Designing Secure IoT Products

Nordic Tech Webinar

Tiago Monte / Developer Marketing Manager

April 2023

Today's hosts

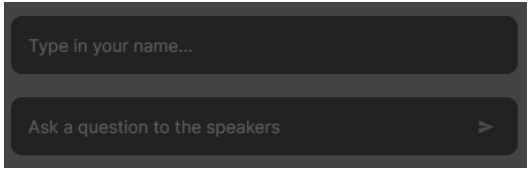
Tiago Monte

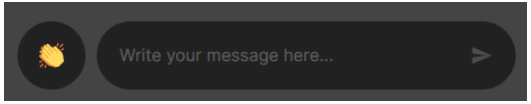
Developer Marketing Manager

NORDIC SEMICONDUCTOR

Practicalities

- Duration: 45 min presentation, 15 min Q&A
- Questions are encouraged!
  - Please type questions on the top of the right sidebar
  - All questions are anonymous
  - Try to keep them relevant to the topic
  - We will answer them toward the end
- The chat on the bottom of the right sidebar is not anonymous, and it should not be used for questions.
- Go to DevZone if you have more questions
- A recording of the webinar will be available together with the presentation at webinars.nordicsemi.com/on-demand





{ DevZone

Agenda

Why — The importance of security

How — The approach to security

What — PSA Certified IoT Security Framework

Why?

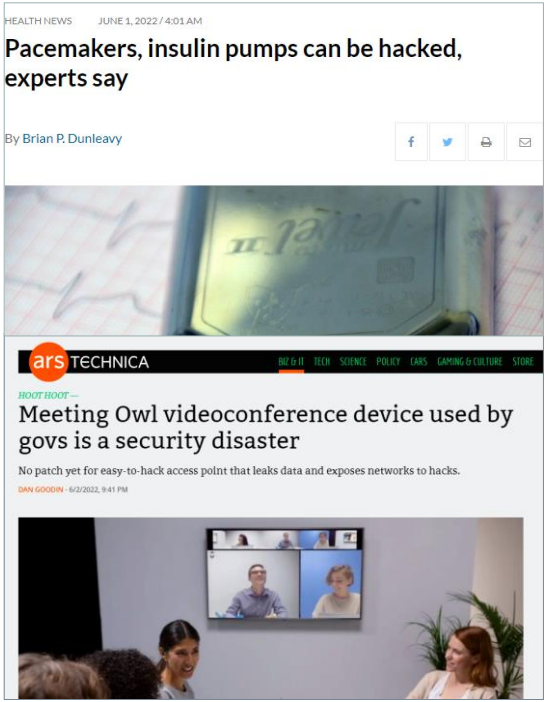
The importance of security

Embedded security is nothing new

SIM and Payment Cards have been getting things right for 20+ years

But still, many get it wrong…

- Security incidents are wide-ranging, from data leakage to potential loss of life
- Consumer confidence can decrease for the entire product category of affected devices
- The more devices come online, the larger the attack surface, and the higher the risk



Security costs, but insecurity costs more

- First half of 2021 saw 1.5 billion attacks on smart/IoT devices
- By 2025 the impact of cybercrime is predicted to reach $10.5 trillion
- IoT-related attacks account for a significant portion of that total

Source: PSA Certified 2022 Security Report (link)

Regulations, Standards, Certifications

- **Regulations:** mandatory and enforceable
  - Developed by governments



Regulations may rely on a **standard**, which defines the requirements.

- **Standards:** optional, a choice, many of them
  - Created by standardisation bodies:

ETSI World Class Standards

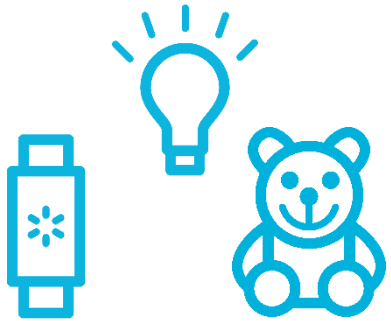
NIST National Institute of Standards and Technology

Standards may rely on external or self-**certification**, as evidence of compliance

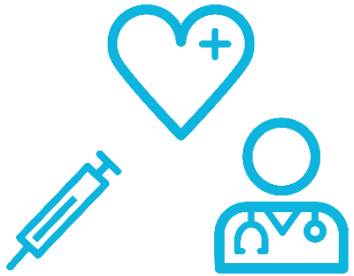
- **Certifications:** optional, many of them
  - Awarded by private organisations (usually)

psacertified™

Varied regulation landscape



Consumer IoT



Medical

For many product categories – there are no mandatory security requirements

Regulators are catching up

Product manufacturers will soon be **required** to meet baseline Product Security requirements for market access – i.e the right to sell their products.

