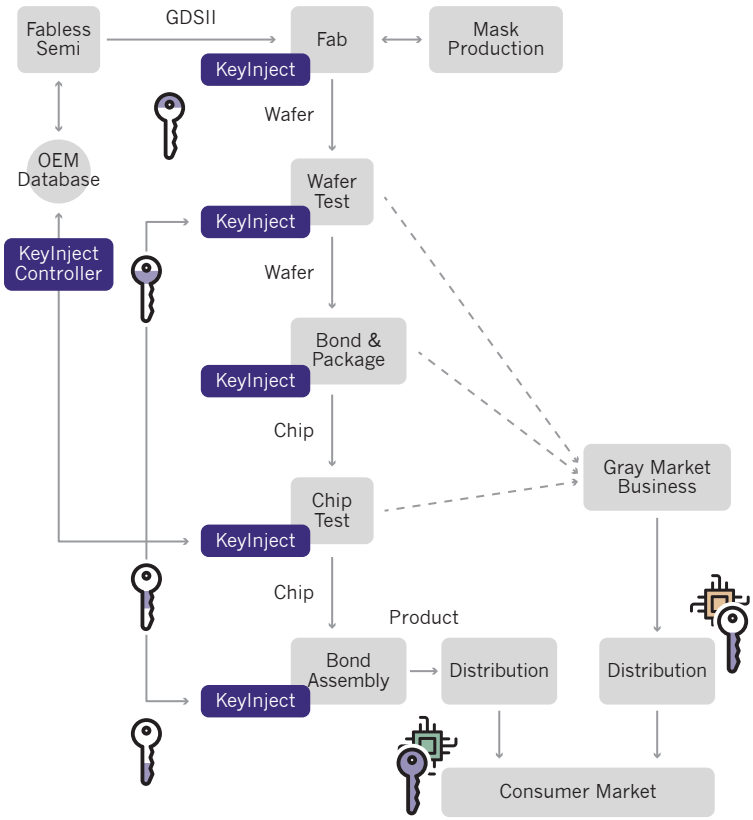
AMS enables device manufacturers and fabless silicon foundries to:

1. **Improve the management and control of electronic serial numbers**
2. **Securely inject cryptographic keys into devices**
3. **Use keys and IDs for feature selection**
4. **Fight cloning and counterfeiting**
5. **Track yield data**

The basic idea behind AMS is to secure remote manufacturing lines by providing visibility and control of offshore manufacturing and test processes to a manufacturer's operations headquarters.

This is accomplished by serializing silicon chips with cryptographic identities on a per-die basis, and tracking those tagged dice throughout production across multiple outsourced contractors and partners.

With AMS various touch points can be easily secured. Therefore, a grey marketer at any step will not be able to gain possession of the complete crypto key, which is only assembled once all the steps have been completed securely at the authorized facilities. Grey market devices, therefore, are easily identifiable and thus cannot supplant authorized devices. The grey marketer is defeated and brand equity and revenue streams are secured.



SERVICE MODULES

AMS has several service modules to address the various requirements of manufacturers.

AMS Service Modules

– **Serialization Service** operates either globally or on a product by product basis to provide serial numbers to devices

– **Yield Log Service** tracks a die from wafer test to final test

– **Static Data Inject** audits devices and locations

– **Processor Data Return** binds secret data to prevent counterfeiting

– **Feature Activation** makes it possible to add features after-market

– **KeyInject®** automates secure key transport, injection, and logging

– **Custom Signing Services (Signature Module)** supports custom signature operations for device personalization.

Signing keys are provisioned for individual product types, allowing them to be managed as protected assets. Signature operations on the factory floor are metered and logged to provide governance and auditability of remote manufacturing sites.

