INTRINSIC ID™

Spring **Security Summit**

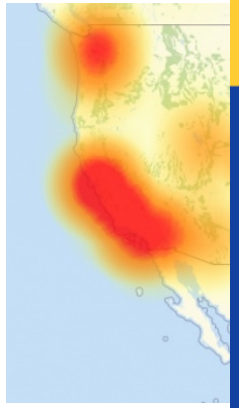
Provisioning secure Identity for Microcontroller based IoT Devices

Mark Schaeffer, Sr. Product Marketing Manager, Security Solutions

Synergy IoT Platform Business Division, Renesas Electronics, Inc.

May 25, 2017

State of the IoT – Internet of “Insecure” Things

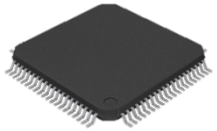


October 2016

Industrial & Medical Sabotage

Hacked Jeep

Elements of a secure embedded platform



Embedded MCU

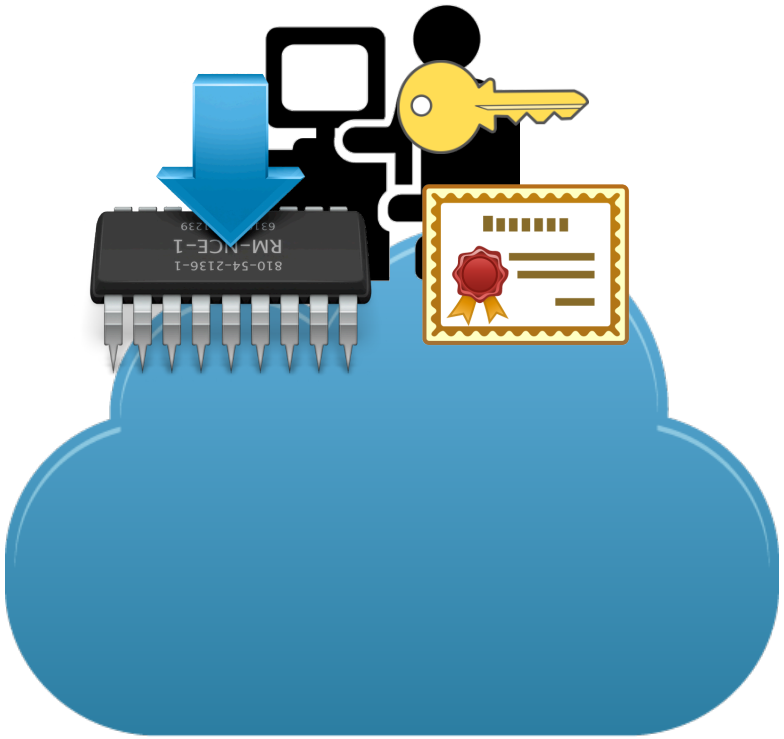
Embedded OS

Secure Memory

Secure Embedded Platform

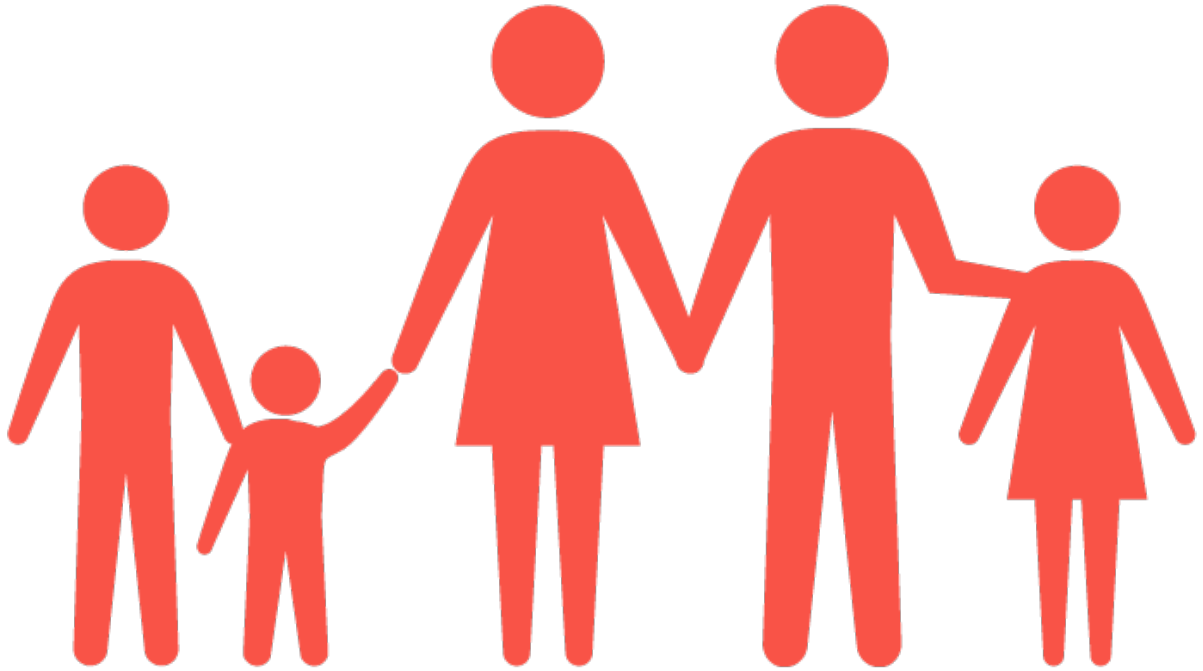
