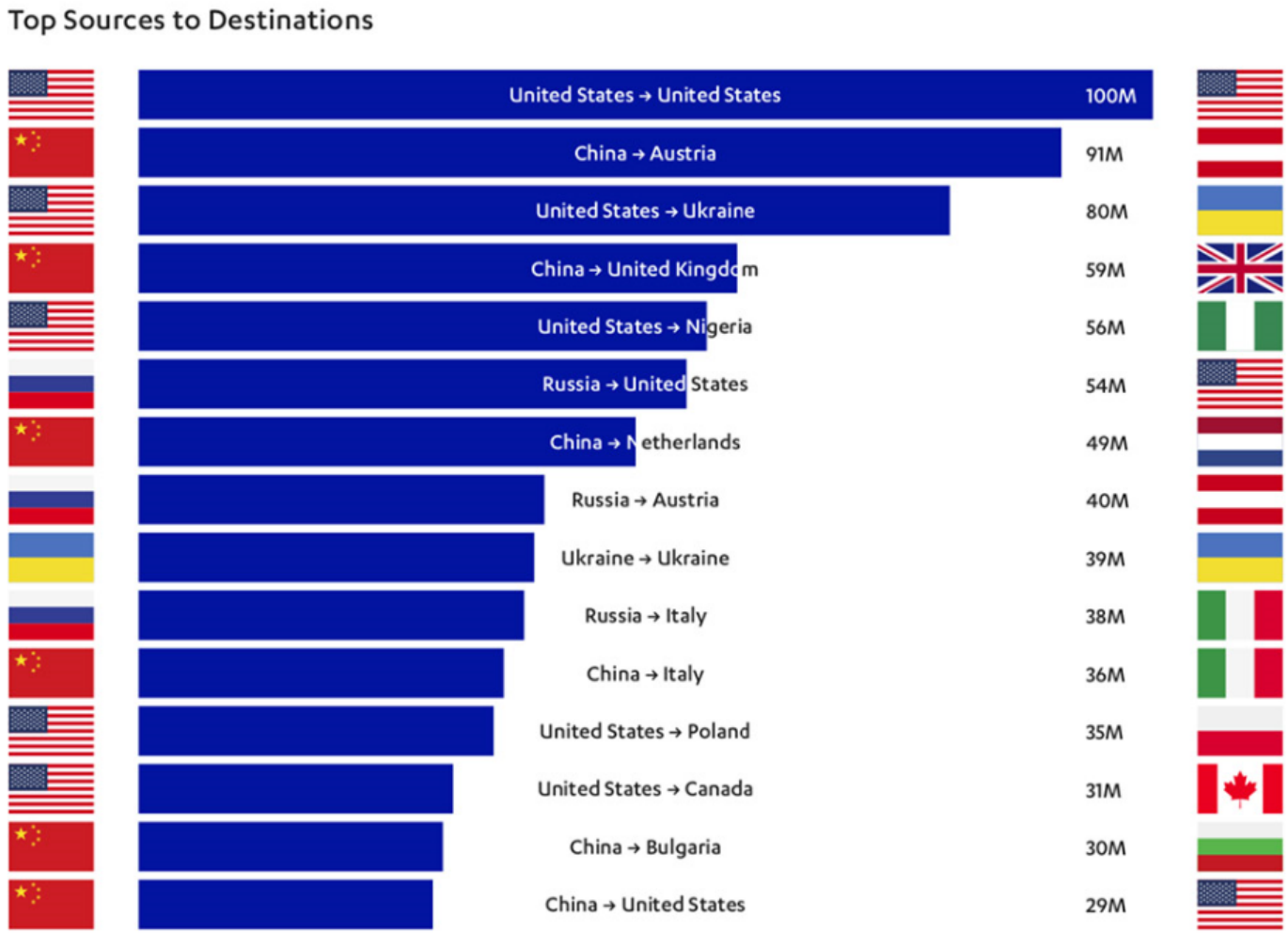
Guidelines to Securing Your Embedded Software IP Using IAR Systems C-Trust

