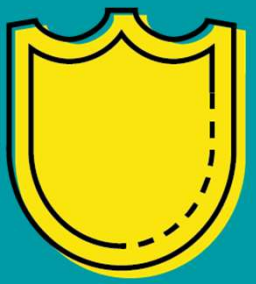
Security Conference

Automated and Continuous Cybersecurity Certification for IoT

Presented by:
Prof. Shahid Raza
Director of Cybersecurity Unit @RISE

18/10/2023

Cybersecurity Unit @ RISE



RISE Cybersecurity Unit

One of the largest cybersecurity research and innovation groups in Sweden

Participate in

- **European Cybersecurity Organization (ECSO)**
- **EU Stakeholder Cybersecurity Certification Group (SCCG)**
- **Standardization (IETF, 5GAA, …)**

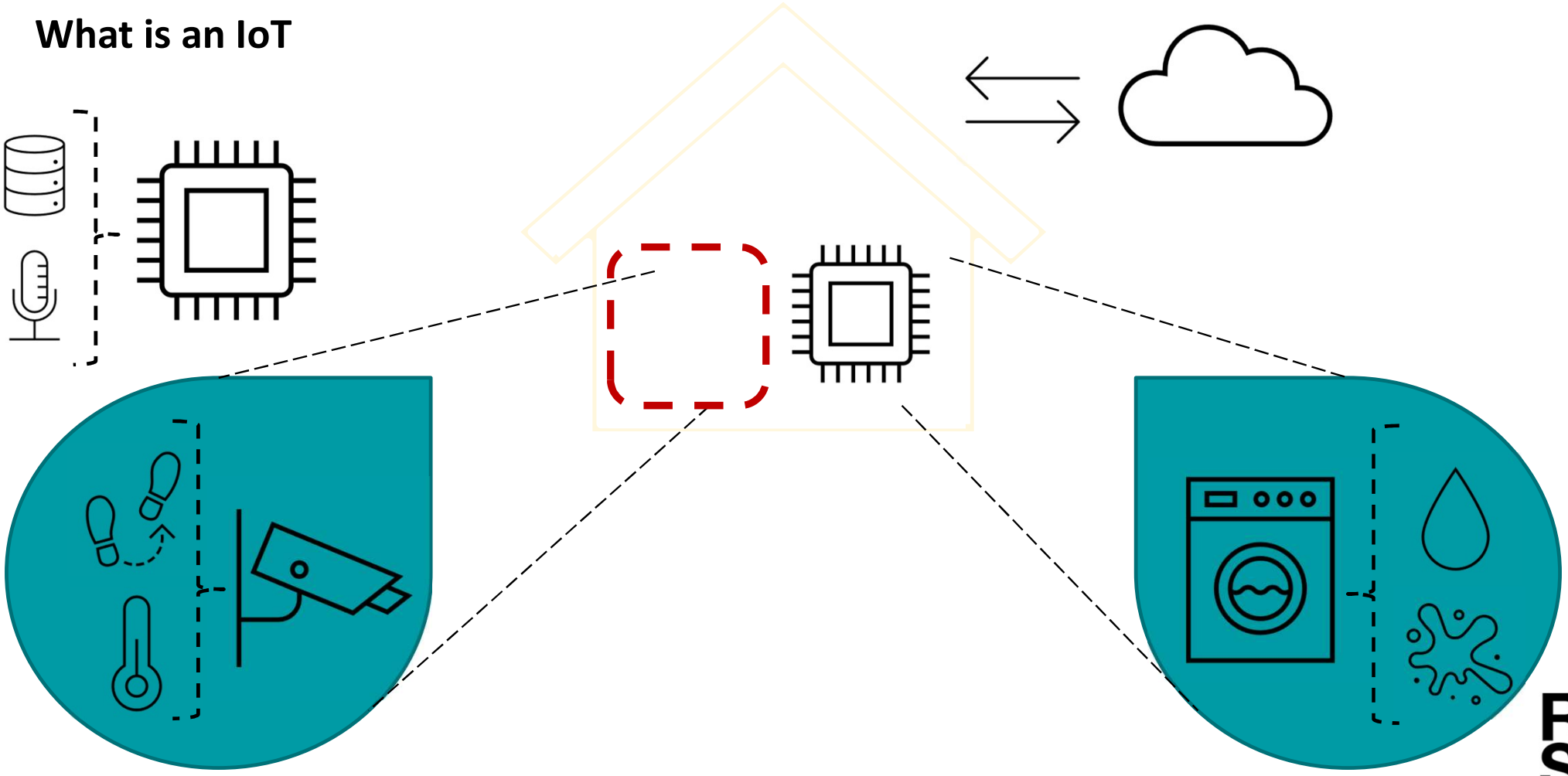
Leading the Swedish National Cybersecurity Innovation Node (part of **NCC-SE**)