Simple security APIs for non-cryptographers

Communications protocols integrated with security



Security Services for managing identity, keys, firmware

Security technology business objectives



Iot chain-of-trust for solutions

Certificate Services
- Silicon vendor Cert
- OEM Cert
- App/customer/TLS Cert

MCU
- Read protection
- Write Protection / OTP
- HW Crypto acceleration
- Secure Code isolation

Root-of-Trust
- Secure Boot
- Secure Firmware Flash (manufacturing / Updates)
- Unique Identity

Application
- Security APIs
- Key / certificate management
- Protocol support

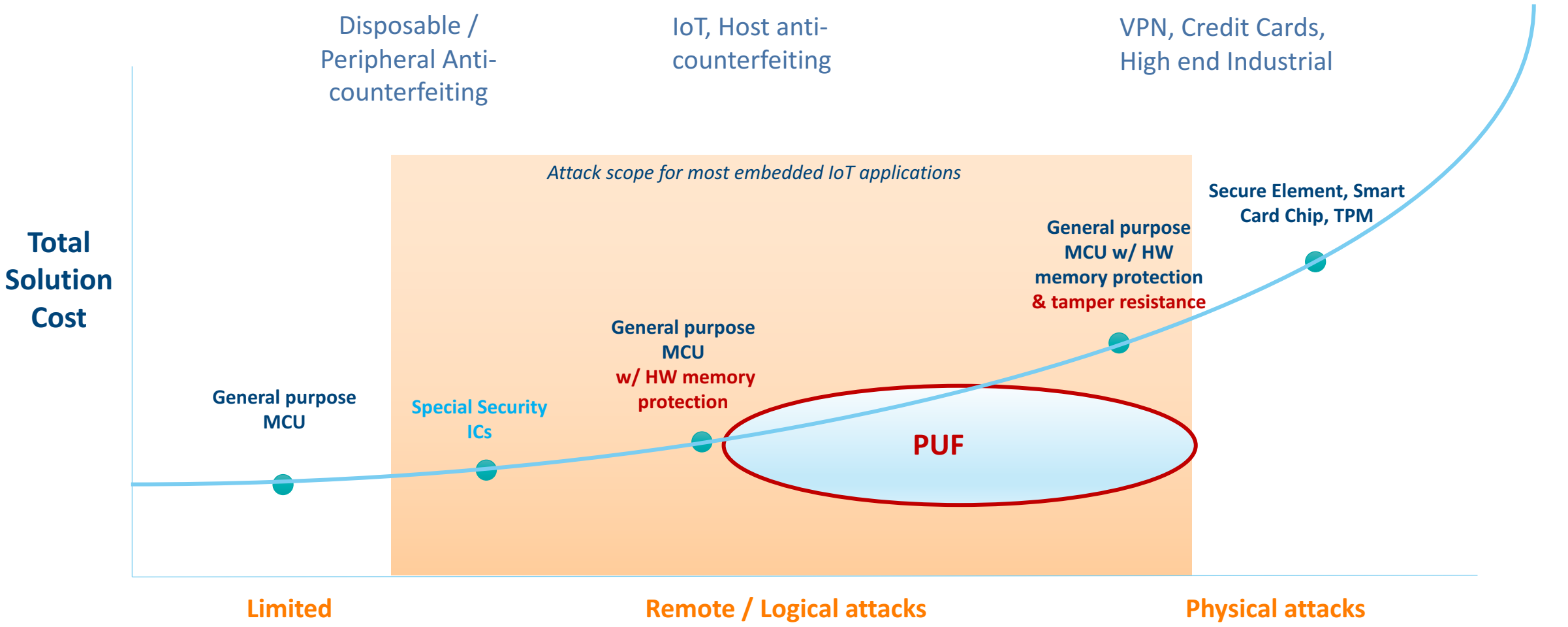
Secure Connectivity
- TLS/SSL
- MQTT
- BTLE
- WiFi
- NFC.

