Product Authentication Certicom AMS

Craig Rawlings

Certicom Corporation

NIST Product Authentication Information Management Workshop

February 17-18, 2009

Certicom Asset Management System

A Proven Solution

XM SATELLITE RADIO

SICON SEMICONDUCTOR

AMD The future is fusion

MICRONAS

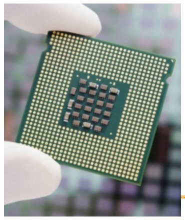
- Installed at ASE, Amkor, UTAC & STATS among others
- Current customers include:
  - One of the largest multi-national semiconductor manufacturers
  - One of the largest multi-national fabless semiconductor companies
  - A number of premiere device / semiconductor manufacturers
    - Names protected by NDA

Certicom Asset Management System

IDM and Fabless Customer Benefits

Benefits:

- ✓Reduced engineering development costs
- ✓Lower manufacturing costs
- ✓Improved time-to-yield
- ✓Product revenue protection (gray mkts)
- ✓Enables after-market business models
- ✓Brand protection



What is the Certicom Asset Management System?

- AMS is a unique enterprise class solution that combines embedded Silicon IP (SIP) and advanced hardware and software cryptography integrated into secure ease-of-use IT infrastructure appliances

- AMS system is composed of –
  - **Platform Products:**
    - ***Asset Control Core*** (SIP)
    - Cryptographic Acceleration Options (SIP)
    - ***AMS Controller*** – management console appliance co-located in customer’s corporate data center
    - ***AMS Tester Agent*** – Secure agent that resides on ATE(s) at the customer site or an OSAT
  - **AMS Appliance Service Modules:** AMS DieMax™, AMS KeyInject™, AMS ChipActivate™, and AMS SysActivate™

Certicom Asset Management System (AMS) Value Centers

- **Corporate**
  - ✓ **AMS DieMax –** Analysts are estimating that $100B of electronic equipment is composed of counterfeit, cloned, or over-production devices
  - ✓ The future damage via the inadvertent development of competitors through off-shore manufacturing relationships is not well understood, but is perceived to be significant to companies in N. America, Europe, and Japan
  - ✓ The price erosion caused by grey markets may be eliminated with AMS DieMax when used to implement anti-counterfeiting, anti-cloning, and IP protection features
  - ✓ The corporate brand image is protected from poor quality and reliability associated with counterfeit or cloned devices
  - ✓ The cost savings due to support for RMA support of non-genuine devices is eliminated
  - ✓ Recycling of used parts as new devices by crooked channels is eliminated
  - ✓ Customers have the ability to validate genuine products and platforms that have been delivered unmodified after leaving the factory
  - ✓ Lost revenue due to grey market activity is recaptured, support costs are reduced, the corporate brand is protected, and gross margins encounter reduced pressure

