



Attestation in ARM

Yogesh Deshpande – Architecture and Technology Group

Date: 15/11/2023

The Threat of Security Inaction Is Growing

World Economic Forum now lists cybersecurity failure as a critical threat in the next two years ⁽¹⁾

55.7 Billion

Connected devices expected to be shaping digital transformation by 2025⁽²⁾

1.5 Billion Hacks

In the first half of 2021 -double the number from the previous half-year⁽³⁾

\$10.5 Trillion


The estimated cost of cybercrime by the end of 2025 ⁽⁴⁾

- (1) World economic forum
- (2) IDC
- (3) Kaspersky
- (4) Cybersecurity ventures


What is PSA Certified?

A complete security framework – openly published.
Independently tested.

Analyze



Threat models
& security analyses



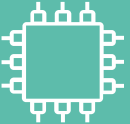
Architect




Hardware &
firmware architect
specifications




Implement



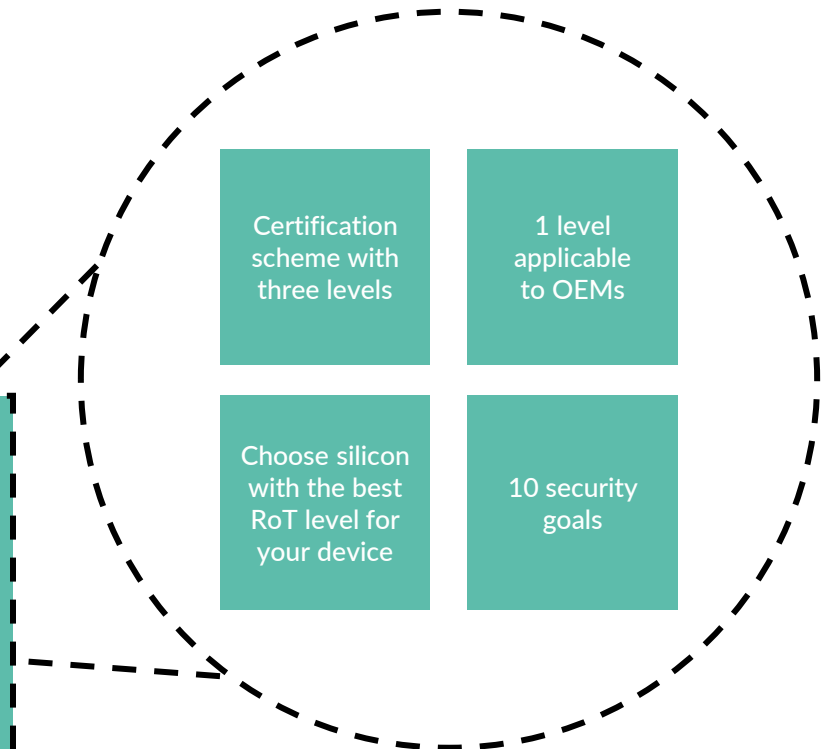

Firmware
source code



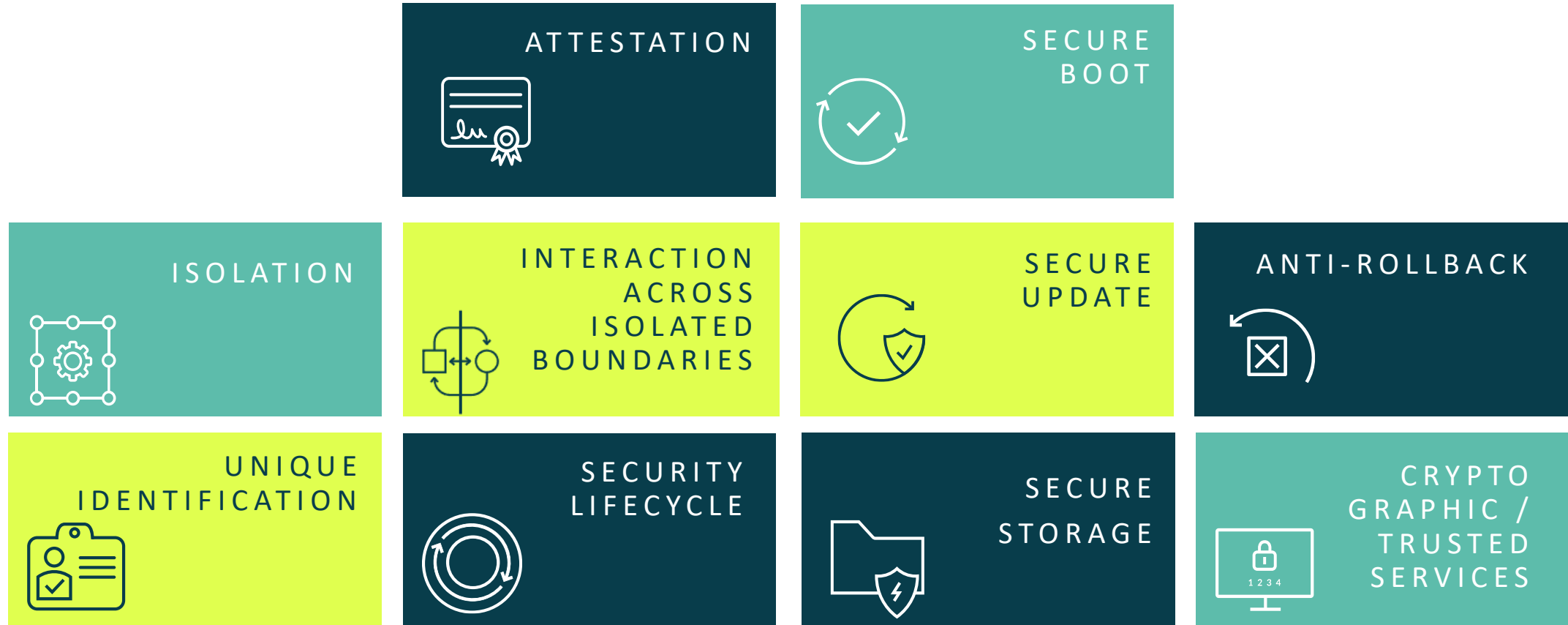
Certify



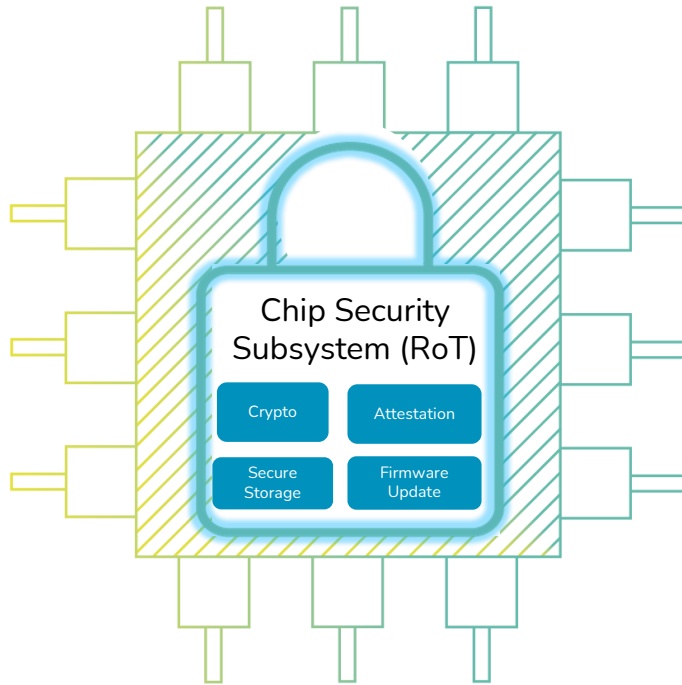
Independently
tested



Key Security Goals to Consider



PSA Core Objectives



Create a RoT for the SoC World



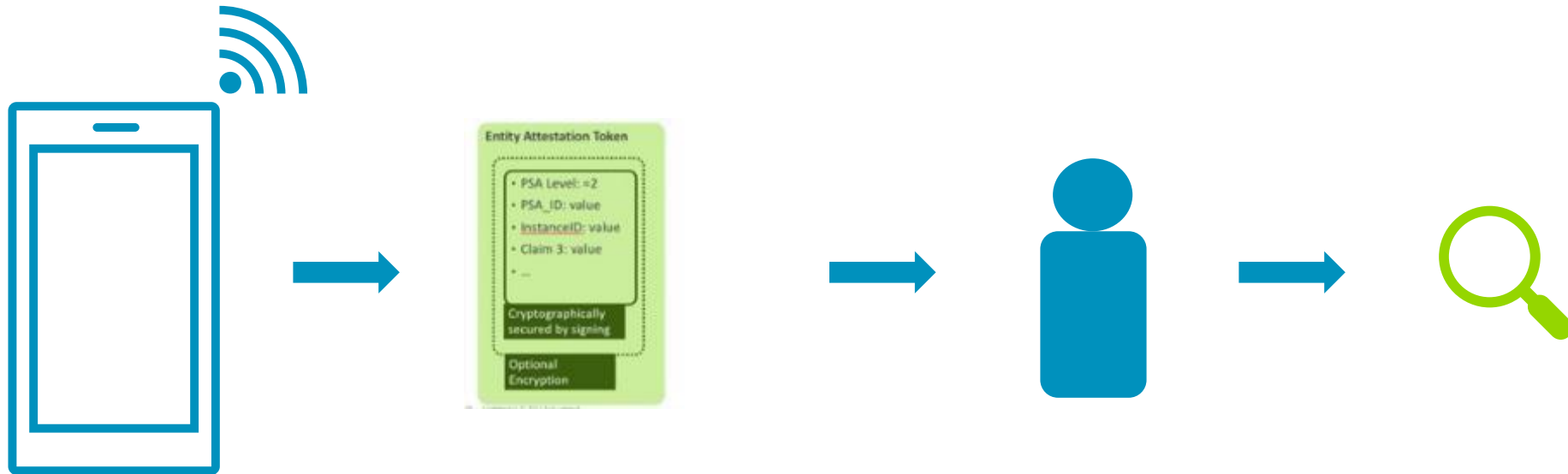
Make it easy to use



Simplify and defragment
Security by Design

Attestation

- + Attestation is the system by which something produces evidence about itself that another party can use to evaluate the trustworthiness of that entity