Globally fragmented process -> with many common requirements.

Radio Equipment Directive – Delegated Act Article 3
EU Cybersecurity Act
EU Cyber resilience Act

Product Security and Telecommunications Infrastructure Act

Executive Order on Improving the Nations Cybersecurity:
Cybersecurity Labelling for Consumers: IoT

Singapore Cybersecurity Labelling Scheme
Voluntary

Finnish Cybersecurity Label
Voluntary

Australian Cybersecurity Label
Proposed

How?

The approach to security

No product is 100% secure

- With enough:
  - Time
  - Money
  - Motivation

Your system can be broken

Security is a balance …

Cost of protection

- Memory
- Data consumption
- Power consumption
- Secure production

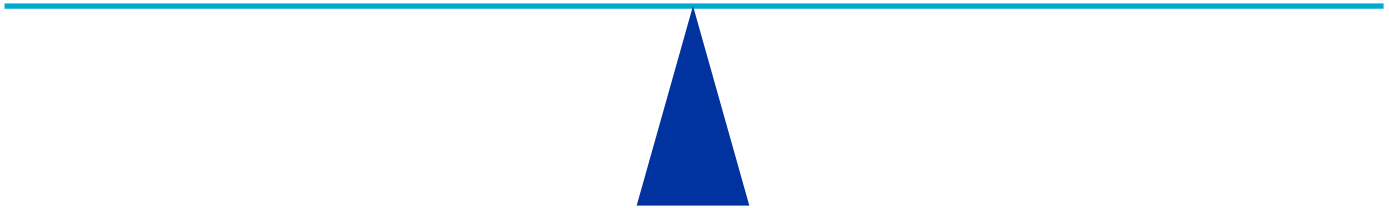
Risk

=

Impact

x

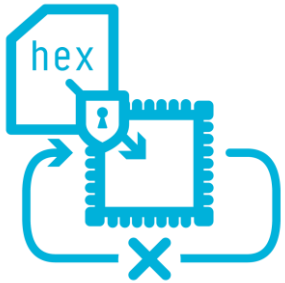
Probability



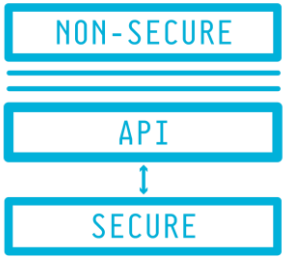
Less security

More security

… with a few simple objectives …



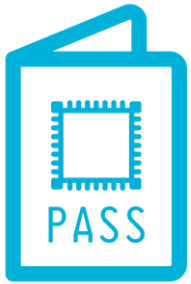
Secure boot and secure update with anti-rollback



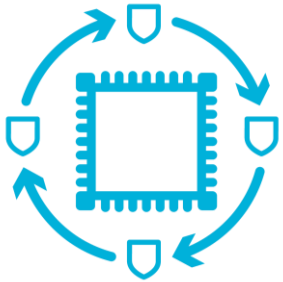
Isolation between secure and non-secure environments