Presenter: Peter Kwak – Principal Embedded Solutions Engineer

MICROCHIP

Threats

Attacks Targeting IoT Devices



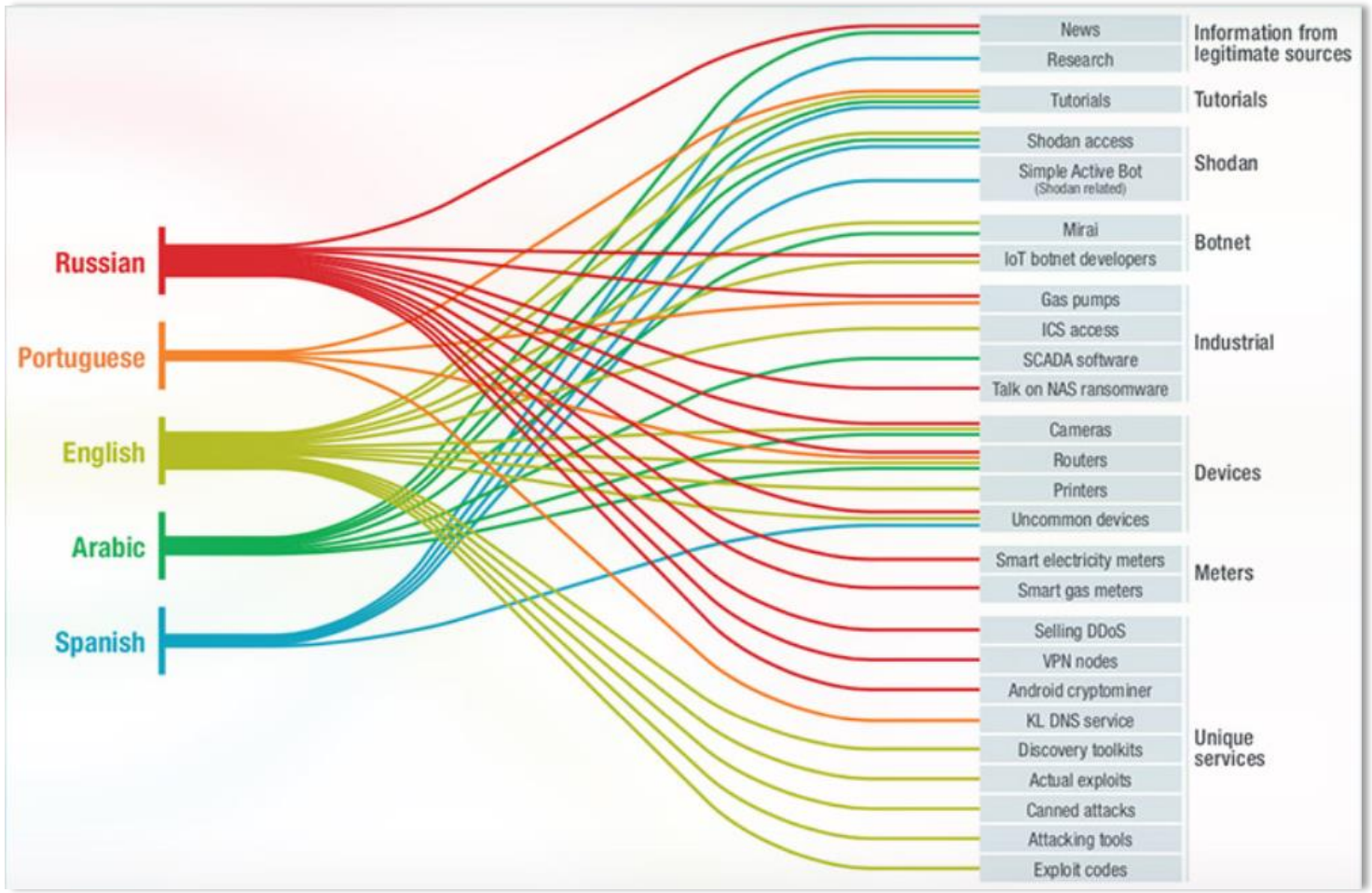
Top countries being targeted, and from which other countries, for the first half of 2019 (Source: F-Secure)

https://www.bankinfosecurity.com/attacks-targeting-iot-devices-windows-smb-surge-a-13082

What is Driving Attacks?