Example of items that need to be evaluated for trustworthiness?

- Is this known Hardware?
 - Not an emulator
 - Known to be built to correct architectural standard
- Is this known Firmware?
 - Recognised to come from a trusted supplier
 - Not known to have any vulnerabilities or exposures (CVE)
- Does it have a **Root of Trust** that can produce authoritative evidence about the device?
 - Recognised security system as source of truth
- plus points:
 - Has the device been certified by a known authority ?
 - Passes test regime
- which factors are necessary to trust depends upon the threat model in use

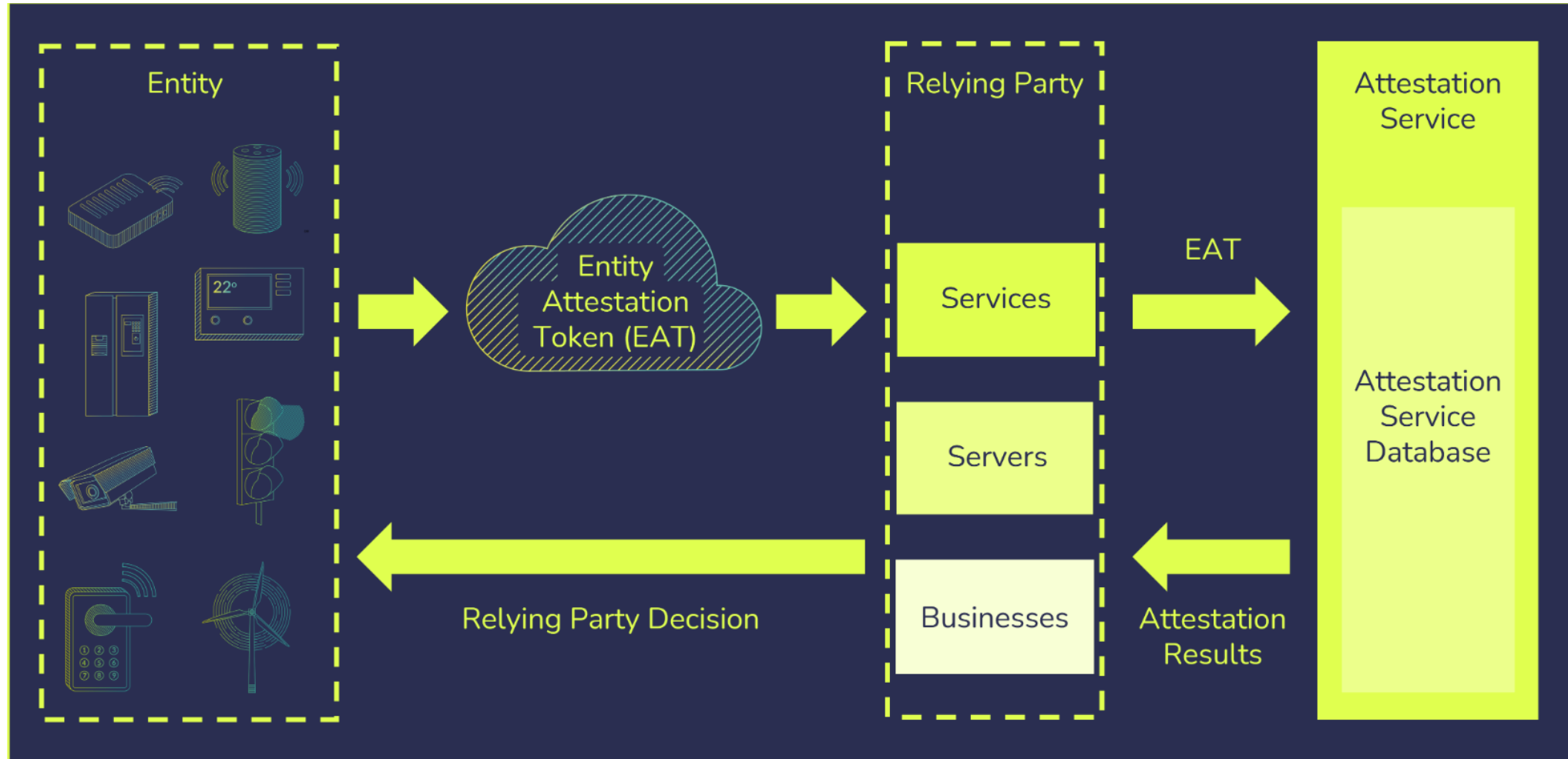
Why attestation is an important security goal?