Secure storage

… every product should meet

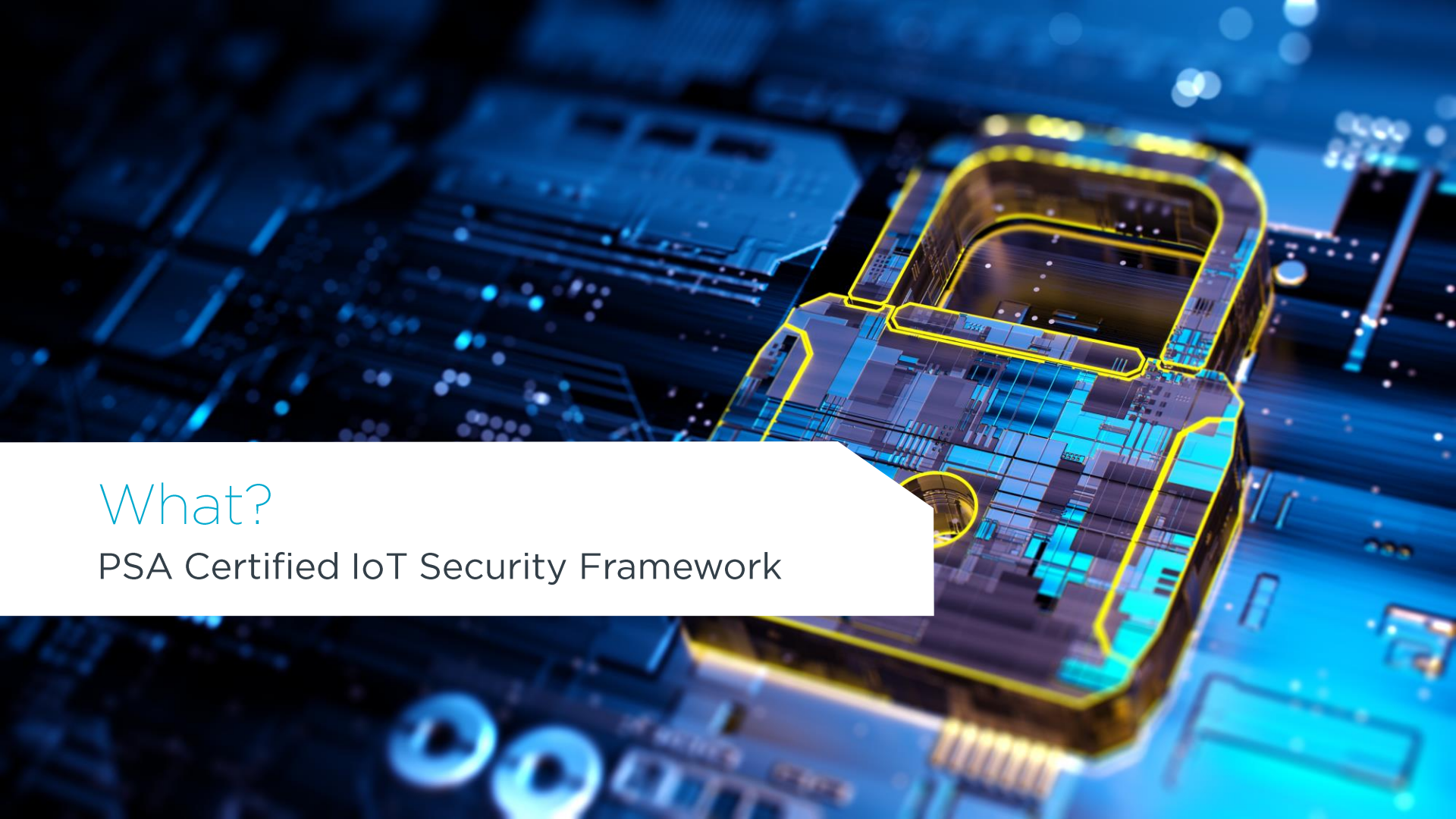


Attestation and unique identification



Security Lifecycle

Cryptographic services



What?

PSA Certified IoT Security Framework

Arm Platform Security Architecture (PSA)

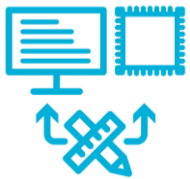
A framework for Secure Product Development

- Platform Security Architecture is a framework to develop a product that integrates the best practices in IoT security.
- It covers design, implementation, and evaluation:

Analyze

Threat models & security analysis

Architect



Hardware & firmware specifications

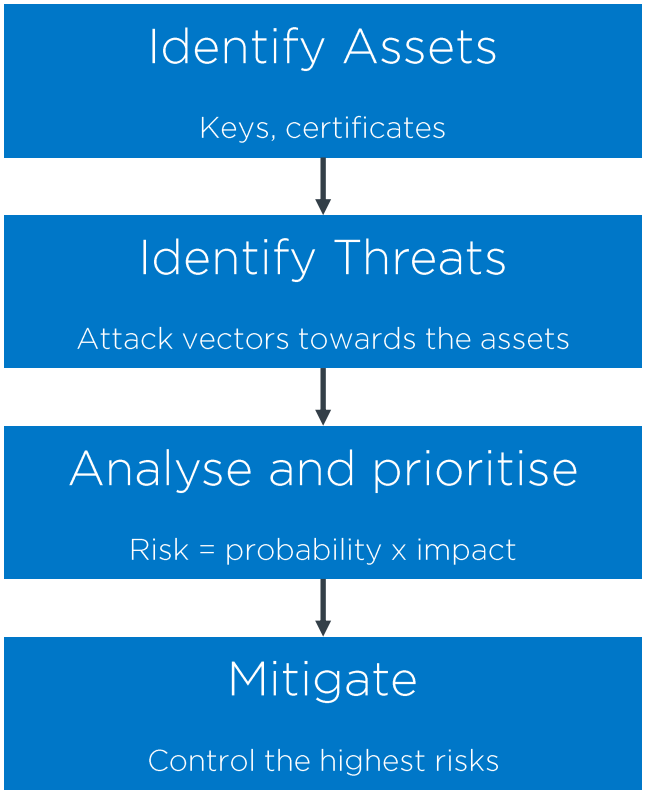
Implement

Firmware source code

Certify

Independently tested

Analyze - Threat modeling



Threat Model and Security Analysis examples available from PSA Certified:

- Asset tracker
- Smart water meter
- Network camera

Search “threat model” on psacertified.org

Analyze - Threat modeling example

Asset	Security Requirement	Threat	Entry point of Threat	Impact of vulnerability	Severity (CVSS Rating)	Mitigation
Firmware	Integrity	Tamper	Malware, bug, mass storage access, JTAG, network update	Install malware	Critical: 9	Secure boot
		Escalation of privilege		Launch DDoS		Enforce principal of least privilege
Credentials	Confidentiality	Disclosure (Tamper)	Malware, bug, mass storage, JTAG, network	Device usurpation	High: 8.7	Secure storage in Trusted Execution Environment (TEE)
		Escalation of privelege		Modify firmware and install malware		
Logs	Integrity	Tamper	Malware, bug, mass storage	Supress critical alerts and events	Medium: 4.9	Enforce access control and principle of least privilege
	Confidentiality	Impersonation		Gain access to system info		Secure storage in TEE

Source: Asset Tracker from PSA Certified threat model training (link)

Architect - HW & FW specifications

Identify **hardware** and **firmware** which can support the needs of the threat model:

-> Hardware Cryptographic Accelerator, Secure Storage, Isolation

Hardware

nRF9160, nRF5340 and nRF52840

PSA Certified SoC and SiP

Certified to meet security best-practice requirements

Firmware

nRF Connect SDK

Flexible, enabling the right security to be applied for your application

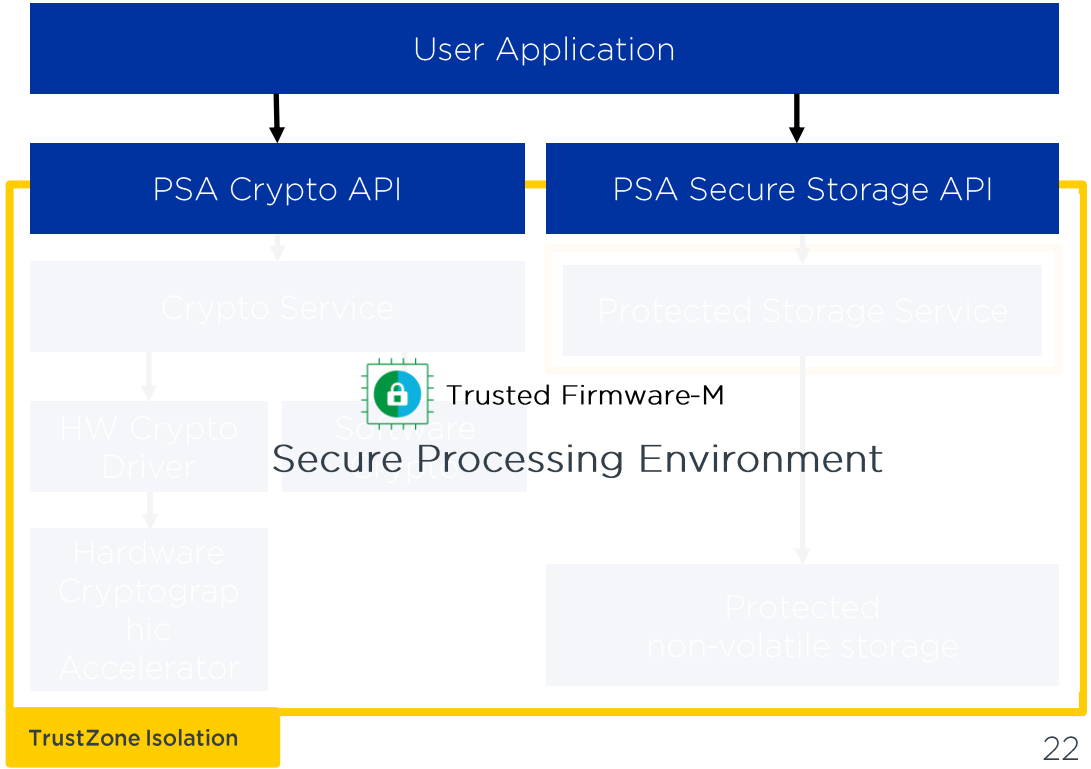
Provides Trusted Firmware-M, a reference implementation of Secure Processing Environment

Implement – Firmware

PSA APIs

Standardised interface towards security services.

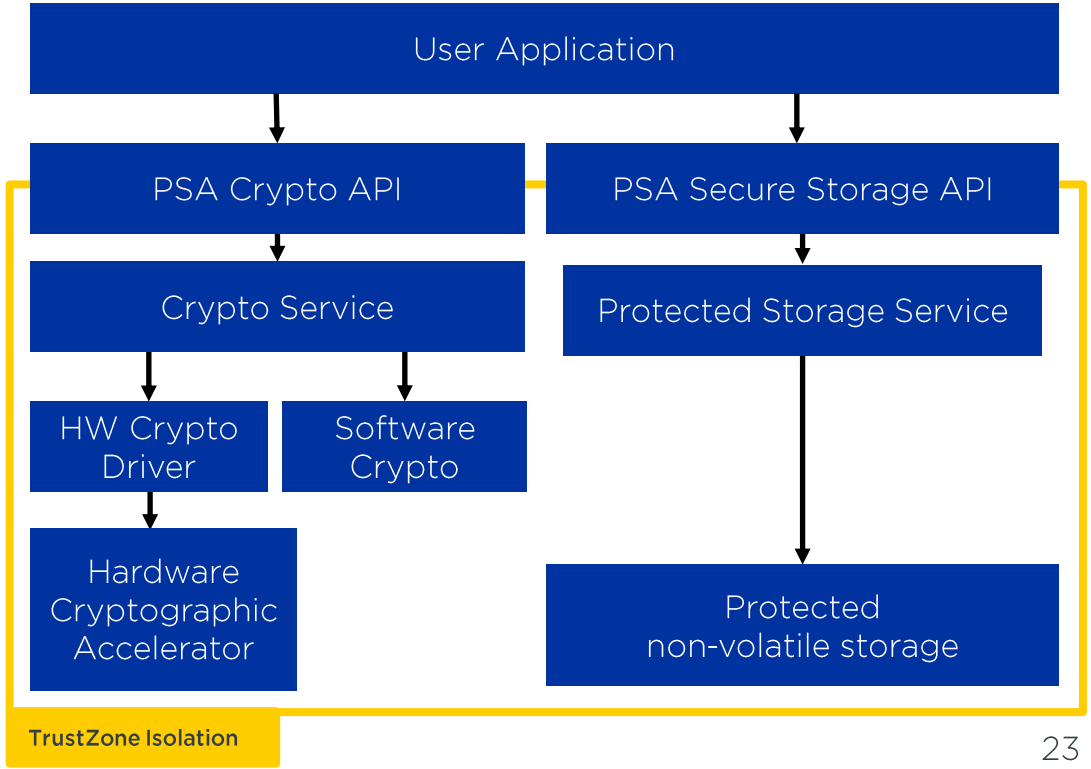
- Enhanced security - enabling devices to meet industry-standard security
- Implementation agnostic - Abstracts hardware/software implementation differences between platforms.
- Flexible and scalable – Supports a variety of use cases, from simple to complex systems
- Future proof – PSA APIs are designed to be updated as security threats evolve



