



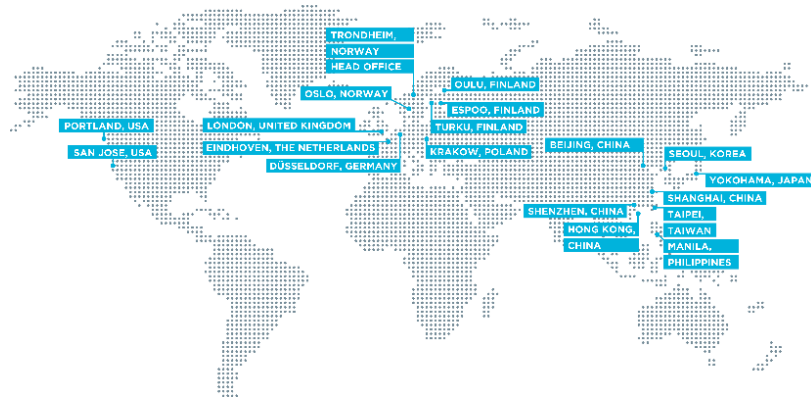
Preparing for an uncertain regulatory future in IoT security

Embedded Conference Finland

Nordic Semiconductor

6 September 2022

Nordic Semiconductor at a glance



- Founded in 1982, Headquartered in Norway
- 1300+ employees
- R&D in Norway, Finland, Poland, Sweden, UK, India and the US
- Publicly listed in Norway under the ticker OBX:NOD
- Key partners: TSMC, AMKOR, ASE

- Fabless semiconductor company - specialized in ULP wireless connectivity and embedded processing for IoT
- Leading short range connectivity market with Bluetooth LE and Thread/Zigbee
- Low power cellular IoT with LTE-M and NB-IoT technologies
- Expanding into Wi-Fi 6 IoT market with the nRF70 Series

Nordic Semiconductor products

Short Range



Bluetooth Low Energy

Matter

Thread/Zigbee

Proprietary

Cellular



LTE-M

NB-IoT

GPS

Wi-Fi



Wi-Fi 6

2.4GHz +5GHz

PMIC

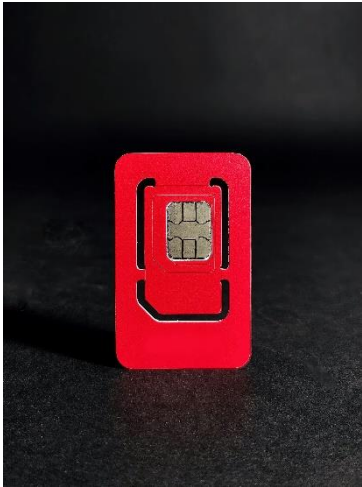


Li-Ion charger

LDO

DC/DC buck
converter

Embedded security is nothing new



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


But many still get it wrong...


CNET Your guide to a better future

Home » Home Security

It's Time to Treat Your Home Security Cameras as Compromised

Commentary: Wyze has taught us a valuable lesson.

 **David Priest** ^{IP}
April 5, 2022 6:00 a.m. PT 5 min read



The Wyze Cam v1 had vulnerabilities that were never patched and that Wyze didn't disclose to customers until three years after it was notified of them.
Chris Monroe/CNET

At the end of March, BitDefender, a leading cybersecurity research firm, published a [damning report about Wyze \(PDF\)](#), one of the leading security brands on the market. The charge: That the manufacturer was notified of a vulnerability that allowed, among other things, unauthorized access to stored footage in its wildly popular Wyze Cam v1 -

ars TECHNICA BUILD TECH SCIENCE POLICY GEAR GAMING CULTURE STORE

HOOT HOOT —

Meeting Owl videoconference device used by govts is a security disaster

No patch yet for easy-to-hack access point that leaks data and exposes networks to hacks.