- Depending on the use case, there can be a wide variety of devices that contribute to a solution
- Devices range from IoT end points, Edge Devices, or in the cloud
- Evidence is needed that all the devices that participate in the ecosystem are trustworthy

How can we do that ?

- Can be accomplished, if they are built using right security standards and practices
- Attestation can be used to help establish their trustworthiness

Attestation ecosystem



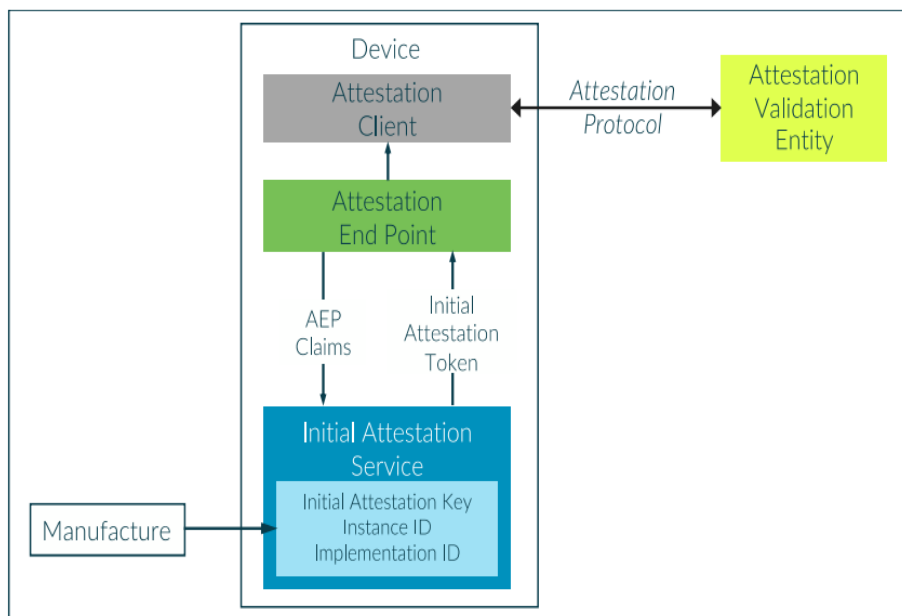
PSA Evidence

- PSA Claims are encoded in CBOR and wrapped in COSE Web Token (CWT) [RFC 8392]
- Is a COSE_Sign1 object
- Some of the important claims include
 1. PSA Implementation ID – Identifies implementation of PSA Root of Trust
 2. PSA Instance ID – Unique identifier of the Initial Attestation Key
 3. Nonce – Supports freshness model for attestation evidence
 4. Profile – Allows a receiver to assign intended semantics to the rest of the claims
 5. Security Lifecycle – Represents current lifecycle state of the PSA RoT, example: provisioning/ debug
 6. Boot Seed – Allows distinction of reports from different boot sessions
 7. Software Components – Measurements of SW component loaded by the PSA RoT
 8. Verification Service Indicator

Attestation Verification

- Confirm security of the Attestation token comes from a known Root of Trust
- Evidence needs to be assessed against known Reference Values from manufacturer
- This should be done remotely as:
 - Ensures validation process is conducted independently from any interference with device
 - Centralised validation service more likely to have up to date information on validity
 - Centralised validation service can simplify access to data from complex supply chains
- Verifier therefore needs to have some out of band trust established
 - Transitive Trust relationship to supply chain
- For a Composite Device, a single Verifier may not have the complete information to appraise all Claims in the Evidence. In such cases, a Verifier may delegate a part of evidence verification to another trusted Verifier

