PSA Certified

Jim Carver
Strategic Business Development Manager, PSA Certified

psacertified™

Agenda

- PSA Certified: An Overview
  - Introducing the ecosystem
  - Key findings from industry research
  - The PSA Certified framework and certification program
  - Aligning and Expanding the Ecosystem
- The OEM journey
  - Walking through a case study
  - The role of collaboration and reusable certifications
- Final Thoughts

Introducing PSA Certified

PSA Certified was founded by a collaboration of 7 security experts, including Arm.

Available for all members of the value chain, we offer certification for silicon, system software and end devices.

PSA Certified is a global partnership providing independent lab-validated IoT security evaluation.

PSA Certified is collaborating with the ecosystem to reduce complexities and raise the bar on IoT security.

psacertified™

Applus laboratories

brightsight the number one security lab in the world

CAICT 中国信息通信研究院

ESEC LABORATORY

riscure

UL

arm

PROVE & RUN

TRUSTCB TRUST AND VERIFY

PSA Certified – From Launch to Now

PSA Certified launched in 2019 with wide support from the electronics industry to solve the fragmentation in IoT security and to promote security by design built on a chip's Root of Trust (RoT)

psacertified™

The Growing PSA Certified Ecosystem

PSA Certified is being adopted by the rapidly growing ecosystem of silicon vendors, software providers and device manufacturers.

Majority of top 10 silicon providers are PSA Certified

100+
Products PSA Certified

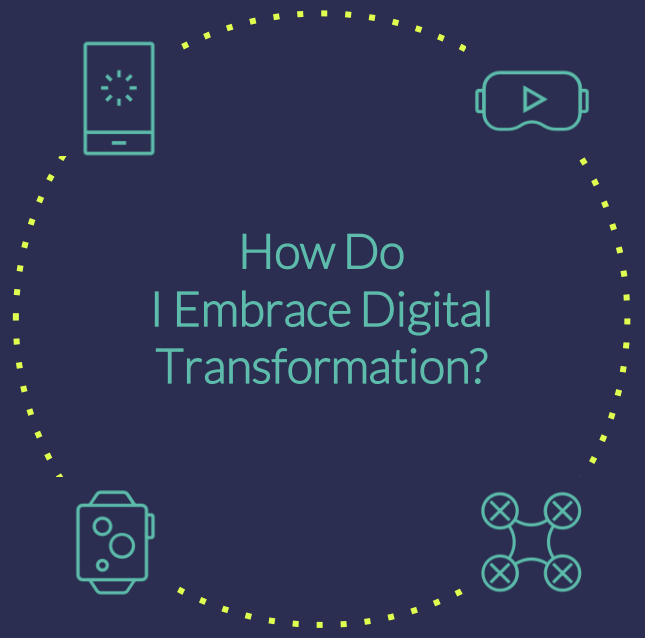
62
Chips PSA Certified

24
Software Platforms PSA Certified

23
Devices PSA Certified

https://www.psacertified.org/certified-products/

OEMs Face Challenges



Unleashing digital transformation is the common denominator of successful companies in the last 10 years

While not losing sight of 'business as usual'

Security is at the heart of all these concerns

Product Development Challenges

- Multiple regulations
- New manufacturing technologies
- Fragmented frameworks
- Inconsistent security

Financial Challenges

- High failure cost
- Total cost of ownership
- Liability
- Data breaches can put companies out of business

Consumer Challenges

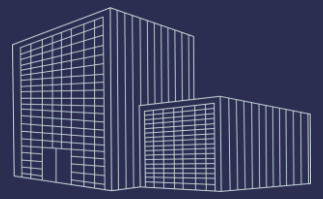
- USP / differentiation
- New revenue streams