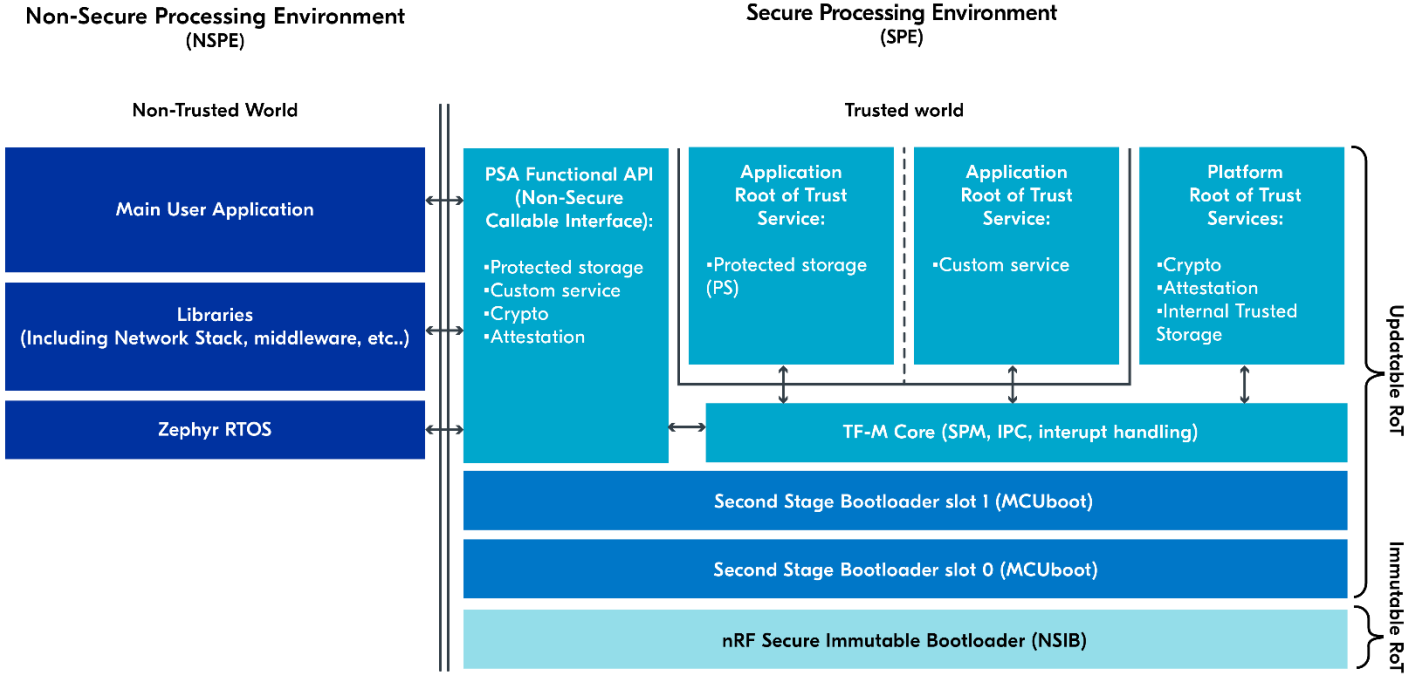
Implement – Firmware

Trusted Firmware-M (TF-M)

- TF-M is a secure processing environment
- Runs on TrustZone enabled hardware
- Isolates critical security services and data from non-secure user application
- Provides PSA Root of Trust and secure services implementation, such as:
  - Cryptographic services
  - Secure storage
  - Attestation service