Attestation Process



- When required, interact with non-secure software to obtain an Attestation report
 - App / User / Network facing service
- Non secure software calls a secure service to request Attestation report
 - Secure service will be in an isolated environment
 - Root of Trust
 - Has access to Boot Time measurements of firmware
- Attestation report is a collection of Evidence about the device makeup & state
- Root of Trust signs the Attestation Report
 - Signature from key derived from Uniquely provisioned secret
 - Secrets only accessible to Boot Code or in separate Security Element

arm

Attestation in Confidential Computing

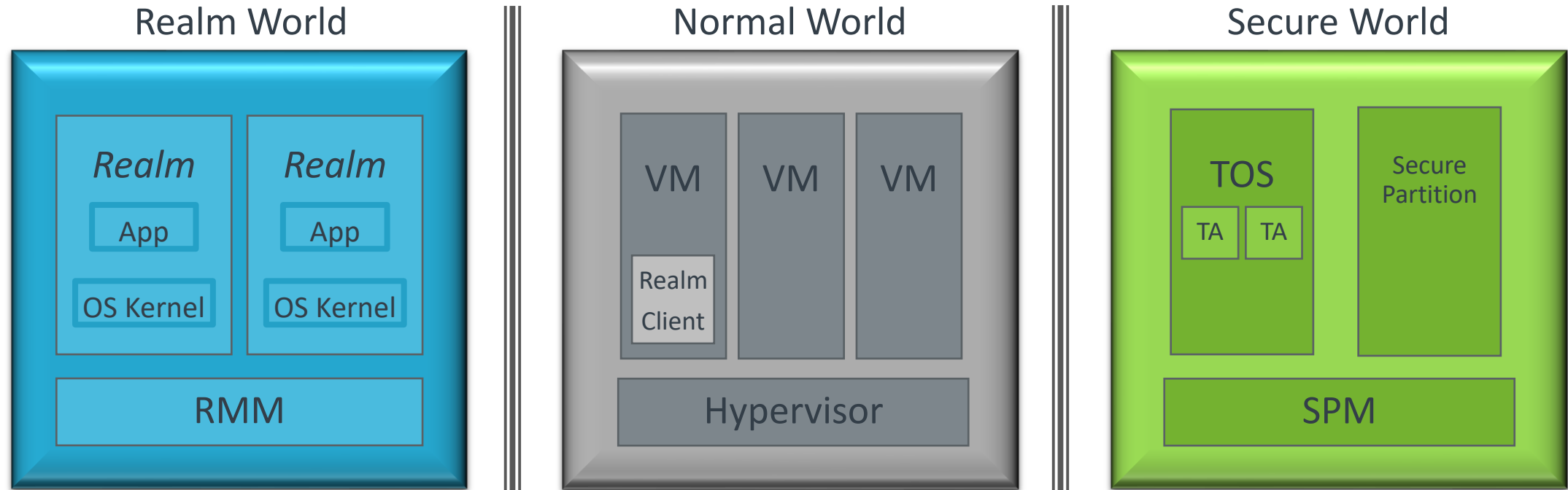
Why Confidential Computing ?

- Compute in early days used to be managed on locally controlled hardware
- Increasingly, this is no longer the case
 - + Cloud Computing
 - + Edge Computing
 - + Prone to wide variety of attacks
- How does this affect access to user data ?
- Data at Rest and Data in Transit are largely solved
- How about Data 'In Use' ?
- Enter: Confidential Computing...

Attestation in Confidential Computing

- Confidential Computing provides a computation environment trusted to be secured against observation or modification by external parties
- Secures 'Data In Use' from access or modification
 - Data and Code
- Full confidentiality requires a combination of hardware and software architectures to secure the execution environment
- Confidential computing requires a way for a user to establish that it is trustworthy
 - Attestation