Cloud Services
- Application
- Lifecycle Mgmt
- Security Policy
- IDS/IPS
- SIEM
- Edge Computing

Delivering a Trusted Device To Customer

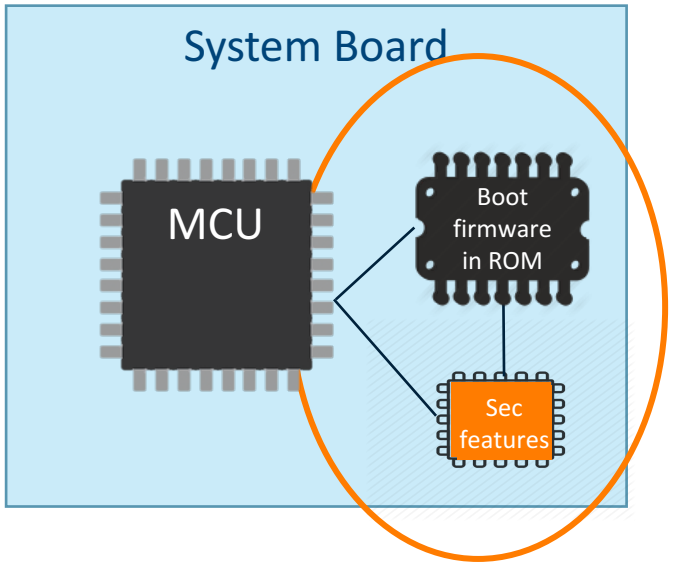
Secure Enrollment and Operations

Spectrum of security features in ICs



Advantage of security in the general purpose MCU

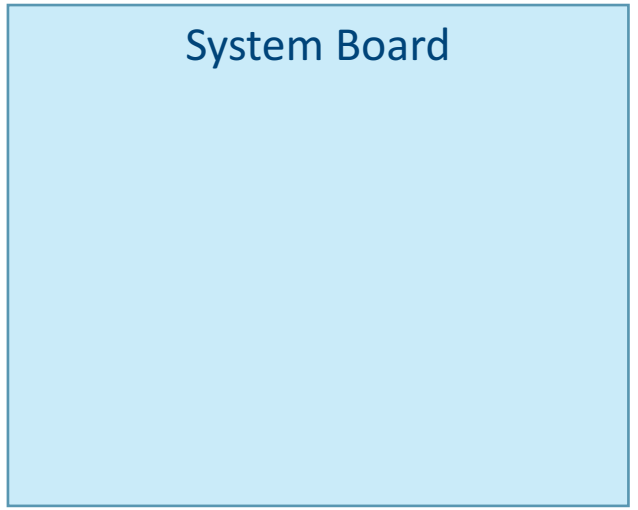