- **Majority of IoT attacks are currently not to subvert IoT infrastructure. Rather they are typical cybercriminals who have evolved into IoT attackers**
  - Discussions about IoT devices typically appeared driven by their being cheap, easy to exploit and monetizable
- **Cybercrime forums traditionally focus on routers, webcams and printers**
- **Abundant tutorials appearing on IIoT and consumer devices**
  - E.g. inner workings of commercial gas pumps, including programmable logic controllers (PLCs) now appearing

Surge in IoT Device Attacks



Visual summary of IoT topics discussed in five underground hacking communities (Source: Trend Micro)

https://www.bankinfosecurity.com/attacks-targeting-iot-devices-windows-smb-surge-a-13082

Legislation

Evolving Legislation

- **Legislation is being driven by the industry's lack of ability to self-regulate with best practice. Hence legislation offers a "least bad" solution.**
- **Current guidance is in the form of best practice**
  - Legislation to give best practice "teeth" will follow
  - Many retailers and industry stakeholders pushing for stronger legal frameworks
  - Punishments inline with GDPR regulations are expected in the 2021+ timeframe

- **Guiding principals for legislation**
  - Reducing burden on consumers and supply chain by standardizing expectations
  - Transparency to enable informed choices
  - Measurability to enable comparison and judgement
  - Facilitation dialog and sharing ideas
  - Resilience in design to limit damage and exposure when systems are compromised

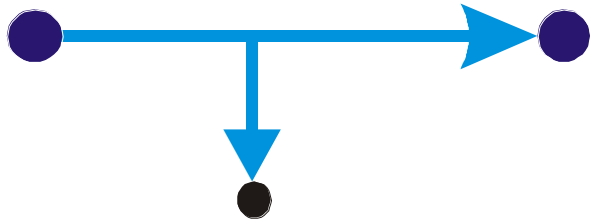
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/686089/Secure_by_Design_Report_.pdf