Owns RISE **Cyber Range**

Co-founder of **Cybercampus Sweden** (cybercampus.se)

Coordinator of **Horizon Europe CUSTODES**, a cyber certification project

What is an IoT



IoT security building blocks

- Software security
  - Code analysis
  - Fuzzing and testing of code
  - Formal methods

- Hardware-based Root of Trust (RoT)
- Endorsement Key (EK) – unique
- Platform Configuration Registers (PCR) store hashes of software present/loaded on the device.

Who ensures that the state-of-the-art cybersecurity is enabled?

Cybersecurity Certification

for IoT software

More than 99% vulnerabilities are software based

High-level step in IoT cyber certification

1. A device vendor communicates the secure state of a device to a conformity assessment body (CAB)
2. The CAB verifies the software integrity of the device and issue an integrity certificate
3. A potential communication end-point (Edge/cloud) of IoT devices verifies that the device integrity certificate is valid and/or the current state and the attested state are the same

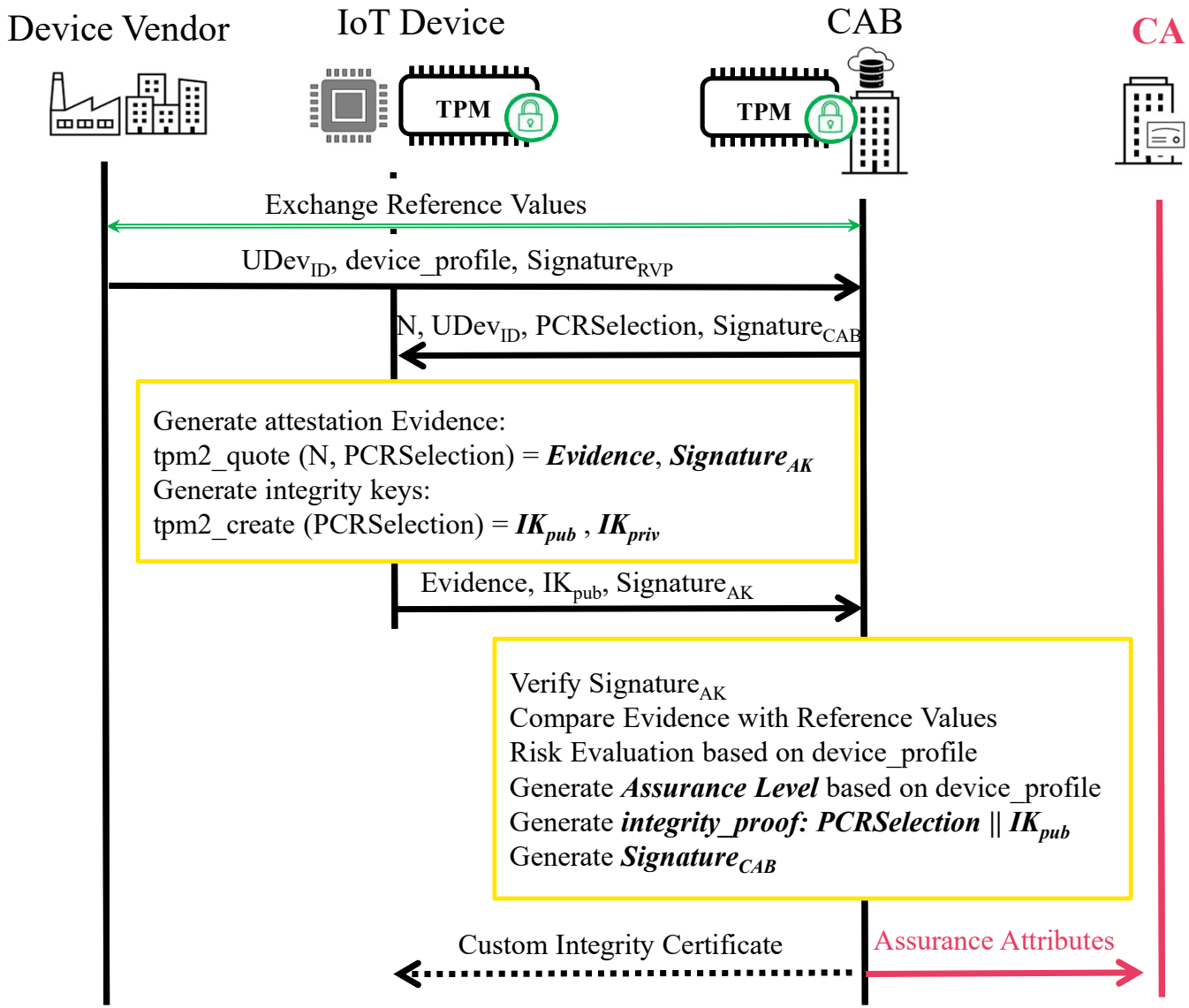
RI.
SE

IoT software certification: **design requirements**

- Digital guarantees: based on math and crypto (not verbal or manual guarantees)
- The process must be automated and lightweight
- Certification should work with future software updates
- Validity & authenticity of the certificate should be easily verifiable
- Certification process should itself be secure

RI.
SE

IoT Device Remote Attestation



Using PKI for both Authentication & Assurance

- Public Key Infrastructure (PKI) is a state-of-the-art digital certificate management system for the Internet
- Can we leverage on PKI infrastructure and use X.509 certificates also as integrity certificate?
  - Include **assurance attributes** in X.509 **extensions**
  - Can be marked as non-critical ensuring compatibility with standard X509 certificates when integrity certificate is not needed

- IETF RFC 9148: Enrollment over Secure Transport with the Secure Constrained Application Protocol
- CBOR Encoded X.509 Certificates (C509 Certificates). draft-ietf-cose-cbor-encoded-cert-05
- PKI4IoT: Towards Public Key Infrastructure for the Internet of Things. Computers & Security journal (Elsevier), Volume 89,Pages 101658, February 2020
- Lightweight Certificate Revocation for Low-power IoT with End-to-end Security. Journal of Information Security and Applications (Elsevier), Volume 73, 103424, March, 2023