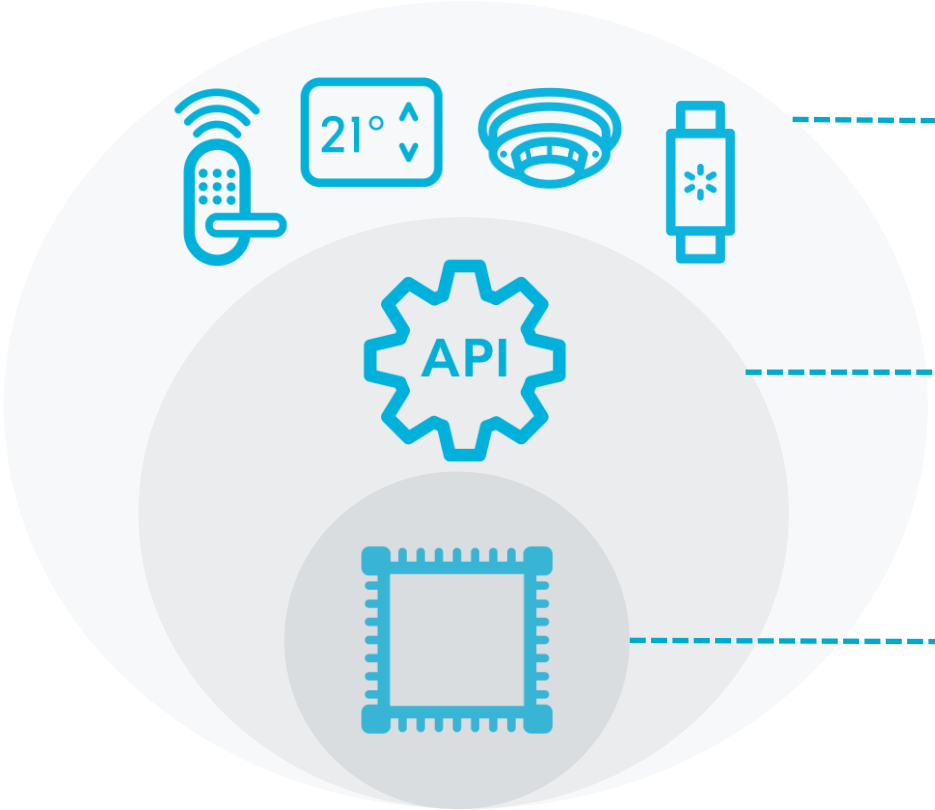


TF-M in nRF Connect SDK



- User application
- TF-M
- MCUboot
- NSIB
- Isolation Level 1
- Isolation Level 2
- Isolation Level 3

Certify – From silicon to device



Device

- Consumes silicon and system software
- Aligns with standards/regulations

System software (e.g. RTOS)

- Leverages PSA-RoT security functions
- Eligible for PSA-L1 certification

Silicon

- Implements PSA-RoT (Root of Trust)
- Evaluated on three levels of security

Certify – Independently tested

- PSA Certified offers security certification for silicon, system software and end devices.
- Independent lab evaluation.
- Global certification programme, aligned with:
  - Existing IoT security standards:
    - ETSI EN 303645
    - NIST 8259A
  - Emerging eco-systems and labelling programmes

PSA Certified Silicon and Root of Trust

nRF9160 SERIES

nRF9160

Cellular SiP

LTE-M and NB-IoT

nRF53 SERIES

nRF5340

Dual-core

Bluetooth LE

and 15.4 SoC

nRF52 SERIES

nRF52840

Bluetooth LE

and 15.4 SoC

psacertified™
level one

PSA Certified Level 1

Assurance of silicon implementing a hardware RoT

Independently reviewed by security evaluation lab and certification body

Aligns with latest baseline cybersecurity requirements and regulations with mapping to:
ETSI EN 303645 and NIST 8259A

Prioritize security

Nordic continues to invest in product security in its hardware, software and services.

Security should be considered early in your design.

nordicsemi.com/security

Learn more from Nordic – be self-driven

devzone.nordicsemi.com

academy.nordicsemi.com

webinars.nordicsemi.com

Thank you

Get started with security today

nRF Connect SDK - security