Security Tools

Cryptography

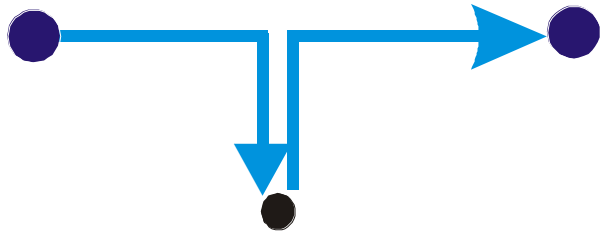
- **Using cryptography ensures ….**

Confidentiality



Sniffing is not possible

Integrity

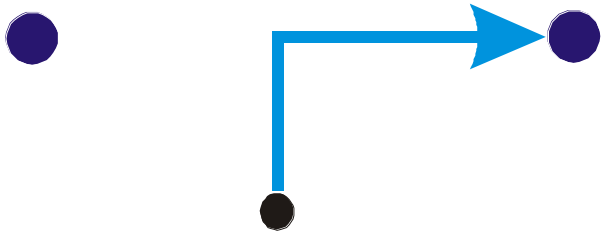


Protects data from modification

Nonrepudiation

The source of information is well known

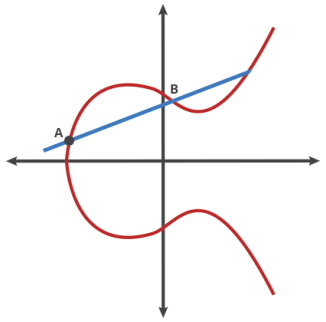
Authenticity

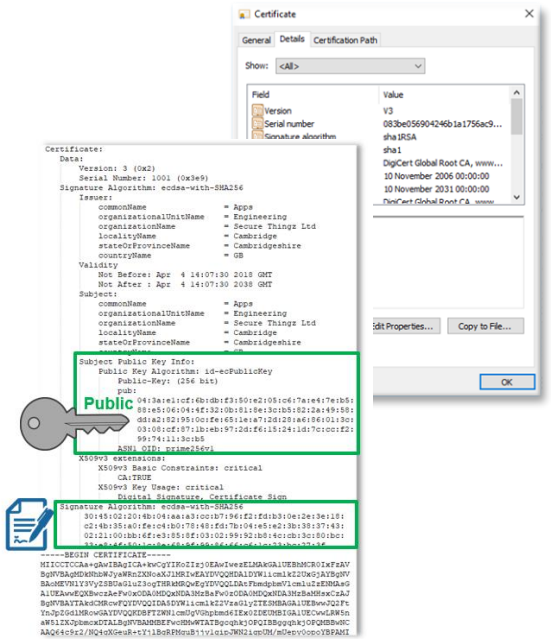


Wrong data is recognized

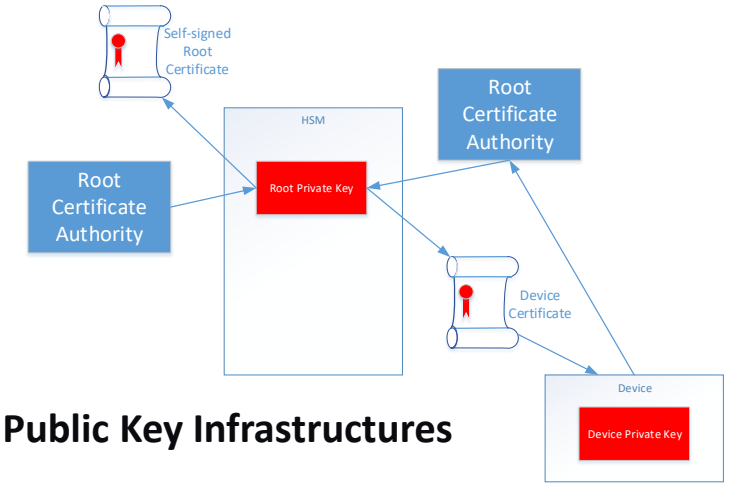
Cryptography

- **However….it is complex to implement.**

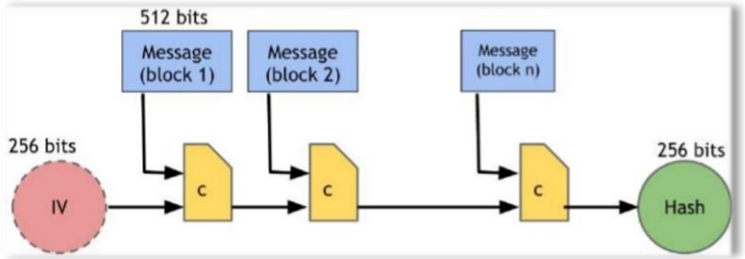




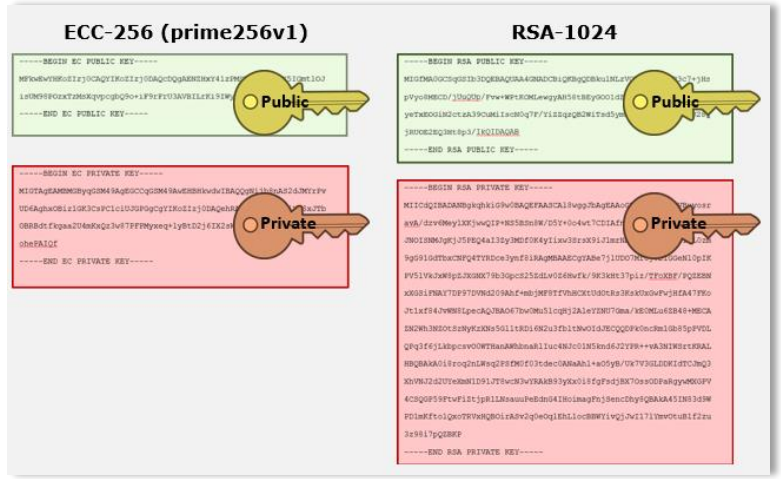
Digital Certificates



Public Key Infrastructures



Hash Algorithm



Elliptic Curve & RSA keys

Hardware

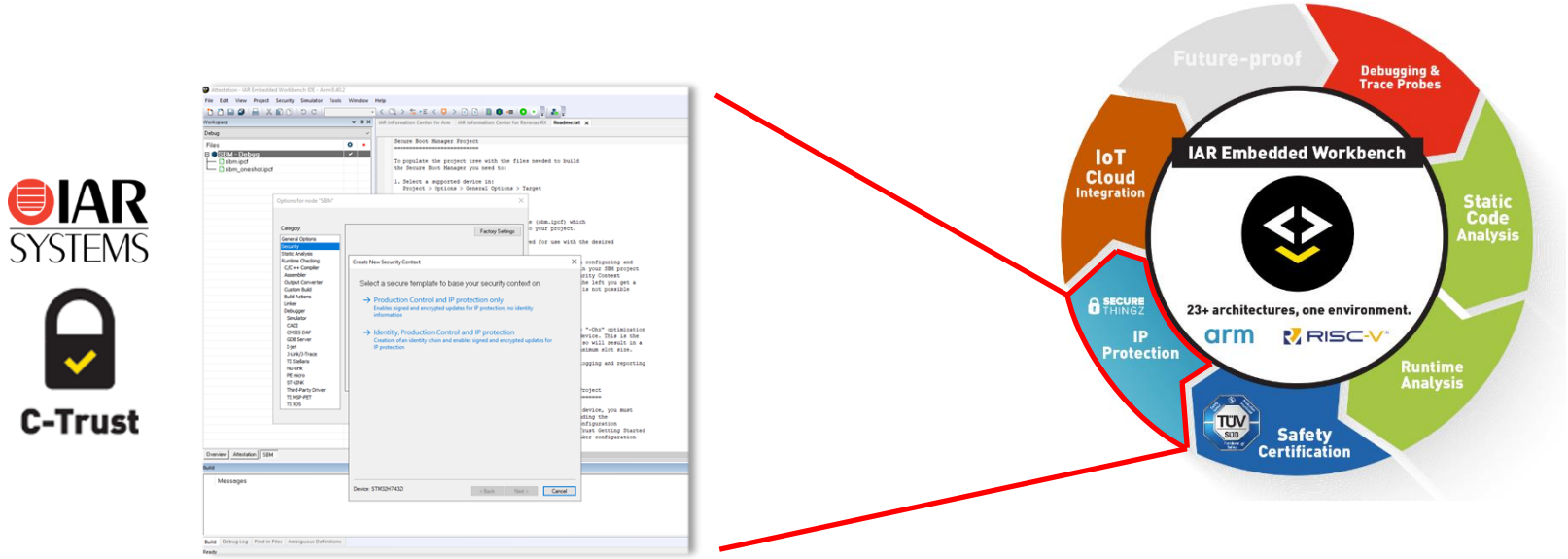
- **Latest microcontrollers now include security features**