Arm Confidential Compute Architecture – Arm CCA

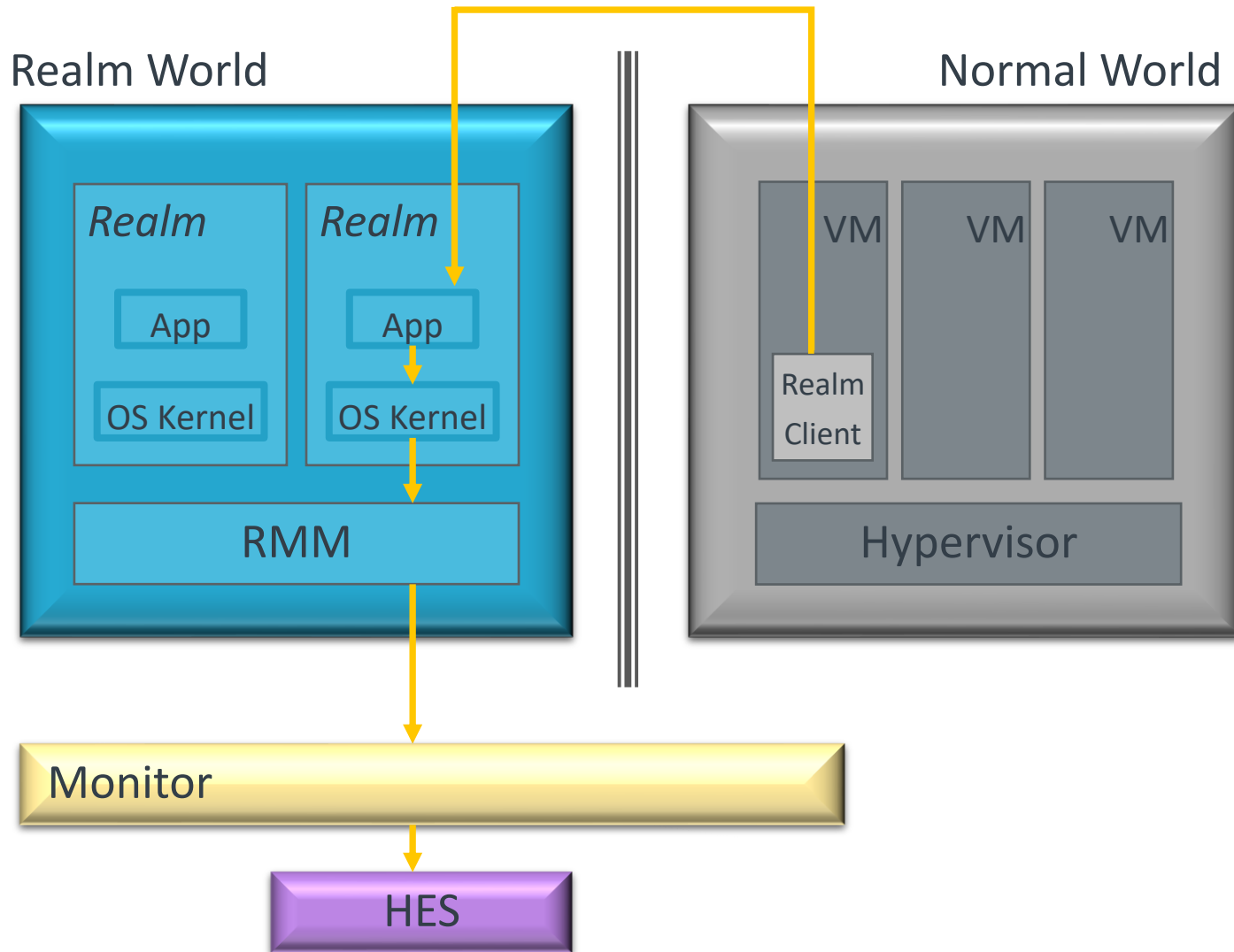


Arm CCA adds a new environment for 3rd party confidential compute: **Realm world**

Arm CCA system provides an attestation mechanism that a Realm User can use to establish trustworthiness in the deployment

Arm CCA adds a new architectural feature, the Realm Management Extension

Attestation Flow for realms



Client of a realm wants to establish trustworthiness before revealing any secrets

Realm can request attestation at any time

Response contains evidence for trust of Arm CCA implementation and software in realm

Arm CCA strongly recommends Hardware Enforced Security (HES)