MCU without security



Requires a set of specialized hardware

..and thus robust security is often not implemented due to cost and complexity

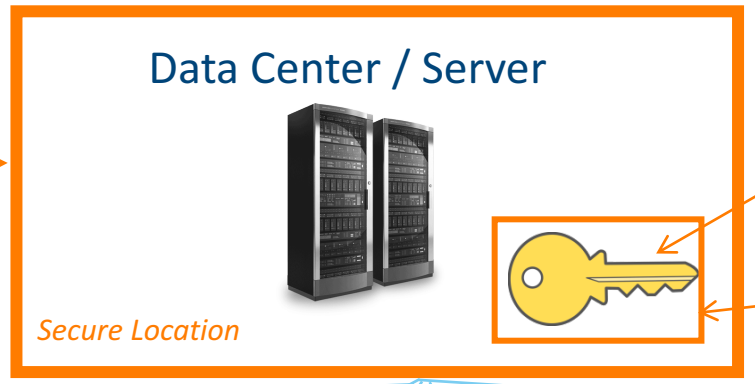
MCU with security



Security is integrated into MCU

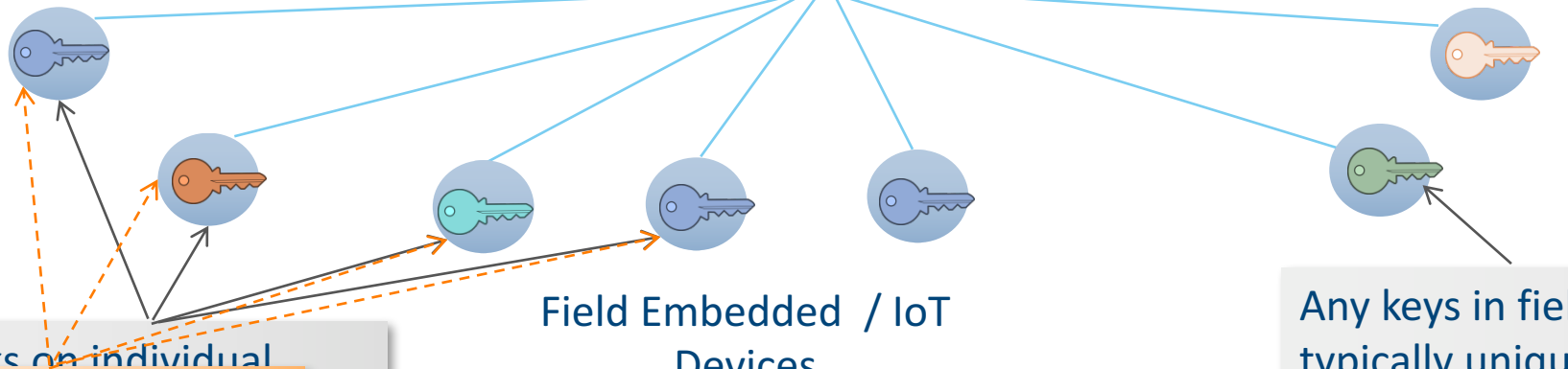
Are physical attacks on keys in scope?