psacertified™

Industry Opinions | PSA Certified Research

600+ technology leaders identified huge challenges

WE NEED TO DEMOCRATIZE SECURITY



41%

are satisfied with the level of security expertise in small companies

52%

consider the additional cost of security to be a top barrier

FRAGMENTATION IS A PROBLEM

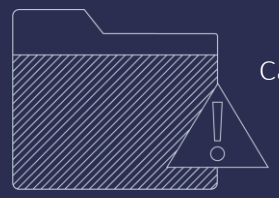
48%

say fragmentation of standards is a top challenge

SECURITY BEST PRACTICE IS BEING SKIPPED

50%

are using external labs to validate their security robustness



47%

carry out threat analysis when designing a new product

PSA Security Report 2022

psacertified™

Security Best Practice in 10 Goals

ATTESTATION

SECURE BOOT

SECURE UPDATE

ANTI-ROLLBACK

ISOLATION

INTERACTION ACROSS ISOLATED BOUNDARIES

SECURE STORAGE

CRYPTO GRAPHIC / TRUSTED SERVICES

UNIQUE IDENTIFICATION

SECURITY LIFECYCLE

PSA CERTIFIED 10 SECURITY GOALS

psacertified™

PSA Certified Explained

A complete security offering – openly published. Independently tested.

Analyze

Threat models
& security analyses

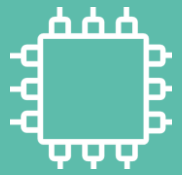
Methodically developed

Architect

Hardware & firmware
architect specifications

Open architecture

Implement



Firmware
source code

TF-M Reference implementation

Certify

Independently
tested

psacertified™

Enabling trust

psacertified™

Easy to Understand Scheme

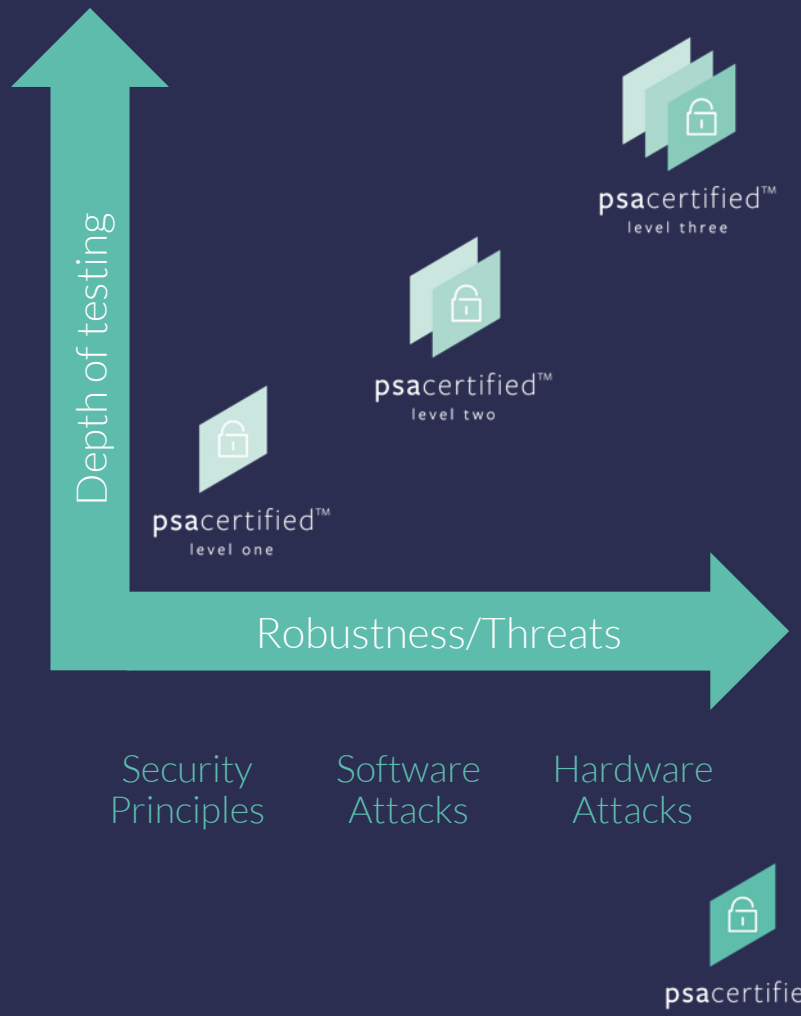
psacertified™

PSA Certified provides three progressive levels of security assurance/robustness

psacertified™ functional API

PSA Functional API Certified enables the ecosystem through a consistent high-level interface to the PSA-RoT