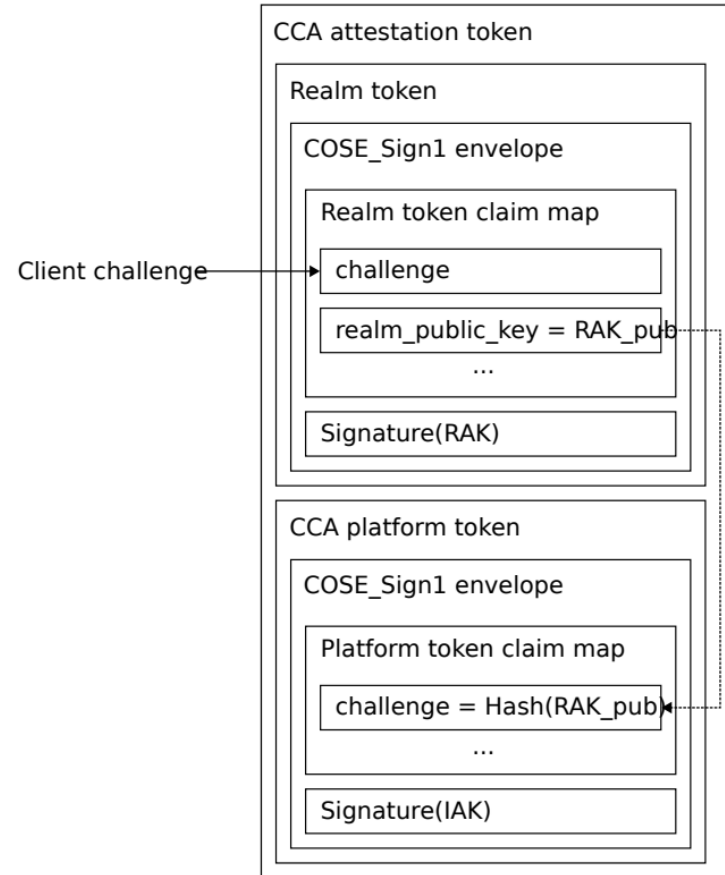
Attestation Security

- Attestation Report is signed with a known key to provide cryptographic proof that it has not been tampered with
- HES (Hardware Enforced Security) is a term covering hardware trusted controllers that can store and process secrets outside of the main AP
- Backing Attestation report with HES gives isolation for signing secrets and measurements
 - Separate execution context
 - Holds provisioned secrets
 - Exposes interfaces to allow storage of boot state & for attestation request
- Monitor is part of EL3 Firmware where the required isolation is programmed
- Request mechanism requires provision of a challenge to support proof of freshness

Arm CCA Evidence for Trustworthiness

- Realm software can request an attestation report for their realm at any time
- Calls are made via the software stack to the RMM to obtain the report
- Attestation provides evidence to enable trust establishment
- Arm CCA Platform
 - Hardware identification
 - Measurements and Identities of all firmware components
 - Measurements and Identities of all Trusted Subsystems
 - Security lifecycle (a statement on the security of platform keys)
- Realm Attestation
 - Policy used to construct the realm
 - Measurement of initial realm contents
 - Debug context
 - Realm runtime boot measurements

Arm CCA Evidence Collection



Arm CCA Verification

Arm CCA Verification is a multi-stage Verification Process

- Platform Verification
 - Verifies the Hardware identity of the Platform
 - Verifies the Platform Root of Trust Measurements
 - Verifies the Boot State of the Platform

- Verifying the binding of Workload to a Platform

- Workload/Realm Verification
 - Verifies the initial configuration of the Realm creation
 - Verification of guest application measurements

arm

Attestation Verification & Project Veraison

Assistance in building Attestation Verification Services

*Arm is contributing to Project VERAISON (**VER**ific**At**ion of **atteStatiON**)*

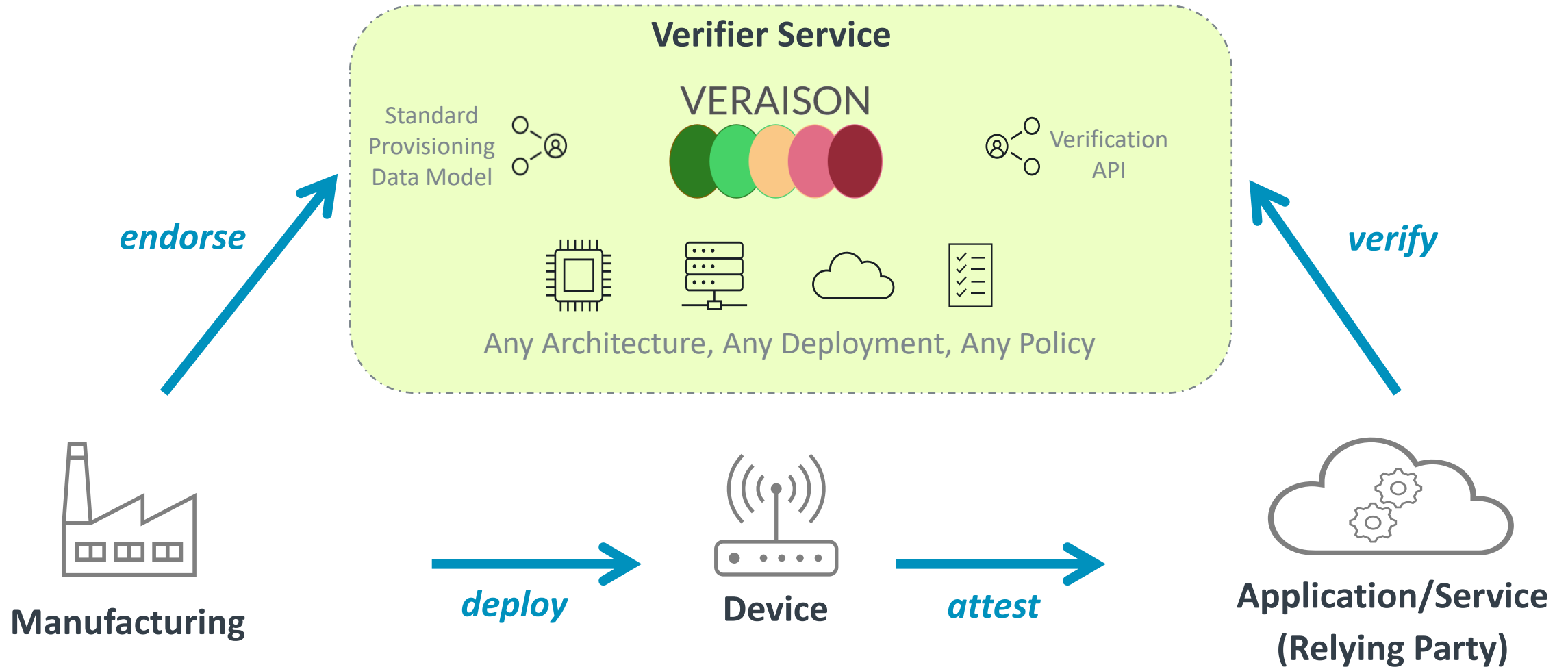
- + Veraison is an OSS project to create software components used to build a Verification Service
- + The availability of common components brings some standardisation and quality levels to deployments and also lowers the cost of building a trustworthy infrastructure
- + Veraison is an extensible, policy driven system targeting multiple tokens
 - PSA, CCA, DICE etc
- + Built embracing standards approach
- + <https://github.com/veraison>
- + A Confidential Computing Consortium Project



