Security Solutions

MPU Team

June 2016

Introduction

- **Atmel is a long-term provider of solutions for the Point of Sales Terminal market**
- **Microchip's MPUs leverage this strong expertise from the Payment standards for addressing security requirements of all the markets**
  - Cryptography for Confidentiality, Integrity and Authentication
  - Intrusion detectors
  - Hardware attack detectors
  - Software and Data Integrity checking
  - Secure Boot for Root of Trust
  - Key Provisioning Tools
- **Let's go through all these features**

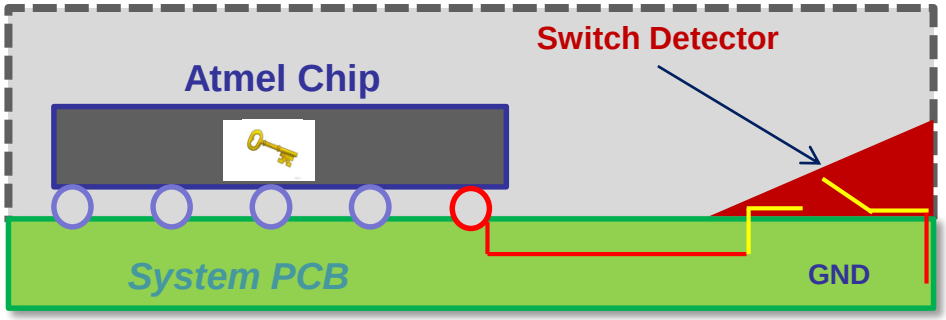
Environmental Monitors

- **Voltage Monitor**
  - Monitors the device power supplies VDDCORE and VDDBU, checks they are operating within the specified voltage range
- **Frequency Monitor**
  - Checks the parts not operating at frequencies out of its specification
- **Temperature Monitor**
  - Checks the part is within its operating temperature range

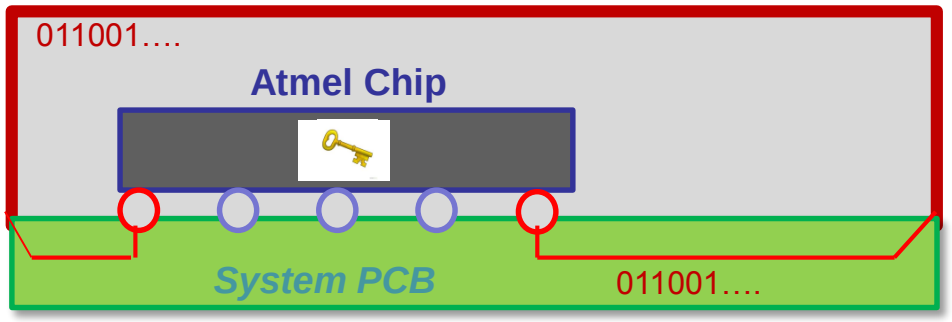
- **Each monitor trigs an alarm if the parameter is out of its range**

Static and Dynamic Tampers

- **Detects Physical Intrusion to the System**
- **Static**
  - Connected to the system enclosure with switches
  - Detects opening