PSA Certified Levels



Three Levels of Assurance

Security Principles

- Methodically created using IoT threat models, 10 Security Goals and regulatory requirements
- Self-filled questionnaire with less than 50 security questions, reviewed by lab & CB

Protection from scalable software attacks

- Time-limited white box testing (ANSSI CSPN style)
- 25 days of analysis and test

Protection from physical attacker & software attacks

- Extensive hardware attacks for example side-channel attacks and perturbation

PSA Certification Level	Silicon	OS	Device
Level 3 Months	✓	Other third party evaluation schemes	
Level 2 1 Month	✓		
Level 1 1 day	✓	✓	✓

psacertified™

PSA Certified Level 1

For device makers, software platforms and chip vendors

- <50 questions on Software Platform and Device based on PSA 10 Security Goals, IoT threat models, government requirements and laws
- Chip section has ~10 requirements and can be fulfilled by a basic chip RoT
- Composite (layered) for efficiency
- Quick and straight-forward – fill in and review with a PSA Certified test lab

Alignment mapping to:

- EN 303 645
- NIST 8259A
- SB-327

psacertified™

Aligning to Industry Regulations

PSA Certified is actively aligning with upcoming regulations and standards including:

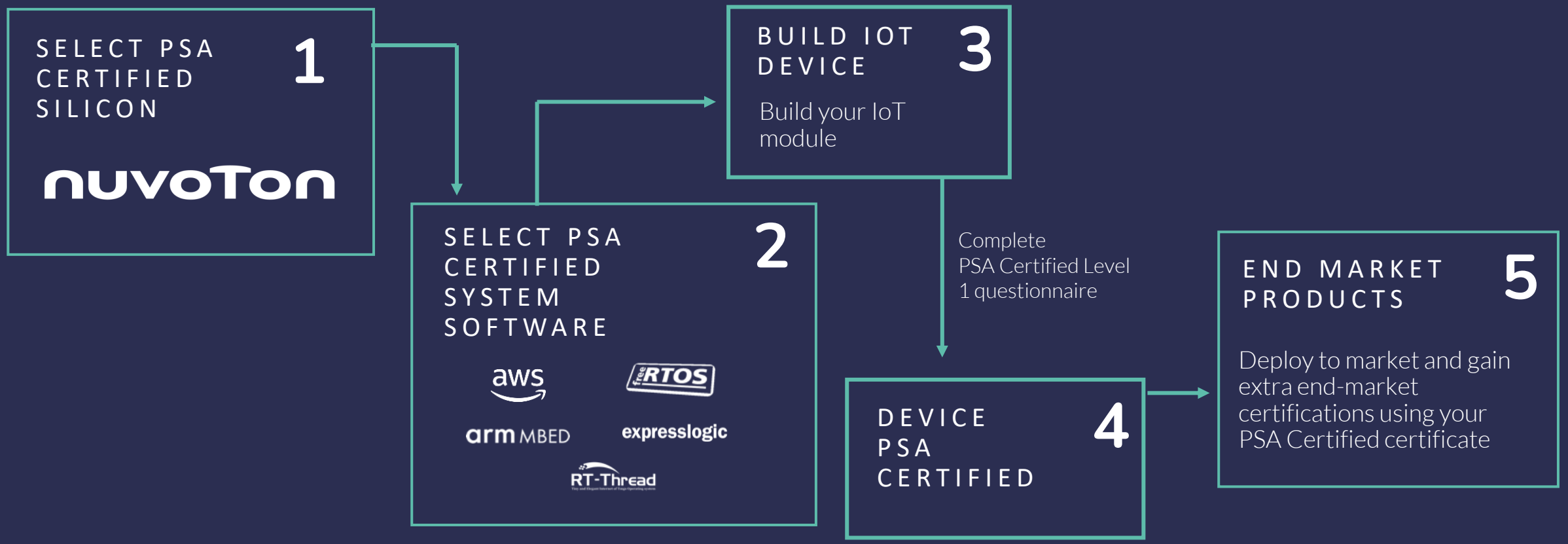
NIST 8259A	(NIST - IoT Device Cybersecurity Capability Core Baseline)
ETSI 303 645	(European standard - Cyber Security for Consumer IoT)
SB-327	(California Law - Security of Connected Devices)
UK DCMS (draft)	(Regulating consumer smart product cyber security)
IEC 62443 4-2 CSA-311	(Security for industrial automation and control systems)