Physical attacks on a single point of failure (Data Center) are IN SCOPE



In modern systems[1], highly sensitive master keys are typically only in a secure location

And are also protected against physical attacks by specialized hardware



Field Embedded / IoT Devices

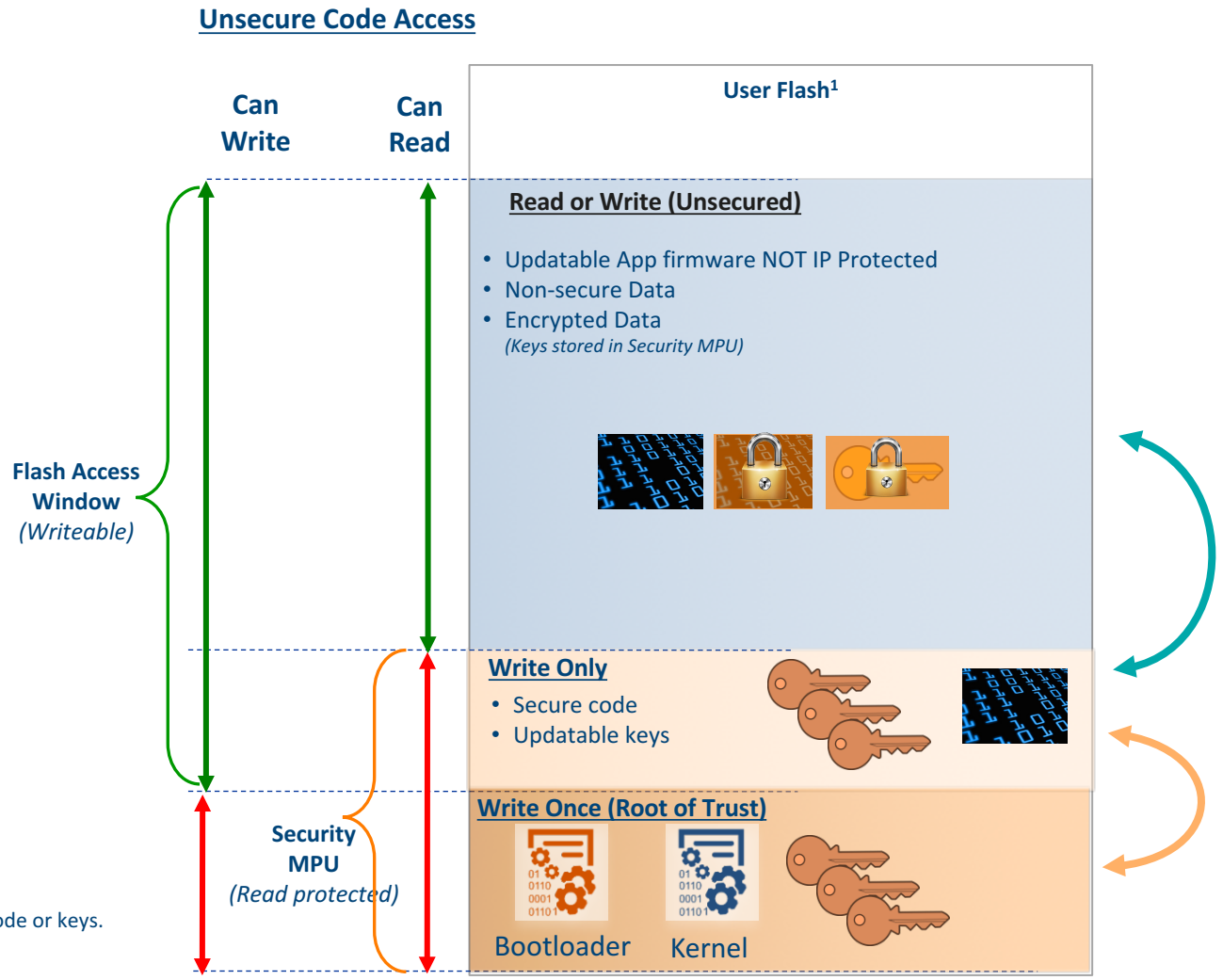
Physical attacks on individual device

Remote software attacks scale

Any keys in field devices are typically unique per device or temporary

[1]The use of modern asymmetric / public key algorithms has reduced the use of secret master keys distributed into the field

