BlackBerry | certicom

Certicom Asset Management System
Securing Automotive and IoT Device Manufacturing

AUTOMATES KEY LOGISTICS, MITIGATES FINANCIAL RISK, AND DELIVERS PROVEN ROI

The world's leading chip manufacturers already rely on Certicom Asset Management System (AMS) technology for both in-house or offshore device manufacturing for serial numbers, certificates, keys, and data objects provisioning.

More than any other form of serialized data, keys are difficult to track. Especially given the liability that manufacturers such as HDCP licensees are exposed to, companies are re-evaluating whether an in-house key management system provides sufficient protection. Not only does building a reasonably secure tracking system consume valuable NRE and operations capacity, most still include manual processes like FTP sites and email that make costly mistakes more likely than a fully automated solution that is tightly integrated with existing systems.

HDCP Licensee Concerns Resolved

- $8M max liability, per Product, if Mishandle Keys

- Tracking of HDCP Rx and Tx Key Inventory

- Contract Manufacturers Double Programming Keys

- Stolen or Lost Keys at Outsourced Assembly and Test

- Keying Issues That Can Stop Production Line

A proven solution for manufacturers, Certicom AMS integrates quickly and easily into your in-house or outsourced manufacturing process, securely delivers HDCP keys to ATE for injection during test, and provides ROI within the first year of operation.

SECURE MANUFACTURING

Using state of the art cryptography, security protocols and tamper proof hardware-based security, AMS keeps your keys protected right up until they are injected into a product.

EASE OF INTEGRATION

From XML reporting for ERP systems to C-APIs for Chip Testers, AMS quickly and easily integrates into existing manufacturing processes and systems.

KEY INVENTORY LOGISTICS

AMS distributes keys to both local and remote factories based on factory throughput and protects them until they are injected on the line. The notification system automatically alerts operations staff about potential issues before they become problems.
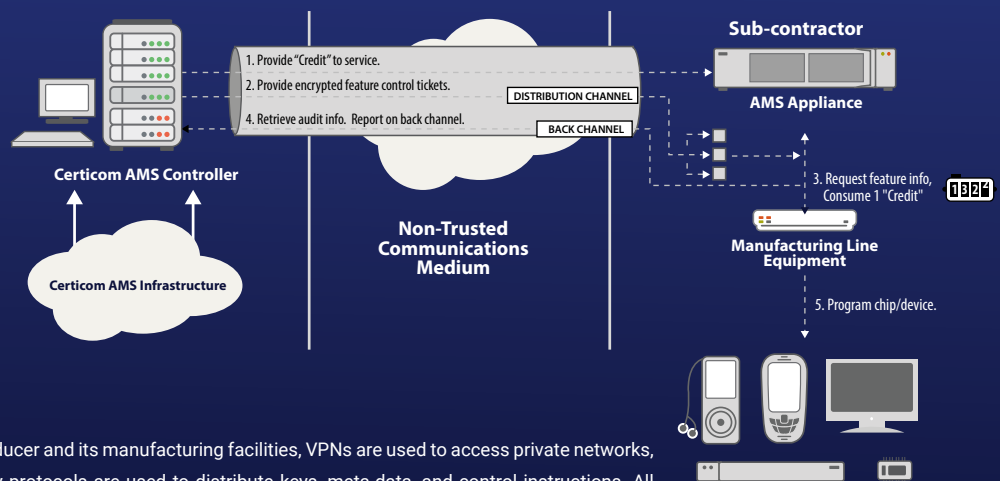
REDUNDANCY AND 24X7 SUPPORT

Understanding the criticality of high availability, AMS systems are always shipped in redundant pairs and KeyInject includes 24x7 support agreements that are tailored to the needs of global manufacturing operations teams.

Certicom AMS KeyInject Includes:

- COTS Infrastructure Components
- Chip Tester Middleware Licenses
- 24x7x365 Operations Support
- Integration Services

Supported ATEs include Verigy, Advantest and others.

Sub-contractor

1. Provide "Credit" to service.
2. Provide encrypted feature control tickets.
DISTRIBUTION CHANNEL
4. Retrieve audit info. Report on back channel.
BACK CHANNEL

AMS Appliance

Certicom AMS Controller

3. Request feature info, Consume 1 "Credit"

Certicom AMS Infrastructure

Non-Trusted Communications Medium

Manufacturing Line Equipment

5. Program chip/device.

Many layers of security are employed by AMS between a chip producer and its manufacturing facilities, VPNs are used to access private networks, SSL authenticates connection sessions, and proprietary security protocols are used to distribute keys, meta-data, and control instructions. All logging data is sequenced and encrypted to ensure that remote logs cannot be tampered with or deleted without being detected.

Certicom Asset Management System

MULTIPLE PRODUCT SKU FEATURES

- Package multiple keys for the same chip
- Track multiple keys associated with the same SKU
- Transmit custom meta data in-band with key data to protect proprietary and secret chip configuration data

SUPPORT FOR MOST KEY TYPES

- Natively supports most other CA and DRM keys
- Custom key type support for proprietary keys using XML definitions
- Control which key types are allowed to be sent to which remote factories

SECURITY FEATURES

- All keys, configuration, and logs are protected by FIPS 140-2 Level 3 HSM hardware
- Implemented with government approved cryptography using ECC, RSA, AES-256 and SHA-256
- Multiple layers of best-in-class security that meet industry standards
- Security protocols that are unique BlackBerry AMS

24X7X365 OPERATIONS SUPPORT OPTIONS

- ATE and test script integration services available
- Business system integration services available
- 24x7x365 support options

CERTICOM AMS INCLUDES THESE COMPONENTS

AMS CONTROLLER

- Located at headquarters or trusted location
- One instance used to control several servers
- Rack-mounted server
- Managed and operated by Operations team or IT
- XML interfaces for integration into existing ERP infrastructure

AMS APPLIANCE

- Located at test house, 3rd party manufacturer, assembly, any keying location
- One instance serves many agents
- Redundant, security hardened, rackmounted servers with FIPS 140-2 Level 3 security modules

SOFTWARE AGENT

- Embedded in ATE or custom test equipment
- ANSI C code pre-ported to all common ATE operating systems
- Integrates with test methods

24x7 Support Plans provide a critical severity response hot line using expert, in-house, technical support staff that work closely with escalation engineers fielded around the globe.

Your keys are never exposed. Certicom AMS KeyInject integrates with any company's proprietary on-chip encryption scheme. And you can also encrypt any keys all the way to silicon for additional security when you combine Certicom AMS.

BLACKBERRY CERTICOM

As a leader in applied cryptography and key management, BlackBerry Certicom provides managed PKI, key management and provisioning technology that helps customers protect the integrity of their silicon chips and devices from the point of manufacturing through the device life cycle. Used to prevent product counterfeiting, re-manufacturing, and rogue network access, BlackBerry Certicom's secure key provisioning, code signing and PKI solutions are field-proven to protect next-generation connected cars, critical infrastructure and IoT deployments.

BlackBerry | certicom