  - Arm® Cortex®-M23 core (with TrustZone®)
  - Secure Boot
  - Crypto Accelerators
  - AES, SHA, GCM
  - Secure Debug
  - True Random Number Generators

In Summary…

- Complex mathematical techniques which are available to ensure information is encrypted
- Public Key Infrastructures that are in place and ensure secure electronic transfer of information can take place over networks
- Semiconductor devices that are available with peripherals and features that allow development of secure products which are connected to networks

Problem Statement

- **Is there a simple tool available that brings all this complex technology together and allows customers to secure their connected products and IP with minimal distraction from their core competencies?**



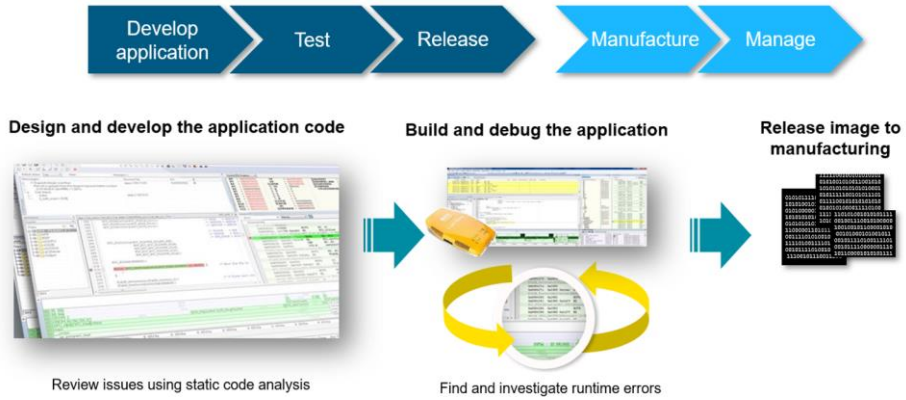
C-Trust

What is C-Trust?