DAN GOODIN - 6/27/2022, 9:41 PM



Enlarge

128

A recently published security analysis has concluded the devices pose an unacceptable risk to the networks they connect to and the personal information of those who register and administer them. The litany of weaknesses includes:

- The exposure of names, email addresses, IP addresses, and geographic locations of all Meeting Owl Pro users in an online database that can be accessed by anyone with knowledge of how the system works. This data can be exploited to map network topologies or socially engineer or dox employees.
- The device provides anyone with access to it with the [Interprocess communication channel](#), or IPC, it uses to interact with other devices on the network. This information can be exploited by malicious

No product is 100% secure

- With enough:
 - Time
 - Money
 - Motivation

Your system can be broken

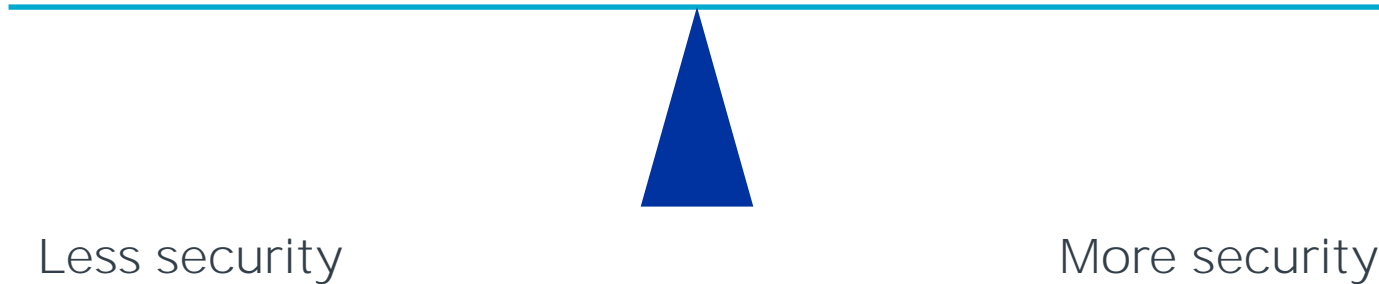
Security is a balance

Cost of protection

- Memory
- Data consumption
- Power consumption
- Secure production

Risk of attack

$$\begin{aligned} &= \\ &\text{Impact} \\ &\times \\ &\text{Probability} \end{aligned}$$



How to ensure that everyone gets the basics right

Regulations, standards and certifications

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:



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



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



Varied regulation landscape



For many product categories – there are no mandatory security requirements

Governments and regulators are catching up

Product manufacturers will soon be **required** to consider Product Security for market access - i.e the right to sell their products