Certicom Asset Management System (AMS) Value Centers

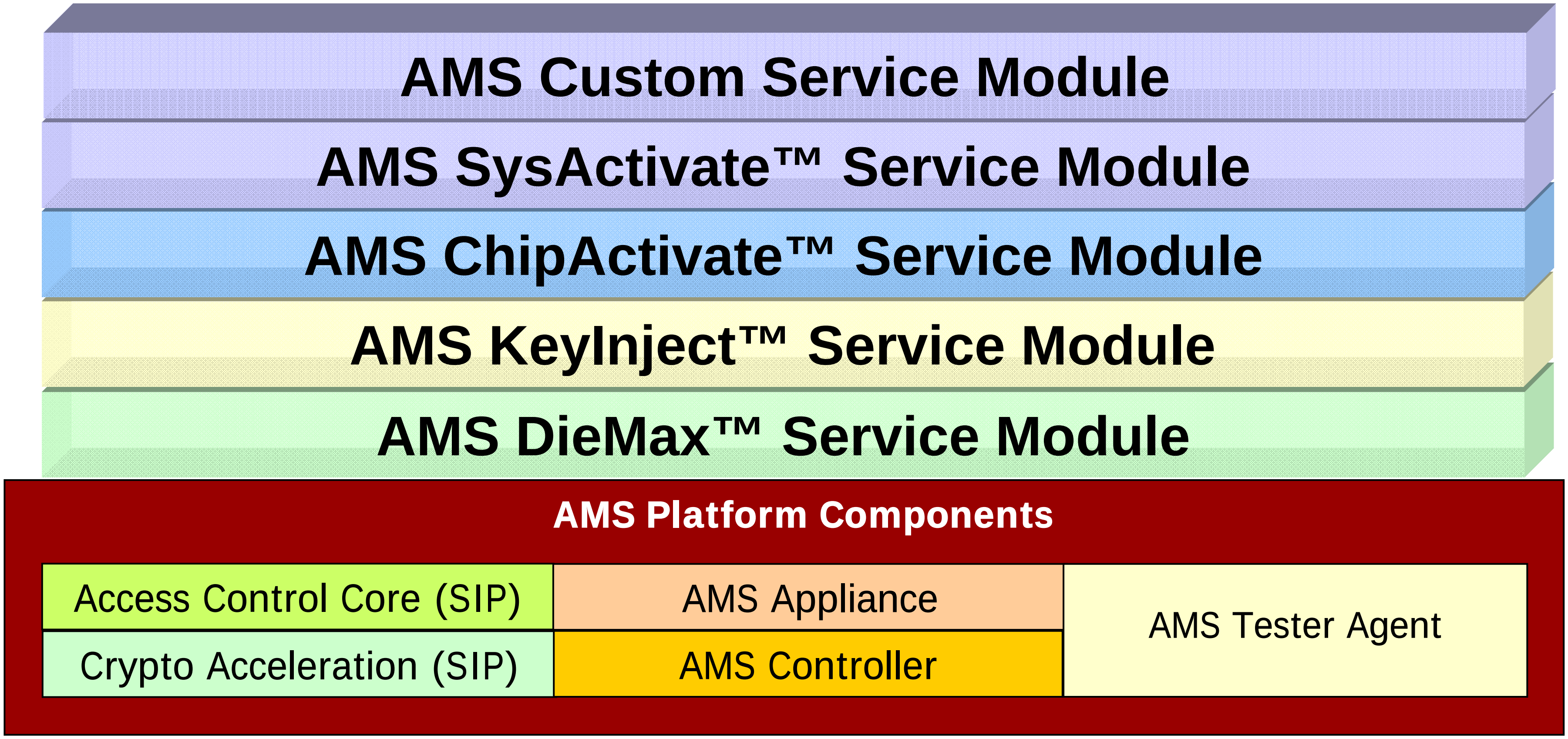
- **Product Development**
  - ✓ **AMS ChipActivate** - Feature activation module enables a single chip to be configured in post production with multiple feature sets. This reduces engineering costs associate with masks, chip design and layout, verification, debug, and testing/qualification
- **Manufacturing**
  - ✓ **AMS DieMax** – Secure and timely reporting of manufacturing (yield) data for work-in-process translates into rapid Time-to-Yield
  - ✓ Sensitive technology information is protected throughout the global supply chain protecting against undesired technology transfer (technology leaks)
  - ✓ Testing may rapidly be optimized based on targeted manufacturing results
  - ✓ Die tracking and tracing for RMA troubleshooting and failure analysis
  - ✓ **AMS ChipActivate –** reduction in SKUs with soft SKU'ing, the ability to configure one physical SKU in post-production in support of Just-In-Time manufacturing or Kanban operations
  - ✓ Reduced cost of forecasted mix errors and their impact on corporate working capital, inventory obsolescence risk, carrying costs, and inventory price reductions

Certicom Asset Management System (AMS) Value Centers

- **Manufacturing (continued)**
  - ✓ **AMS KeyInject** – Secure key management protecting against liabilities associated with liquidated damages, the amount owed to the key licensor in the case of exposing a key to a protected key to a third party (up to $8M for HDCP keys)
  - ✓ Automated and secure distribution of protected and/or sensitive data throughout the global supply chain over the internet
  - ✓ Tracking and management of sensitive data such as protected keys for business processes and operations; KeyInject assures that no unique keys are programmed into more than a single device; inadvertently unused keys are identified, re-inventoried, and available for use
  - ✓ Sensitive Key information such as HDCP Keys may be transported from the licensor to the key licensee using Certicom's eCourier™ (endorsed by DCP LLC for electronic distribution of HDCP keys)