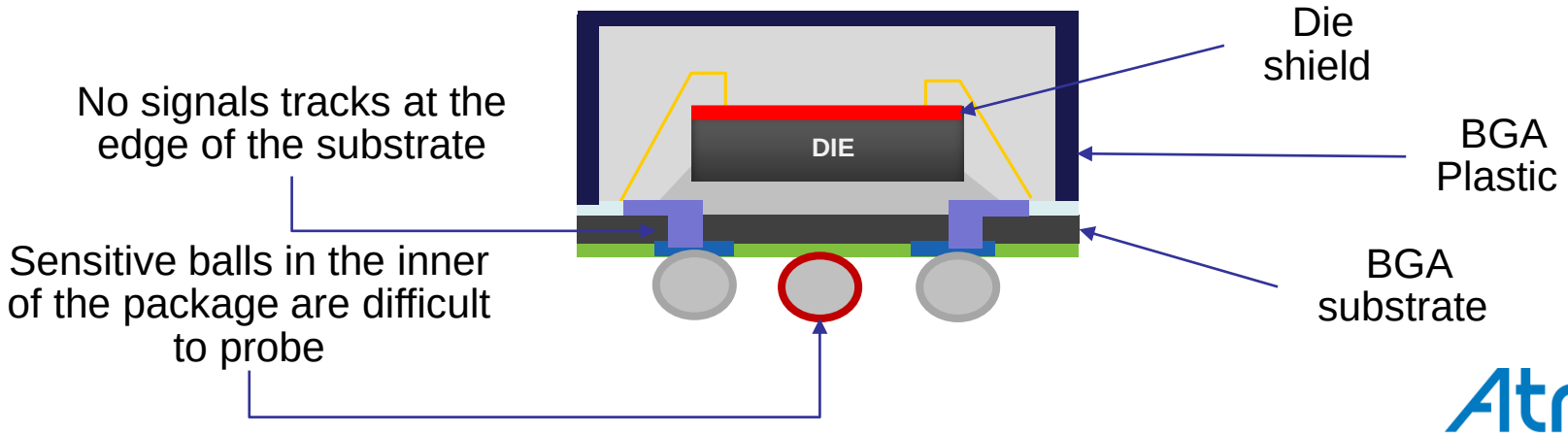


- **Dynamic**
  - Connected to an external shield to protect critical PCB area
  - Detects
    - Removal
    - Drilling
    - Perturbation



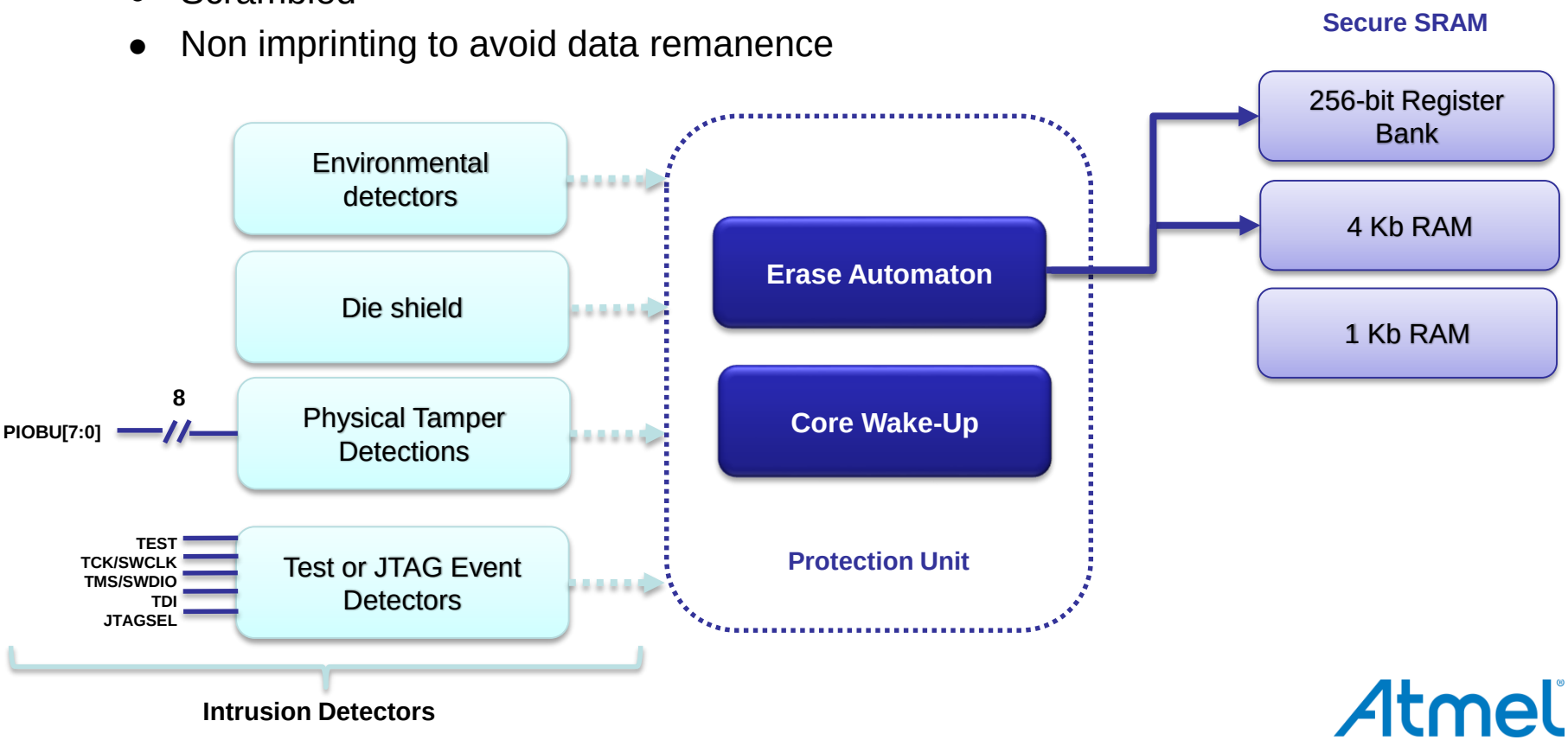
Die and Package Security

- **Die active shield**
  - An extra metal layer carries random patterns and triggers a tamper in case of die probing
- **Stubless package**
  - Signals tracks on the package's substrate are kept away from the edge avoiding microprobing attempt
- **Protection of sensitive signals**
  - Sensitive balls are placed in the inner section of the package to be protected while soldered on the PCB