This is a fragmented process - different approaches - different requirements



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



Singapore Cybersecurity Labelling Scheme
Voluntary



Product Security and Telecommunications Infrastructure Bill



Finnish Cybersecurity Label
Voluntary



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



Australian Cybersecurity Label
Proposed

How we will prepare for globally fragmented security requirements



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 analyses

Architect




Hardware & firmware
architect specifications

Implement



Firmware
source code

Certify



Independently
tested

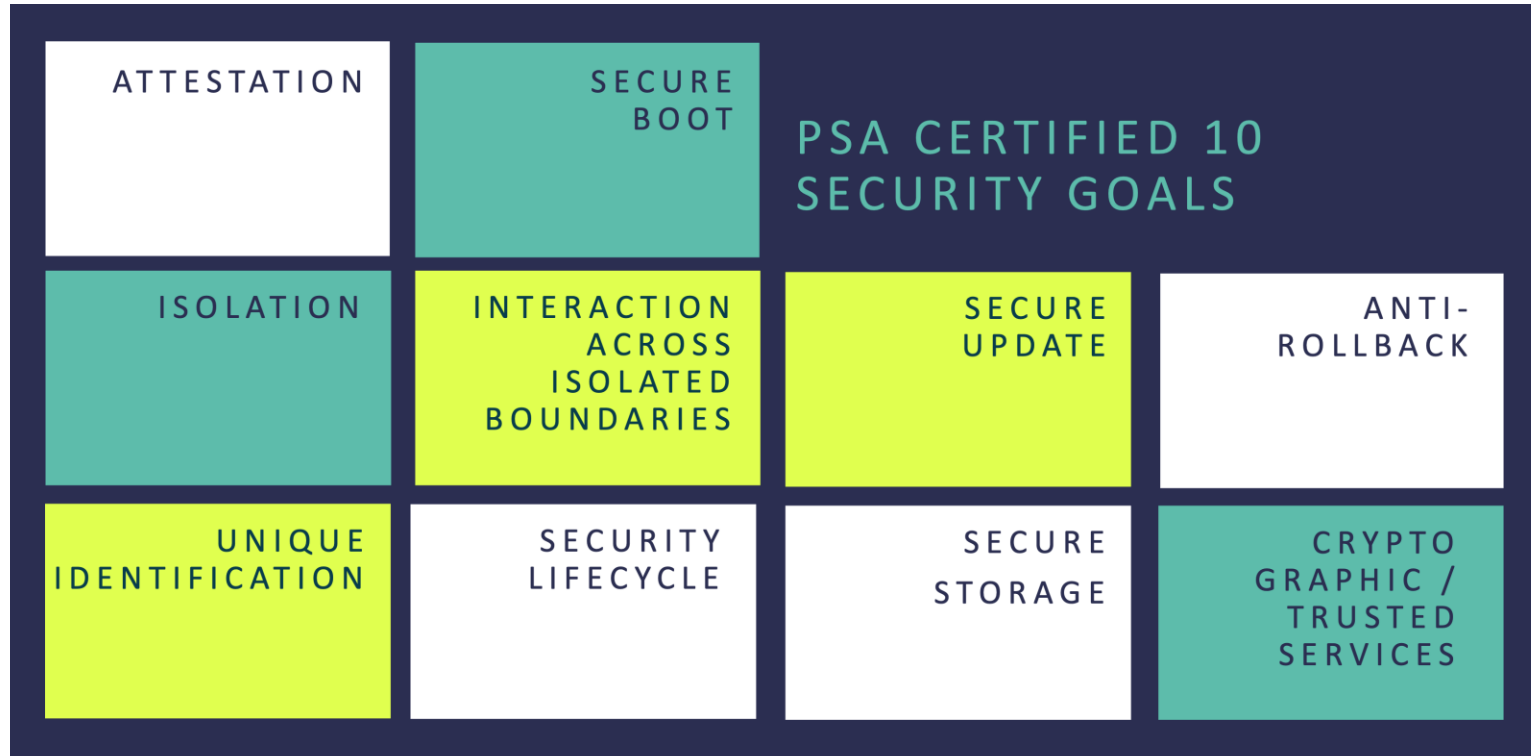


PSA Certified providing 3rd Party Assurance

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

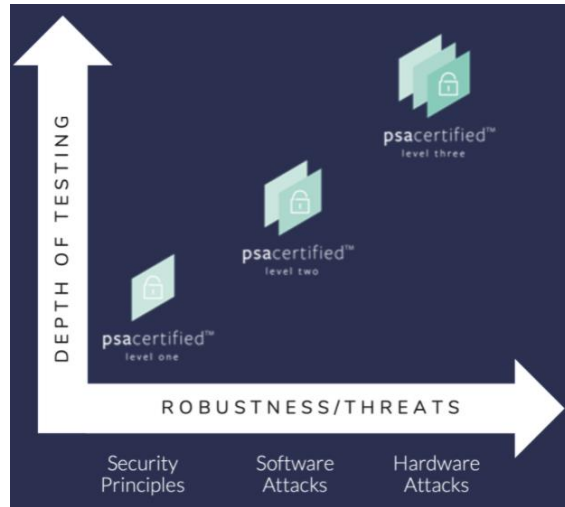


PSA Certified providing 3rd Party Assurance



PSA Certified: Three levels of evaluation

It provides three progressive levels of security assurance/robustness:



PSA Certification	Silicon + Root of Trust	OS	OEM
L3	✓ Independent lab testing 35 days	Third-party evaluation scheme	
L2	✓ Independent lab testing 25 days		
L1	✓ Independent lab REVIEW 10 days	✓	✓

PSA Certified Silicon and Root of Trust

nRF 91
SERIES
nRF9160
Cellular SiP
LTE-M and NB-IoT

nRF 53
SERIES
nRF5340
Dual-core
Bluetooth LE SoC

nRF 52
SERIES
nRF52840
Bluetooth LE SoC



PSA Certified Level 1

Assurance of silicon implementing a hardware RoT

Assessment questionnaire independently reviewed by security evaluation lab and certification body

Moving up from PSA Level 1

Security by isolation - utilising TrustZone hardware security features

Isolate security critical functions from the user application:

- Cryptographic libraries
- Private keys
- Peripherals interacting with critical hardware