- **Marketing**
  - ✓ **AMS ChipActivate / SysActivate –** Improved forecasting accuracy and delivery times to customer change orders and reduced incidence of customer allocation exercises
  - ✓ More timely response to changes in market and product requirements and extended product life cycles mean increased customer satisfaction and increased market share
  - ✓ Increased market share and new revenue opportunities may be captured by selling base features at a low cost and up-selling after-market features at a premium price

Certicom Asset Management System



AMS Custom Service Module

AMS SysActivate™ Service Module

AMS ChipActivate™ Service Module

AMS KeyInject™ Service Module

AMS DieMax™ Service Module

AMS Platform Components

Access Control Core (SIP)

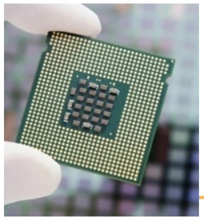
Crypto Acceleration (SIP)

AMS Appliance

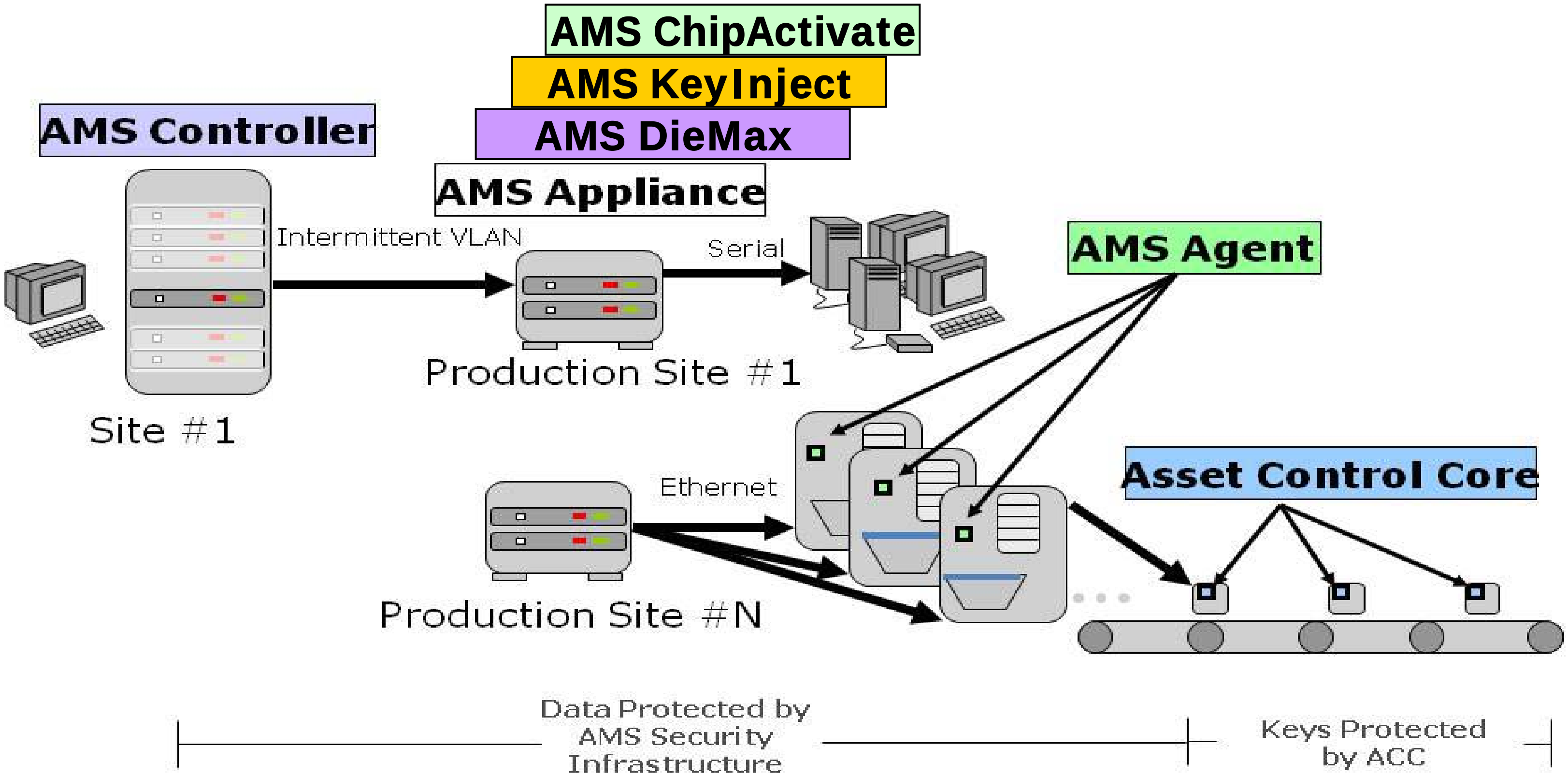
AMS Controller

AMS Tester Agent

AMS is composed of modular components that are integrated specific to the customer's requirements