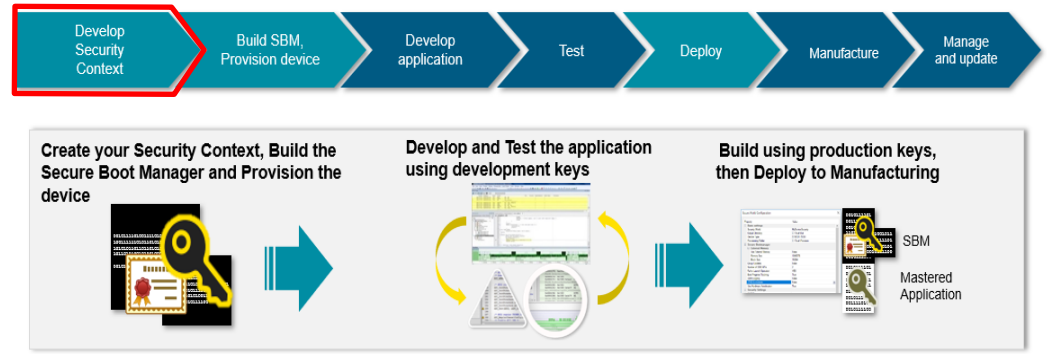
- **Complete security development environment extension to IAR Embedded Workbench toolchain. It includes:**
  - Security wizard for easy configuration of the projects' Security Context
    - Auto key and certificate generation (Root of Trust)
    - Secure Boot Manager generation/configuration
    - Application update policy configuration
    - Auto device memory layout and protection configuration
    - Export to production package (OVA and manufacturing)
  - C-STAT static analysis tool

Security Workflow

Common development workflow



Security development workflow

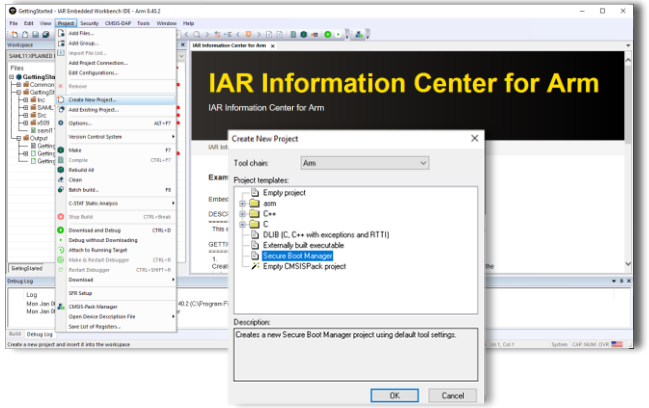


Security measures must be implemented at the start of the design cycle.