AMS Service Modules

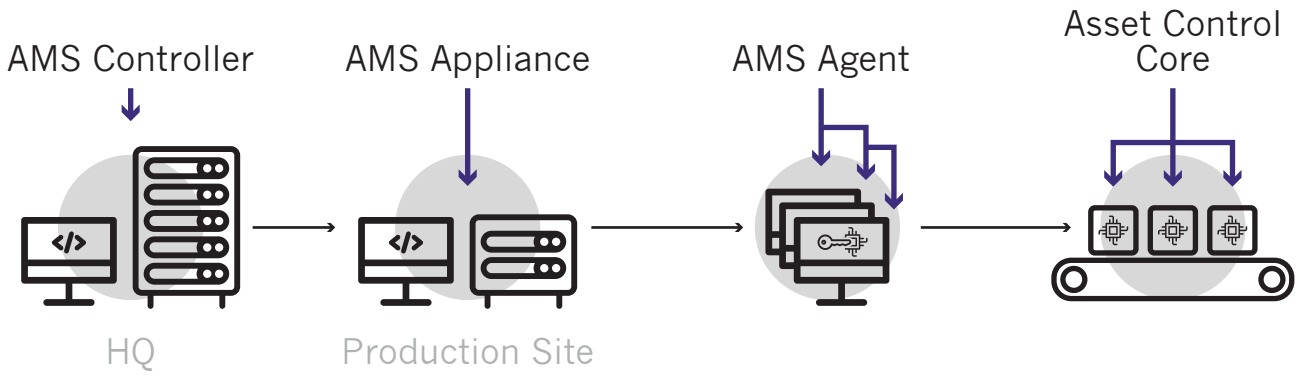
Serialization (DieMax) | Yield Log | Processor Data Return | Key Inject | Feature Activation Service | Static Data Inject | Custom Signing Services

IMPLEMENTATION

Secure appliances being deployed at remote sites enables visibility and control.

As you can see in the diagram, the **AMS Controller** is secured in the operations headquarters. **AMS Appliances** operate in the outsourced manufacturing sites. AMS Appliances communicate with the local automated test equipment (ATE) in the production facilities. The **AMS Agent** runs inside the manufacturing test program installed in the ATEs at the manufacturing sites.

The **Asset Control Core** is an optional IP block built into an ASIC chip (or FPGA), which acts as a feature and key lockbox. Adding the Asset Control Core and provisioning it via the AMS system provides an extremely high level of end-to-end manufacturing and feature provisioning security.



Rack Mounted Appliance
Secure servers with dedicated security hardware located at headquarters. Operated by IT or operations to control remote production sites

Rack Mounted Appliance
Each appliance is made of 2 redundant security servers with dedicated security hardware. One appliance can service many testers.

Tester Software & Device Firmware
AMS Agent is export-approved security software used for integration with the automated test equipment (ATE)

Soft IP RTL Code License
Asset Control Core is RTL code that is integrated into the chip. The chip accepts secure messages from the AMS Agent for customer-defined feature activation and/or secure data and key injection.

SECURING THE SUPPLY CHAIN

With things, such as cars, appliances, medical devices, and other embedded applications becoming connected inside and out, security must become very robust. BlackBerry is well positioned to help design, develop, deploy, and defend security because of Blackberry's experience and reputation in securing the highest volume application to date: mobile enterprise.

Making connected things, infrastructure, and the supply chain secure is where Certicom's AMS and PKI solutions come into play. AMS and managed PKI work together to provide secure key injection and distribution as well as certificate management services to issue, manage, renew, and revoke security certificates.

ASSET MANAGEMENT SYSTEM

Secures manufacturing supply chain to prevent cloning and inject security keys

MANAGED PKI

Certificate management for telematics, IVI, ECUs, domain/area controllers, V2X, OTA & anything that connects

EXAMPLE USE CASE: SIRIUSXM SATELLITE RADIO (KEY INJECT)

Certicom provided SiriusXM Satellite Radio with a complete security solution including initial consulting; designing the security architecture; customizing conditional access design and implementation; and providing firmware, middleware, and a key provisioning system.