Secure SRAM

- **Secured backup memories allows keeping critical keys and data safe**
  - Supplied on VDDBU (Backup Supply)
  - Automatic erasure upon tamper or alarm detection
  - Scrambled
  - Non imprinting to avoid data remanence



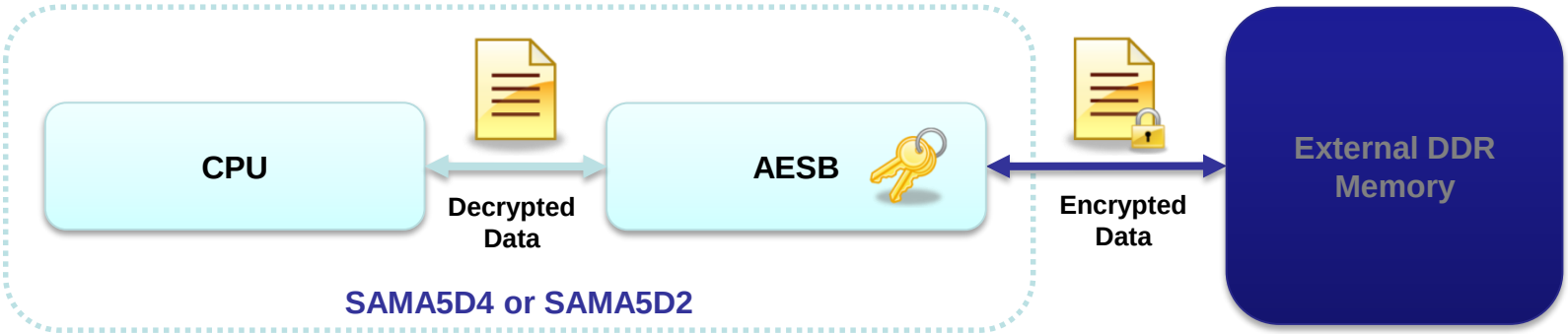
Integrity Check Monitor

- **The ICM monitors data integrity in memories**
  - Up to 4 regions, performed in background
- **It is a DMA Controller that performs SHA-based memory hashing on different memory regions**
  - Internal Memories: Secured SRAM (SECURAM), SRAM
  - External Memories: SRAM, PSRAM, DDR2, LPPDR1, LPDDR2
- **Hash value (also called digest) can be**
  - Moved to memory as a reference digest (ICM Hash area)
  - Compared to a reference digest from the ICM Hash area

- **A digest mismatch will trig an interrupt**
- **Bus Burden Control to reduce ICM bandwidth on system bus**

External Memory Encryption

- **The AESB is an AES Bridge operating on-the-fly on a data path**
  - It cyphers data written into the DDR or into the QSPI
  - It decrypts data read out of the DDR or out of the QSPI
- **128-bit key AES**
  - The key has to be programmed in an AESB register
- **Features counter measure**
  - In order to avoid retrieving the customer key by SPA/DPA analysis