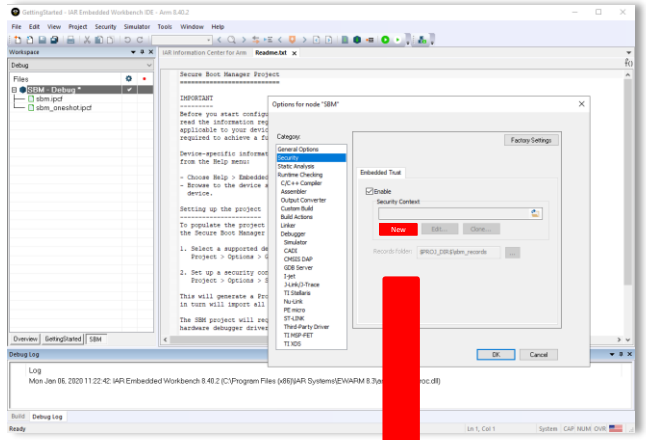
Security Measures = Security Context

Security Context Wizard

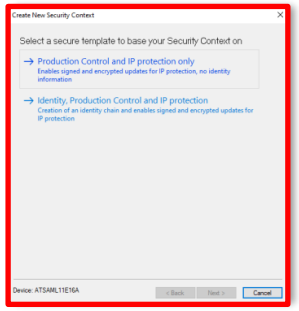
Common Development Workflow



Security Development Workflow

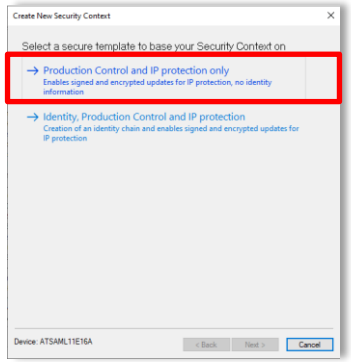


Security Context Wizard

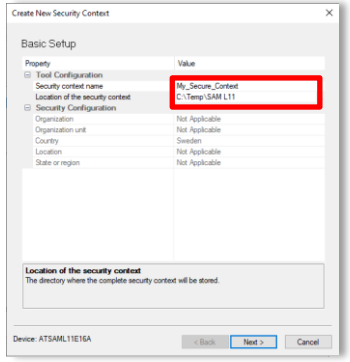


Wizard Flow

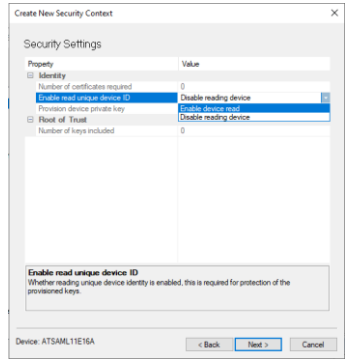
Select Template



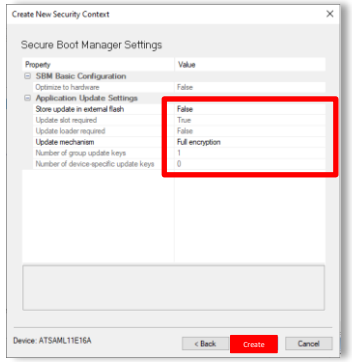
Context Name & Location



Select Unique Device ID Option

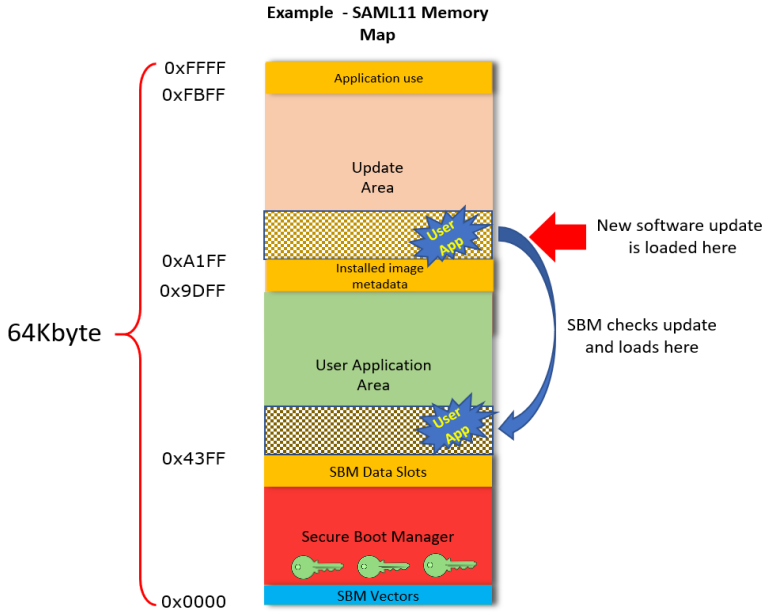


Configure Boot Manager



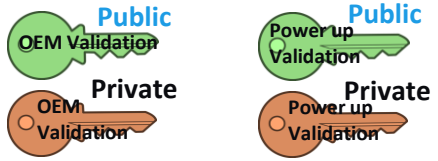
What Did I Create?