Certicom's three product lines of security libraries, Asset Management System, and Managed PKI System provide a convenient way to implement a highly secure conditional access system.

User-Friendly Activation and Authorization

User-friendly activation is a key feature for satellite radio because it helps to avoid putting bona fide customers through a painstaking and time-consuming activation process. The heart of the solution is a unique hardware key that is burned into each radio during manufacturing and stored in a tamper-resistant memory location to provide seamless activation and authorization.

Content Protection

Content protection, as the name implies, protects valuable media assets (the content) from piracy. Content is encrypted for transmission over-the-air so only intended recipients can decrypt and listen to the satellite radio service. The content is decrypted in tamper resistant hardware, which protects against unauthorized replication or copying, preventing attackers from obtaining a digital copy of the clear content.

Conditional Access

Conditional access limits reception to authorized subscribers. It relies on certain secret information, burned into the receiver, and other data that is transmitted over the air on a Broadcast Authorization Channel (BAC). To block unauthorized users from access, only authorized subscribers receive the decryption keys

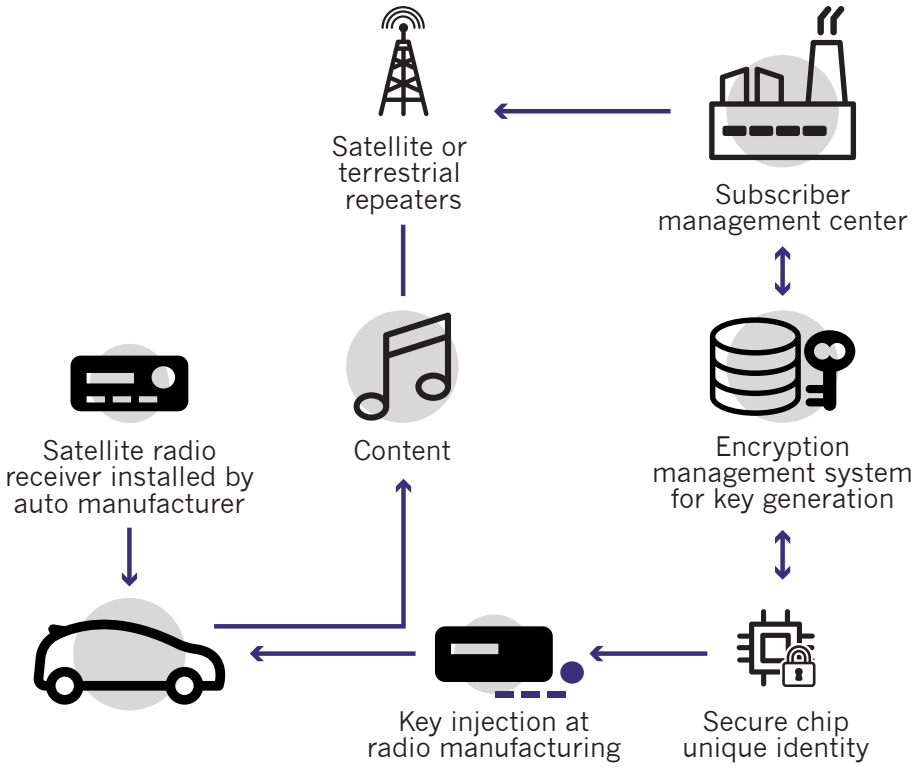
Renewability

If a radio has been cloned, the service revokes service to that radio. This reduces the costs associated with cloning.

Manufacturability

Certicom worked directly with receiver manufacturers to ensure the proper design of security mechanisms and cost-effectiveness.

A Certicom-based conditional access system maximizes revenues by safeguarding against theft of service, protecting content against over the air copying, integrating security mechanisms transparently for an unimpeded user interface, and supporting service renewability to manage content and enable revocation in the event of an attack.