Key features

- Multi Architecture
 - Deconstruct Verification process into common pipeline
 - Add pluggable modules for architecture specific details
- Flexible Deployment Model
 - Public, private, hybrid, multi cloud service
 - Single or Multi-tenant
 - Potential to deploy locally `e.g. in adjacent isolation such as TrustZone

Endorse, Attest, Verify



Standards and OpenSource Reference Materials

Description	Location
ARM Security Features	https://www.arm.com/architecture/security-features
PSA Security Model	https://www.psacertified.org/app/uploads/2021/12/JSADEN014_PSA_Certified_SM_V1.1_BET0.pdf
PSA Certified API's	https://arm-software.github.io/psa-api/
Open-source TF-M,TF-A,TF-RMM and other reference implementations	https://git.trustedfirmware.org/
RFC 9334 IETF RATS Architecture	https://www.rfc-editor.org/rfc/rfc9334.html
IETF Attestation Results for Secure Interactions	https://ietf-rats-wg.github.io/draft-ietf-rats-ar4si/draft-ietf-rats-ar4si.html
IETF Concise Reference Integrity Manifest	https://ietf-rats-wg.github.io/draft-ietf-rats-corim/draft-ietf-rats-corim.html
ARM CCA Description	https://www.arm.com/architecture/security-features/arm-confidential-compute-architecture
ARM CCA Security Model	https://documentation-service.arm.com/static/610aaec33d73a34b640e333b?token=
Project Veraison	https://github.com/veraison

Engaging with standards bodies (IETF/TCG)

- Actively contributed to development of RFC 9334 IETF RATS Architecture
- For Attestation Evidence, PSA Entity Attestation Token is a profile of EAT token standard
- Attestation Verification needs Endorsements and Reference Values from various Supply Chain entities (example OEM, ODM, ISV etc)
- Active contributions to IETF & TCG Concise Reference Integrity Manifest (CoRIM) standard for Endorsements/Reference Values
- Attestation Results (AR) are consumed by the Relying Parties. To handle results for a broad range of Devices, one needs a standardized AR. Active contributions in the development of AR standard
- In addition to this, multiple initiatives around Bundled Evidence (EAT Collection) and EAT Media Types under progress

ARM Vision on Attestation

- Attestation as a technology has many barriers
 - Custom solutions by individual organizations, which hinders inter-operability
 - Cost of building and deployment of an Attestation System
 - Complexity of the technology
- Arm's vision is to reduce barriers to Adoption of Attestation as a Key Security Feature
 - Engage with the community
 - Active contribution to development of standards
 - Provide open source reference implementation of libraries and tools that implement the standards
- This will lead to easy to use, standards based, inter-operable Attestation ecosystem

arm

Thank You

Danke

Gracias

Grazie

谢谢

ありがとう

Asante

Merci

감사합니다

धन्यवाद

Kiitos

شكرًا

ধন্যবাদ

תודה



The Arm trademarks featured in this presentation are registered trademarks or trademarks of Arm Limited (or its subsidiaries) in the US and/or elsewhere. All rights reserved. All other marks featured may be trademarks of their respective owners.

www.arm.com/company/policies/trademarks