New Memory Map



ECC-256 Cryptographic Key Pairs

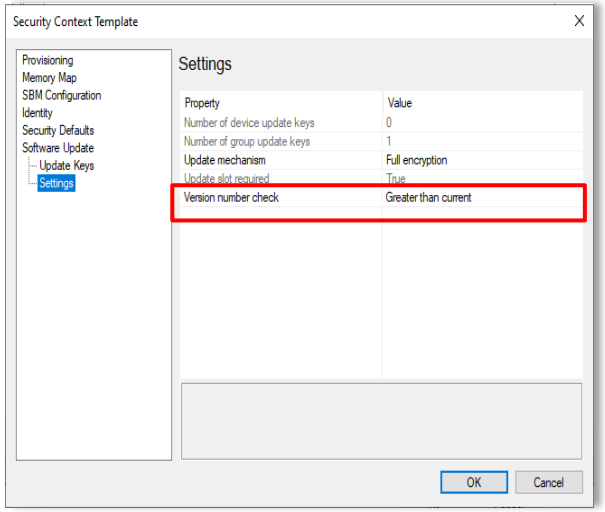
Software update validation keys



Validates software update owner (OEM)

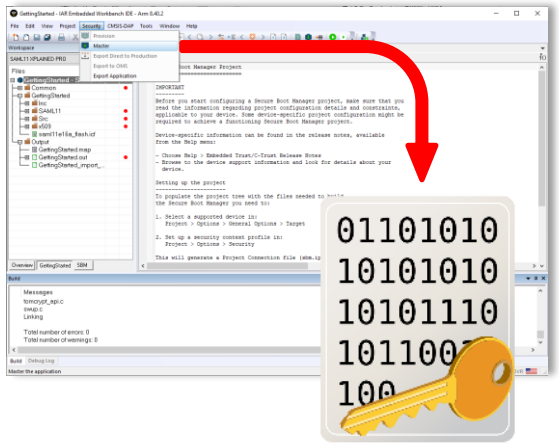
Validates software update integrity (used during every power up)

Automatic Update Policy



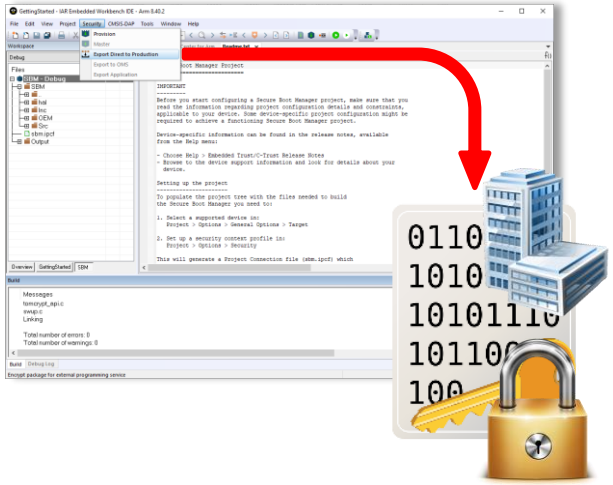
How Do I Use It?

Create New Version and Master



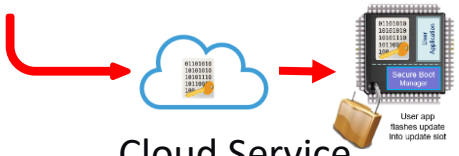
Generate Encrypted User Application

Create Secure Production Package for Manufacture



Sign & Authorize Manufacturing

Send to Manufacture



Cloud Service

How Do I Get C-Trust?

- **C-Trust works as an extension to IAR Embedded Workbench – it's easy to add to an existing or new license!**

→**Get in touch with your closest IAR Systems office at iar.com/contact to get to explore this possibility.**

- **Read more about the tool at iar.com/ctrust**

Summary

- **C-Trust**
  - Greatly simplifies security
  - Uses the latest cryptographic techniques to secure your IP
  - Uses security hardware functions provided by SAM L11
  - Protects against over production and cloning
  - Simplifies software update process
  - Auto generates Secure Boot Manager to manage updates and update policy

Thank You