EXAMPLE USE CASE: OVER THE AIR (OTA) UPDATES

To address the growing need for secure over the air (OTA) updates to cars (and other types of equipment) secure manufacturing techniques such as AMS, certificate management, and connectivity can be brought together to create an innovative secure over the air (OTA) software update management platform. Such a platform can be globally scalable and securely establish a cryptographic root of trust, provision devices, perform authentication, and securely make software updates via easy to use web based tools.

OTA PROCESS

Creation	Upload	Distribution	Installation
▪ Software package(s) are created by OEM or suppliers.	▪ Packages are uploaded to a hosted or cloud based service. ▪ Made available to vehicle via service API.	▪ Vehicle or embedded system checks for updates via polling or are notified of pending updates.	▪ Vehicle or embedded system checks update and installs on target.

Certicom's AMS and Managed PKI work together with other BlackBerry technologies and services including the mission-critical QNX OS, BlackBerry IoT infrastructure, and BlackBerry CyberSecurity Services to enable a highly secure OTA solution for vehicles and other embedded systems.

In the OTA application AMS provides secure device provisioning of a secret cryptographic key via the key inject module using secure equipment deployed at manufacturing sites. Certicom's Managed PKI System manages authentication by being the root certificate authority and by issuing, managing, renewing, and revoking certificates during the life of the target device. (These functions and others are called out in the table below.)

BLACKBERRY OTA SECURITY - END TO END

Device Provisioning

Certicom

- Silicon asset management (AMS)
- X.509 certificates

QNX OS

- QNX layered security
- Secure boot
- Access control
- Intrusion detection
- Others

Authentication

Certicom

- Root certificate authority to verify vehicle certificate
- Certificate issuing, management, renewal, & revocation (Managed PKI Services)

Device and User Auth Flows

- Mutual Authorization
- OAuth 2.0
- Permissions firewall
- Service token
- AES 256
- Token Revocation

Secure Data Transmission

- TLS 1.2 encrypted data channels
- ECDSA 521 bit packet signing
- Strong hash on package contents
- Signed manifests
- Forward secrecy so historical packages cannot be decrypted

Threat Response

BlackBerry CyberSecurity Services

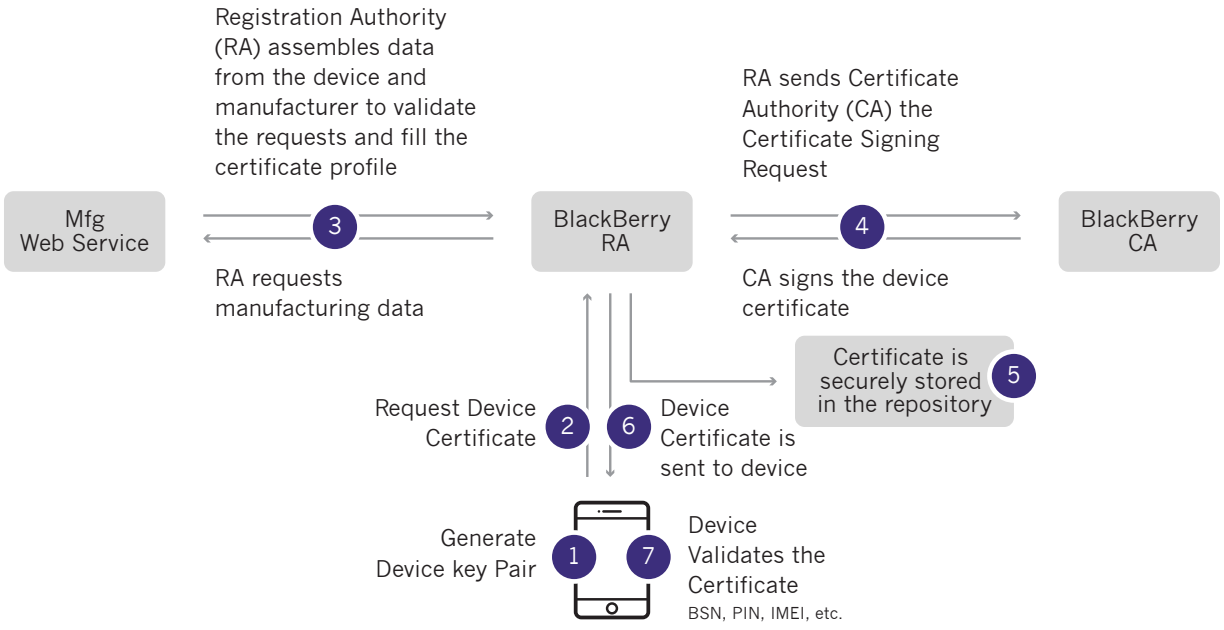
- 24/7/365 monitoring of applications infrastructure and service
- Proactive penetration testing
- Incidence response teams
- Threat containment
- Global redundancy
- Security consulting