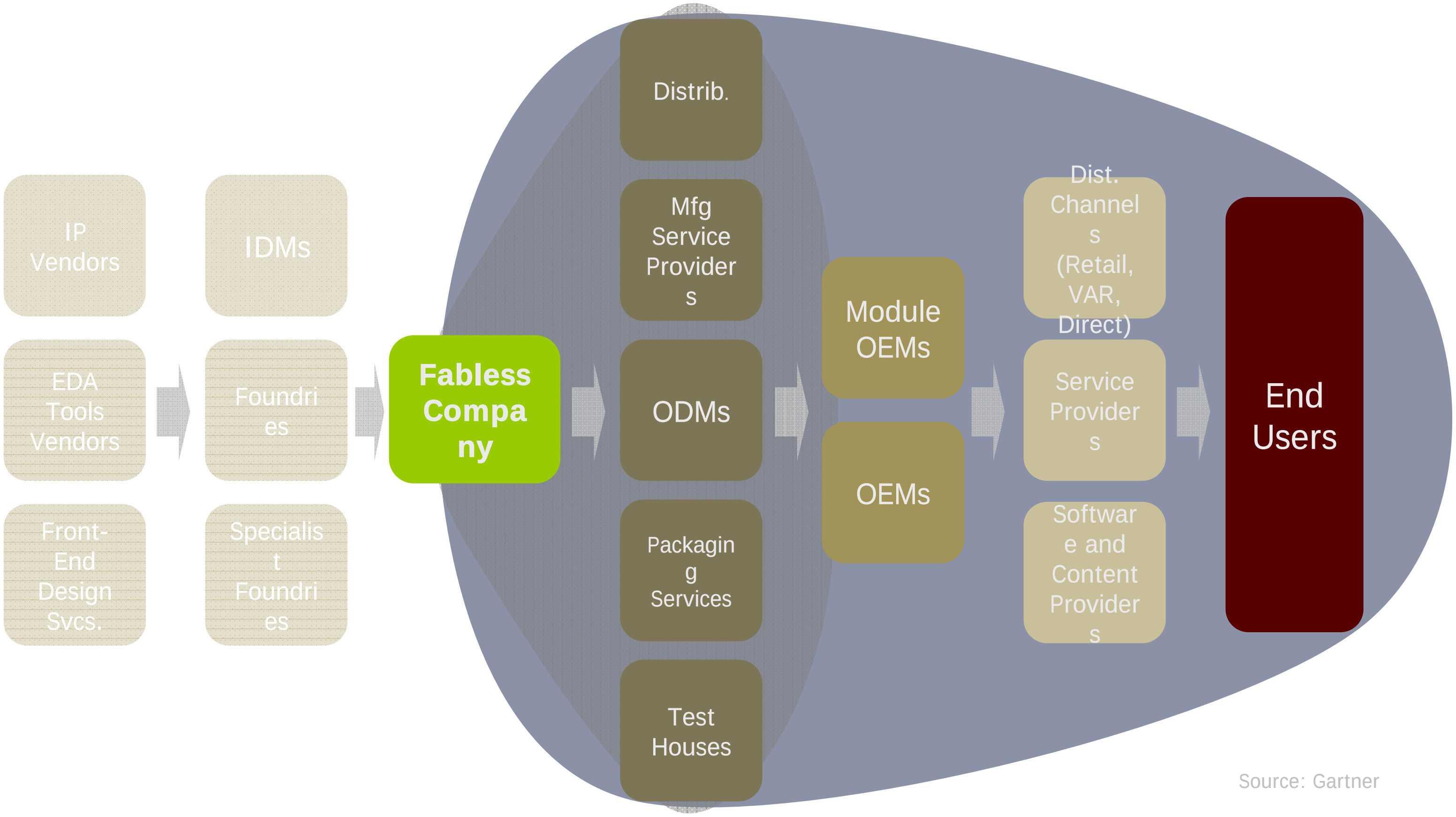


Certicom AMS Topology



Certicom Silicon Asset Management

Expand your influence within the Semiconductor Value Chain

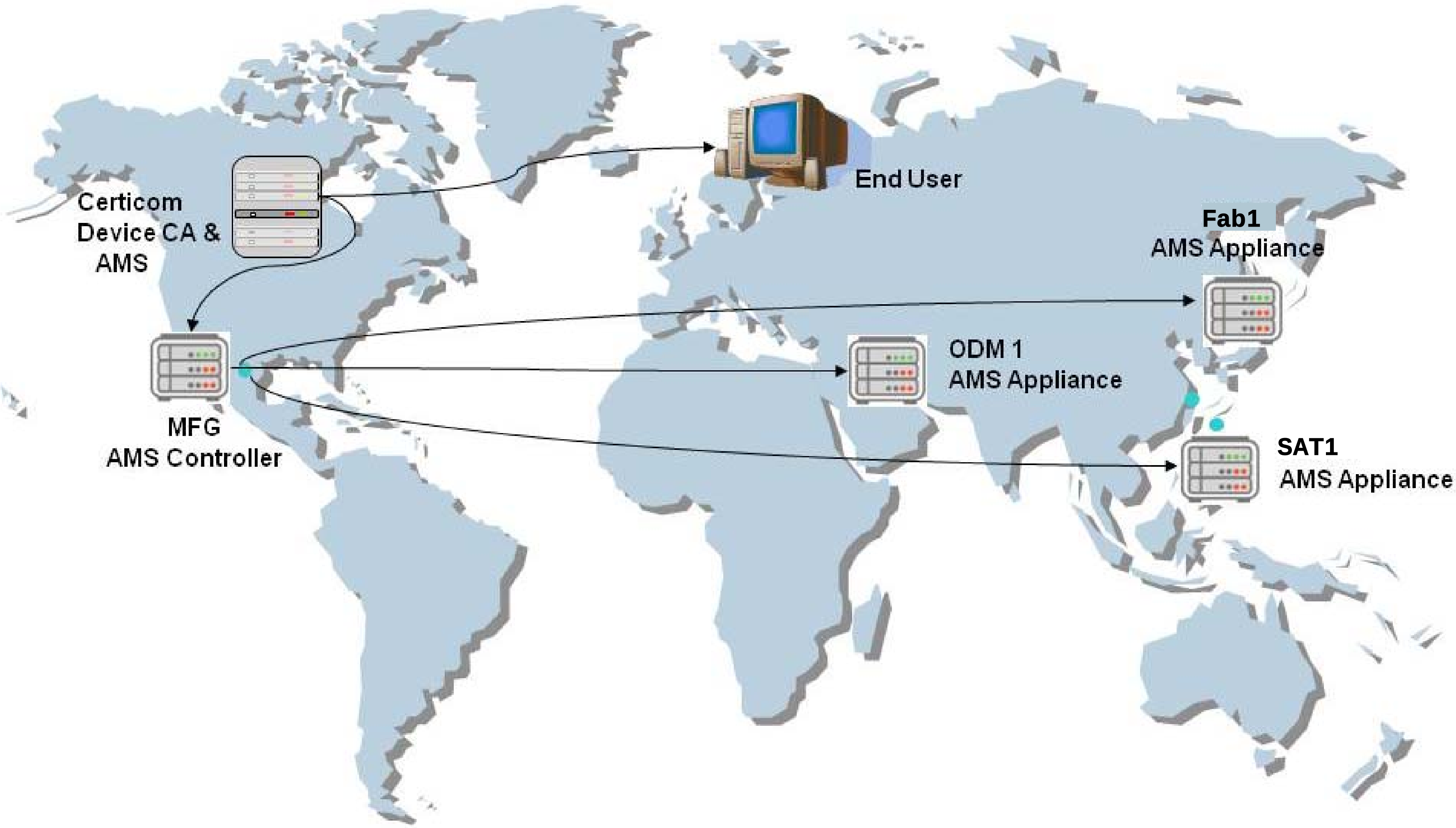


Source: Gartner

Gain vision and control throughout your outsourced manufacturing environment

Certicom AMS Deployed

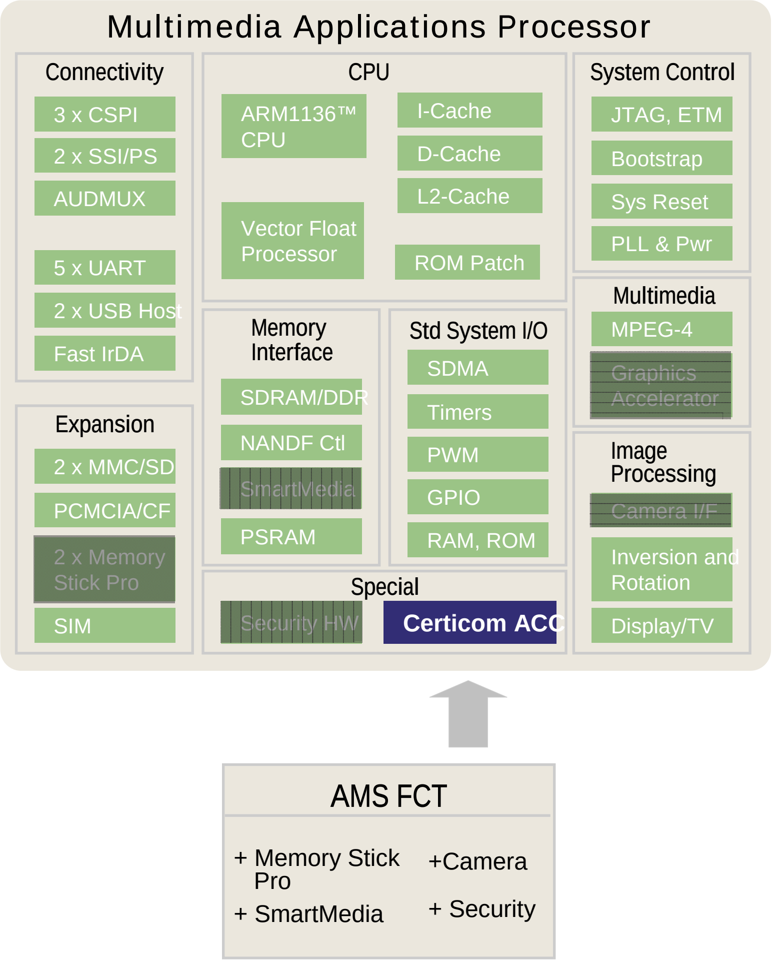
Secure Control - Anywhere



AMS Controller/AMS Appliance

AMS Platform Silicon IP –
Asset Control Core

- Certicom Asset Control Core (ACC)
  - The chip endpoint for AMS