UL	"UL will recognize PSA Certified as a fast-track for achieving UL's Secure IoT Component Qualification"[2]
ioXt internet of secure things	"ioXt has selected PSA Certified as a foundational Root of Trust scheme and will recognize it in its product evaluations"[3]
SESIP™	PSA Certified is now available with a choice of evaluation methodology: CSPN-style and GlobalPlatform SESIP
DLC Energy · Quality · Connectivity **(To be announced early 2022)**	Initial agreement to recognize PSA Certified meets DesignLights Consortium specification Criteria for acceptable cybersecurity standards. Intentions is to add PSA Certified Level 2 and PSA Certified Level 3 to the list of options for cybersecurity certification that manufacturers can choose.
matter **(WIP)**	Work with Matter, contribute to security specifications with active participation in security workgroups.

[2] www.ul.com/news/ul-recognizes-psa-certified-fast-track-uls-secure-iot-component-qualification
[3] https://www.ioxtalliance.org/news-events-blog/ioxt-alliance-psa-certified-align-to-improve-iot-device-security

psacertified™

The OEM Journey to a PSA Certified Connected Device



psacertified™

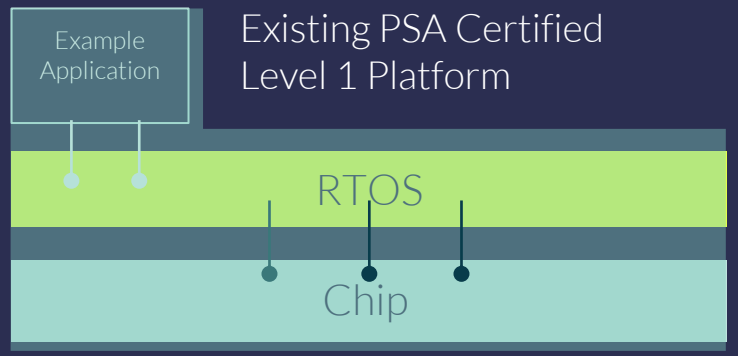
Advantages to Using PSA Certified Silicon from NUVOTON

- To earn PSA Certified Nuvoton silicon has undergone extensive penetration testing by independent security labs
  - Testing was developed in conjunction with TrustCB to insure test coverage
  - Result: Strong security that you can trust for your designs
- Nuvoton supports the PSA Functional API specification
  - Well understood APIs to simplify application development with secure MCUs
  - Result: Faster time to market and better code reusability
- Certified Chips from Nuvoton and Certified System Software allows developers to develop secure products which can themselves be certified at the device level
  - Assurance for your end customers from independent laboratories that you are providing a secure solution that complies with NIST and ETSI security standards.

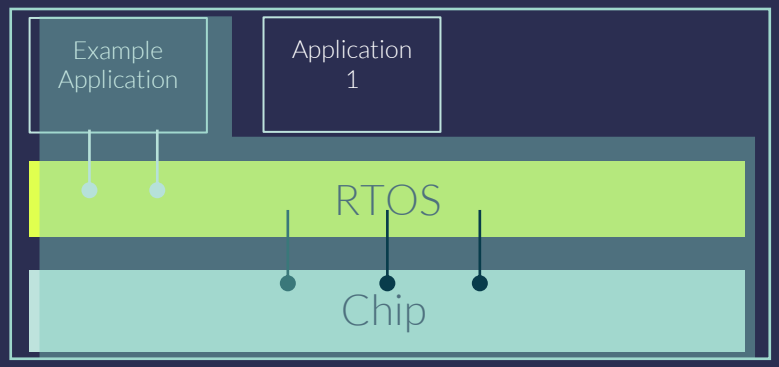
psacertified™

Re-using a PSA Certified Platform

Vendors can benefit from reusing a PSA Certified platform for their own PSA Certified efforts.