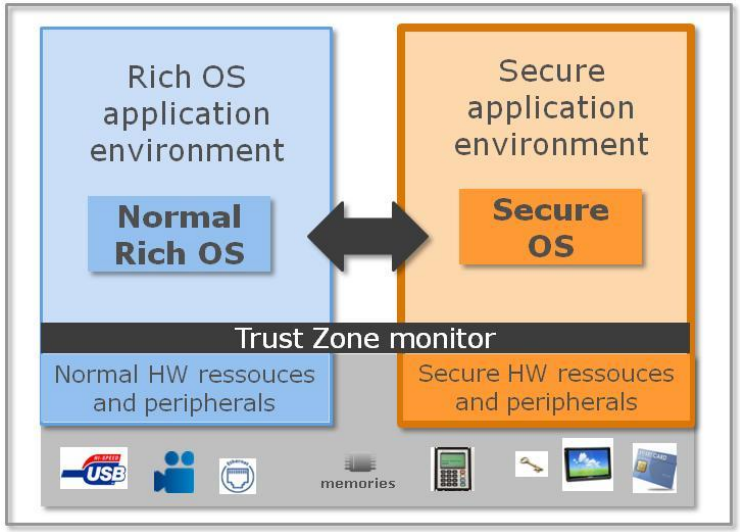


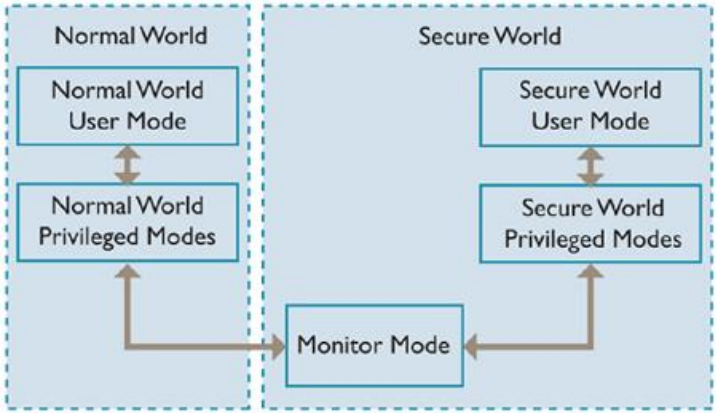
Cryptography Solutions

- **Hardware Accelerators**
  - Symmetric
    - 128, 192 and 256-bit AES, DES and 3DES
  - Asymmetric
    - RSA up to 5408-bit, RSA CRT up to 6144-bit
    - ECC up to 1504 bit, ECDSA up to 1504 bit, DSA, Key Generation
  - Hashing
    - SHA 1, SHA-256, 384 and 512
- **Cryptography Library**
  - Asymmetric Crypto Library including counter measure
- **True Random Number Generator (TRNG)**

TrustZone

- **TrustZone is an ARM technology allowing a system to be partitioned in 2 worlds on a single core**
  - Trusted and Non-Trusted
  - Most often used to create a Secure world
    - A normal Rich OS (Linux) which executes in the Normal world
    - A TrustZone Monitor managing the system security
- **The SAMA5D4/D2 matrix supports TZ**
  - Each peripheral can be defined Secured or Non-Secured
    - Except a few which are always secured
  - Memory areas can be defined as secure or non-secure
  - The device has 2 Interrupt Controllers
    - One Secure driving the FIQ
    - One Non-Secure driving the IRQ





CoreTEE

- **TEE = Trusted Execution Environment**
- **CoreTEE is a Sequitur Labs technology**
  - Based on OP-TEE + Significant feature enhancements
  - Global Platform's TEE standards compliant
- **CoreTEE Features**
  - Secure Boot
  - Secure Peripherals
  - Secure data storage
  - Trusted Applications and Application Provisioning
  - Concurrent TA execution
  - Trusted remediation in case of rich OS failure
  - Key Management
  - TEE services simplify secure access to:
    - RNG, PKCS, SHA, AES, TDES, AESB, ICM

Secure Boot

- **The boot application is encrypted and signed before being stored in the external NVM**
  - Encryption with AES-CBC
  - Signature with AES-CMAC or RSA
  - The Encryption Keys are stored in a fuse matrix
- **Then at startup, the bootloader in the ROM Code**
  - Downloads the image
  - Authenticates the image
  - If authenticated, decrypts it and stores it in an embedded SRAM
    - Embedded SRAM only, of course, never in external memories
  - Then, gets it started
- **If the image is not authenticated, nothing happens as it could be a malicious code**
  - Ends in a while(1), with watchdog activated

SAM-BA in Secure Mode

- **SAM-BA is used**
  - To program the boot application in Secure Mode
  - To program the keys in the fuses
- **SAM-BA has 2 operating modes**
  - SAM-BA Cypher encrypts the boot application
  - SAM-BA Loader downloads the encrypted boot and programs the keys
- **Improvements to come**
  - SAM-BA to support key diversification
    - Selects a new key for each system, re-encrypts the boot application and program the encrypted image as well as the new key

PCI Pre-certification

- **PCI 4.0 is required for POS market**
- **SAMA5D2 has been pre-evaluated by a PCI accredited lab (UL)**
  - Extensive invasive and non-invasive testing on the chip
  - Testing report for customer's lab saving cost and time during PCI certification process
  - Provided with a set of recommendations for the system level integration

Summary

- **Security is a growing requirement**
  - In all markets, but more specifically the communicating objects
- **Securing an embedded system might differ significantly in function of the application and what should be protected**
  - System-level analysis required
- **Security is most often new for customers**
  - They do feel they need to secure their embedded system
  - But they do not know exactly what is required, what it represents
- **Microchip's MPUs feature all what customers need to protect their system, even for the highest security requirements**

Secure Features per Product

	SAM9			SAMA5		
	5- series	G46/M11	CN12	D3	D4	D2
Environmental Monitors	-	-	-	v	v	v
Tampers	-	-	-	-	v	v
Die and Package Security	-	-	-	-	-	v
Secure SRAM	-	-	-	-	v	v
Integrity Check Monitor	-	-	-	-	v	v
External Memory Encryption	-	-	-	-	v	v
Cryptography	v	v	v	v	v	v
TrustZone and CoreTEE	-	-	-	-	v	v
Secure Boot	-	v	v	v	v	v
SAM-BA in Secure Mode	v	v	v	v	v	v
PCI Pre-certification	-	-	-	-	-	v