PSA APIs (TF-M)

nRF53 / nRF91

Application Core

Non-Secure

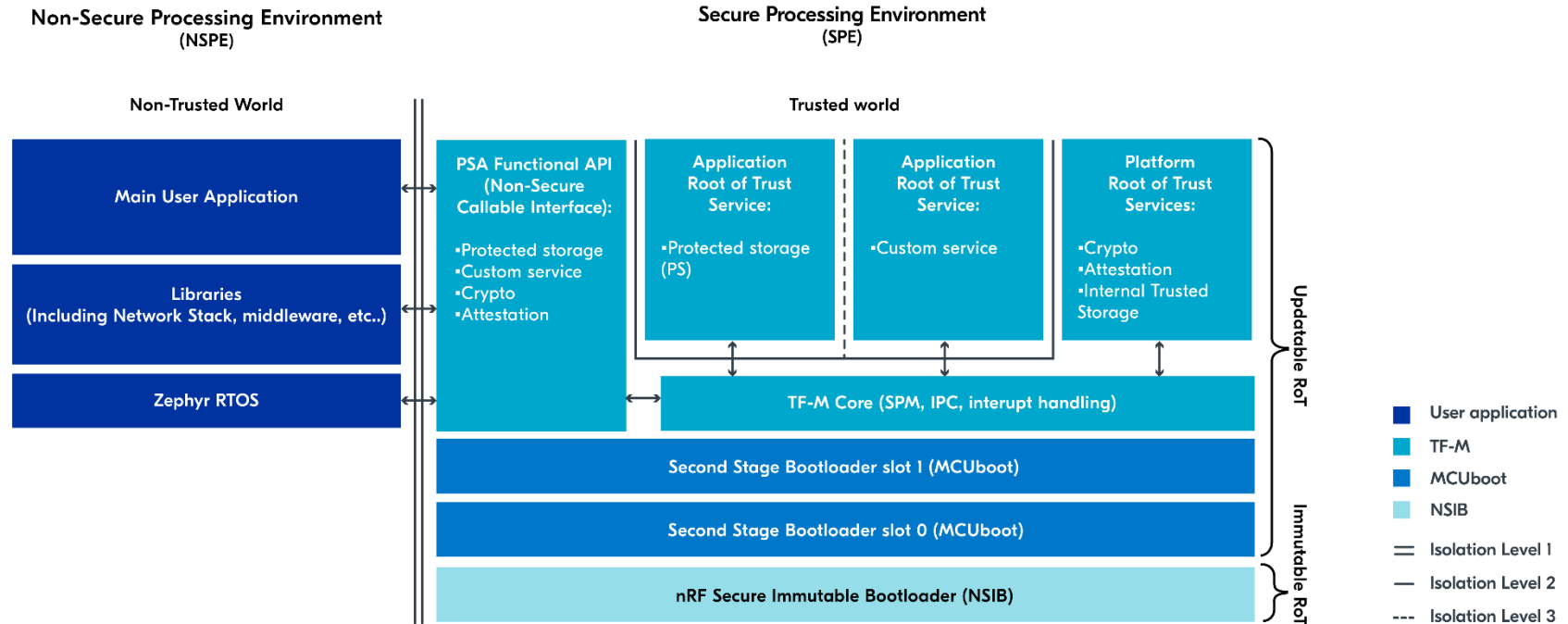


Secure

Supported in nRF Connect SDK



Trusted Firmware-M in nRF Connect SDK



How to decide what security level is required?

Threat modelling is a critical step in the design journey

Identify Assets

Keys, certificates

Identify Threats

Attack vectors towards the assets

Analyse and prioritise

Risk = probability x impact

Mitigate

Control the highest risks

Threat Model and Security Analysis examples available from PSA Certified:

- Asset tracker
- Smart water meter
- Network camera
- Smart speaker

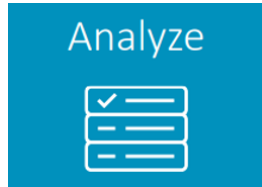
Search “threat model” on psacertified.org

Security is top priority

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

Security should be considered early in your design.

Get started with securing your next product



Perform Threat Modelling on your product

Understand the assets, threats and cost-benefit of protection.



Explore the TrustedFirmware-M samples in nRF Connect SDK

Understand how TF-M can be used to protect your most important assets.



Speak to us on **DevZone** if you need support

Learn more from Nordic



- DevZone
 - devzone.nordicsemi.com
 - Leading community in the industry
 - >80K developers, 2.4M annual site visits
 - Strong tech support team
 - Blogs, guides, and tutorials
- Nordic Developer Academy
 - academy.nordicsemi.com
- Nordic Tech Webinars
 - webinars.nordicsemi.com