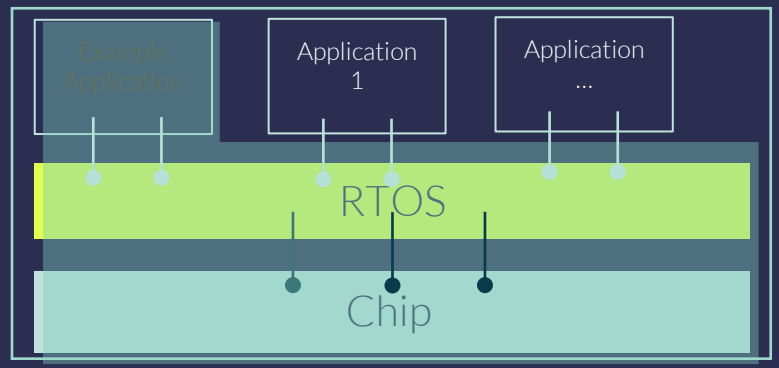


Existing PSA Certified Level 1 Platform



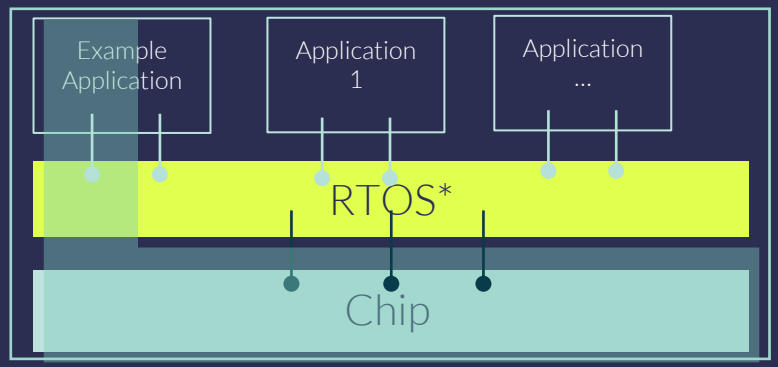
Scenario 1: No security related changes.

E.g. vendor changes branding and colors etc. Mostly reuse.

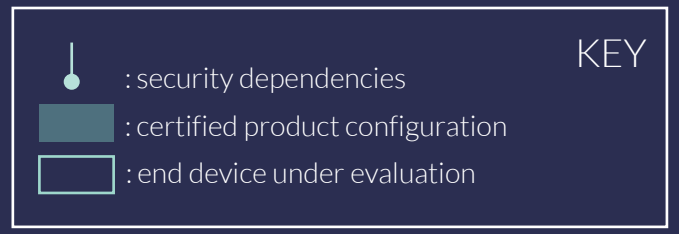


Scenario 2: Application security changed/added. RTOS & Chip no change.

E.g. vendor changed the application, adding/modifying security features of the certified product. RTOS is not changed. ~50%* can be re-used.



Scenario 3: Application & RTOS security changed. Chip no change.
~30%* can be re-used.



psacertified™

Why should you care about PSA Certified?

- IoT devices need to be trusted products
  - IoT Devices form the trust anchor in a system's chain of trust
  - Regulations are evolving and strengthening, new design must be futureproof
- Developing secure products can be time consuming and challenging
  - New software architectures need to be used
  - Solutions need to be extensivity tested to identify potential vulnerabilities
- Developing with PSA Certified solutions can solve this problem
  - Certified Chops and System Software have already been evaluated by independent security labs.
  - Using PSA Functional APIs increases code reusability
  - Result: Faster time to market with lower risk

Start Today

DOWNLOAD:
PSA Certified Level 1 questionnaire

LATEST RESEARCH:
report.psacertified.org

JOIN US ON TWITTER & LINKEDIN:
@PSACertified

ACCESS TRAINING MATERIAL, RESOURCES AND WEBINARS
PSACertified.org/resources

Contact Jim or Anurag for more details
Jim.Carver@Arm.Com or Anurag.Gupta@Arm.Com

Thank You

Jim.Carver@arm.com

psacertified™