Memory segments in a single processor

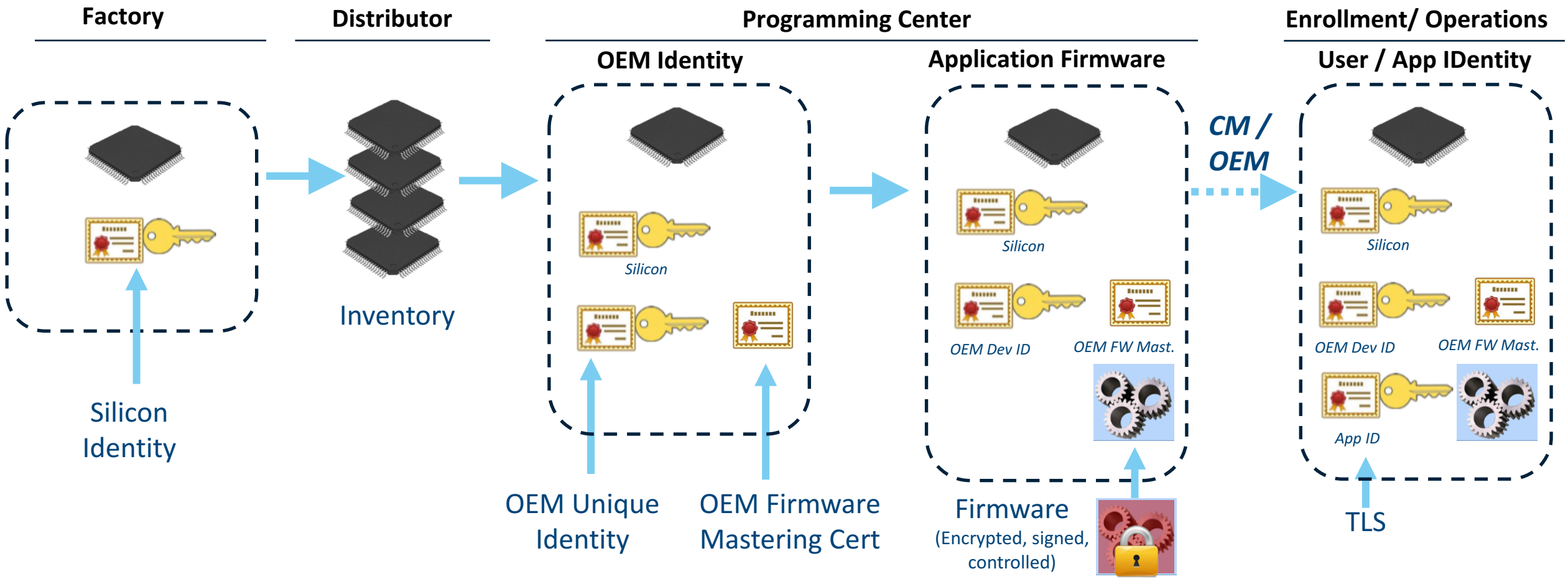


Unsecure Data is accessible by any code

Secure Data is only accessible by Secure Code

[1]The same scheme applies to SRAM, but generally contain any code or keys. Secure SRAM is available to secure flash and vice-versa.

Develop your provision scheme early on…



Advanced Security features & services Providing a chain-of-trust for solutions

Certificate Services
- Renesas Cert
- OEM Cert
- App/customer/TLS Cert

Secure Firmware Flashing Partners
- Secure Manufacturing
- Secure Updates

Bare MCU
- MPU[1] (Read protection)
- FAW[2] (Write protection)
- HW Crypto acceleration

Security Software Modules
- Secure Boot
- Secure Firmware Flash
- Unique Identity

Security Ref Soln

SSP API's, Toolbox Ref Design
- Security API's
- Working application examples with simulated cloud server and Certificate Authority

Security Toolbox

Secure Connectivity
- TLS/SSL
- MQTT
- BTLE, etc.