  - Control chip configuration, fuse blowing, NVM access
  - Enable/Disable/Re-enable chip features
  - Extends trust to firmware
  - Ultimate protection during communication
  - **Key once, manage the entire chip lifecycle!**



Multimedia Applications Processor

Connectivity
3 x CSPI
2 x SSI/PS
AUDMUX
5 x UART
2 x USB Host
Fast IrDA

CPU
ARM1136™ CPU
I-Cache
D-Cache
L2-Cache
Vector Float Processor
ROM Patch

System Control
JTAG, ETM
Bootstrap
Sys Reset
PLL & Pwr

Multimedia
MPEG-4
Graphics Accelerator

Expansion
2 x MMC/SD
PCMCIA/CF
2 x Memory Stick Pro
SIM

Memory Interface
SDRAM/DDR
NANDF Ctl
SmartMedia
PSRAM

Std System I/O
SDMA
Timers
PWM
GPIO
RAM, ROM

Image Processing
Camera I/F
Inversion and Rotation
Display/TV

Special
Security HW
Certicom ACC

AMS FCT
+ Memory Stick Pro
+Camera
+ SmartMedia
+ Security

AMS Now More Than Ever…

- ✓ To reduce development costs
- ✓ To reduce operating costs
- ✓ To protect against counterfeiting
- ✓ To protect against technology transfer
- ✓ To create new revenue opportunities
- ✓ To gain a competitive edge and increase market share
- ✓ To protect corporate branding