EXAMPLE USE CASE: BLACKBERRY MOBILE DEVICES

The iconic use case showcasing Certicom's Asset Management System (AMS) for secure chip provisioning is that of BlackBerry mobile devices. Using AMS allows BlackBerry to govern outsourced manufacturing and fight cloning.

Provisioning of the core mobile chip in the BlackBerry device is done in a factory that has been secured via the deployment of AMS. The Key Inject module of AMS, as the name implies, securely injects the private key. That injected key acts as an endorsement key, which is used to establish a chain of trust that securely ties the device-generated key pair to the root of trust, which is the BlackBerry Certificate Authority (CA). AMS is used in conjunction with Managed PKI to install, manage, renew, and revoke certificates according to the applicable security policy. Given the large number of BlackBerry devices, it should be clear that this system is designed for scalability.

The diagram shows the registration process using the endorsement key that was securely injected by AMS into the chip and subsequently installed in the phone.



NOT JUST SECURE, BUT BLACKBERRY SECURE

There is a reason that BlackBerry is synonymous with security

It is because security is as elemental to an electronic system as DNA is to an organism—and security is BlackBerry's DNA.

Robust security cannot just be bolted on. It must be infused right from the start, which is why BlackBerry Security has been trusted by world leaders for over two decades and is the mobility partner of all G7 governments, 16 of the G20 governments, 10 out of 10 of the largest global banks and law firms, and the top five largest managed healthcare, investment services, and oil and gas companies. BlackBerry Security has earned more than 70 government certifications and approvals - greater than any other mobile vendor.

Vulnerabilities are growing rapidly and present a serious risk, so BlackBerry continues to expand its coverage with advanced technologies, tools, design consulting, and testing services for true end-to-end, layered security.

World leaders
in government and
industry trust
BlackBerry Security
to help run their secure
communications,
networks,
in-car systems,
nuclear infrastructure, and
other mission-critical
functions.

Learn what they have
already discovered.

BlackBerry and its subsidiaries, Certicom and BlackBerry QNX, provide products and services that make things not just secure, but BlackBerry Secure.

Certicom Corp., subsidiary of BlackBerry manages and protects the value of content, applications, and devices with government-approved security. Elliptic Curve Cryptography (ECC) provides the most security-per-bit of any known public key scheme. As the global leader in ECC, Certicom has licensed its security offerings to hundreds of multinational technology companies, including IBM, General Dynamics, and SAP. Founded in 1985, Certicom's corporate office is located in Mississauga, Ontario, Canada.

www.certicom.com

BlackBerry QNX, subsidiary of BlackBerry is a leading vendor of operating systems, development tools, and professional services for connected embedded systems. Global leaders such as Audi, Cisco, General Electric, Lockheed Martin, and Siemens depend on QNX technology for vehicle infotainment units, network routers, medical devices, industrial automation systems, security and defense systems, and other mission- or life-critical applications. Founded in 1980, QNX Software Systems Limited is headquartered in Ottawa, Canada.

www.qnx.com