Cloud Services
- App
- Life Cycle Mgmt
- Security Policy
- IDS/IPS
- SIEM
- Edge Computing

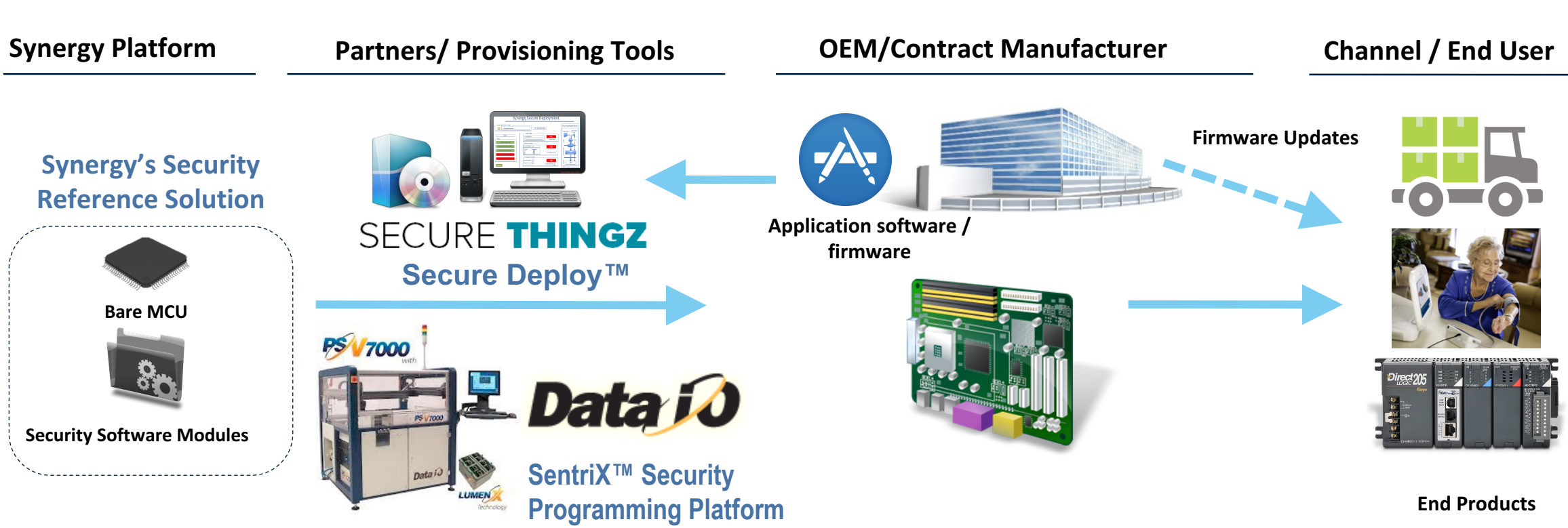
Secure Flash Programming Solution

End-to-End IoT solutions with Ecology Partners

[1]Hardware Memory Protection Unit
[2]Hardware Flash Access Window / One-time-programmable Features

RENESAS Synergy's Security Reference Solution:

A Firmware Flash Programming Solution Overview



The Synergy MCU provides hardware-protected memory segments integrated with an asymmetric cryptographic engine to validate and decrypt the firmware.

Security toolbox

- Reference examples and sample protocols (Medical Device, Industrial Controller)
  - Crypto API
  - Key exchange
  - Salt / Anti-replay
  - Identity with certificates
  - Integrity / Signature
- Certificate creation & usage
  - Key generation
  - Simple sample Certificate Authority
  - Validating Chain-of-trust
  - Public key validation and usage

INTRINSIC ID™

Thank You!