RI.
SE

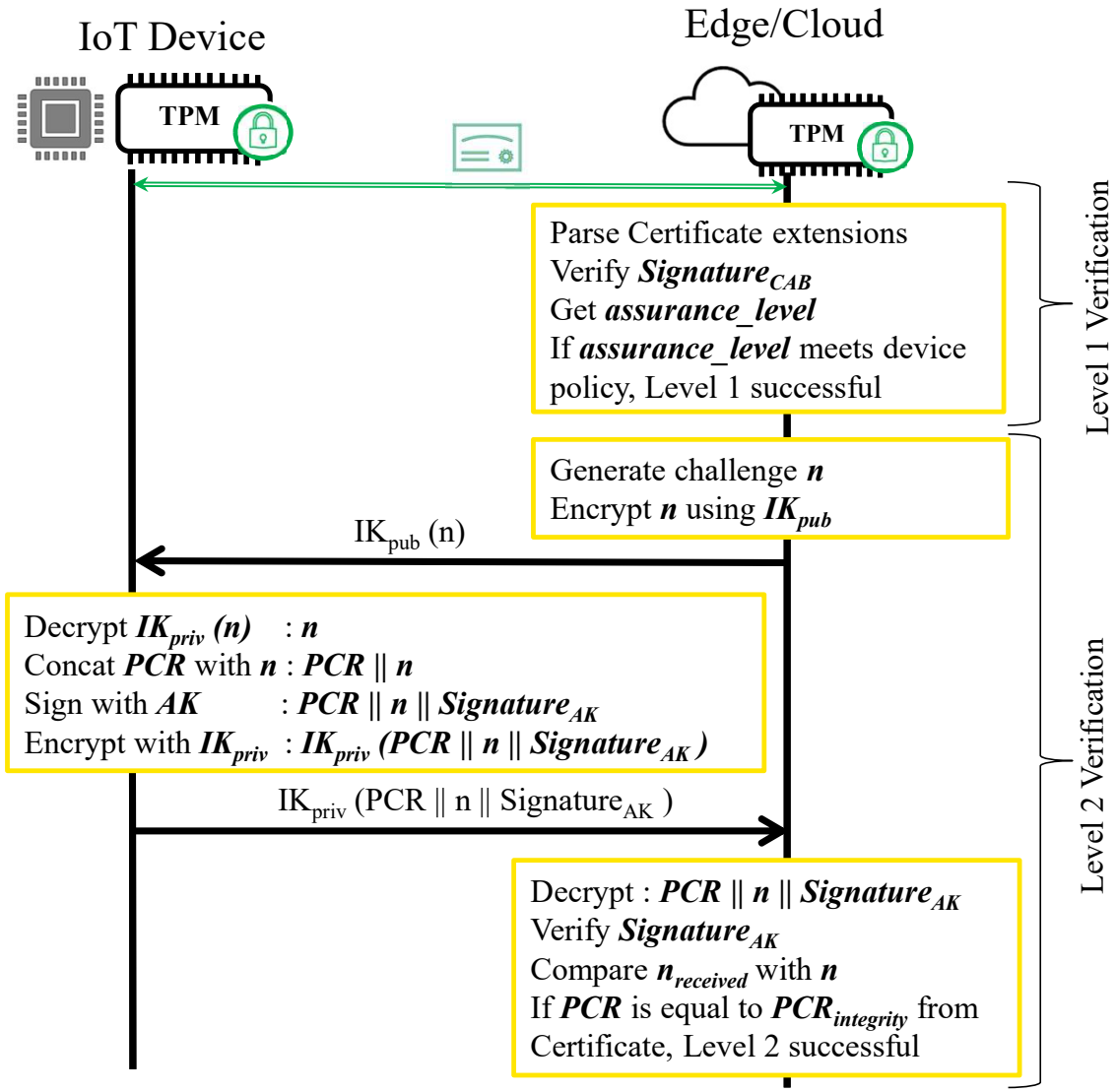
Combined Authentication & Assurance Certificate

$Cert_{AC}$ - X509 certificate with extensions			
Data	Version	:	V3
	Serial number	:	e 4 b b 2 f 3 d 4 5 e f a 6 b c d...
	Signature	:	ecdsaWithSHA256
	Issuer	:	CA Name
	Validity	:	Friday, Feb 28, 2022 12:00:00 to Friday, Dec 31, 2022 12:00:00
	Subject ($UDev_{ID}$)	:	'Device Name :: CA Name' or EUI-64
	Subject public key info	:	ecPublicKey, prime256v1 & 64-byte uncompressed ECC public key
	Issuer & subject *uniqueID*	:	-
Extensions	*Assurance Level*	:	OID : xx . xx . xx . xx Critical : No Value : High
	integrity_proof	:	OID : xx . xx . xx . xx Critical : No Value : PublicKey
	$Signature_{CAB}$	:	OID : xx . xx . xx . xx Critical : No Value : 21 a6 09 f4 11 06 .....
Signature	Signature algorithm	:	ecdsaWithSHA256
	Signature	:	30 82 01 0a 02 82 01 01 .....

Addressing TOCTOU issue

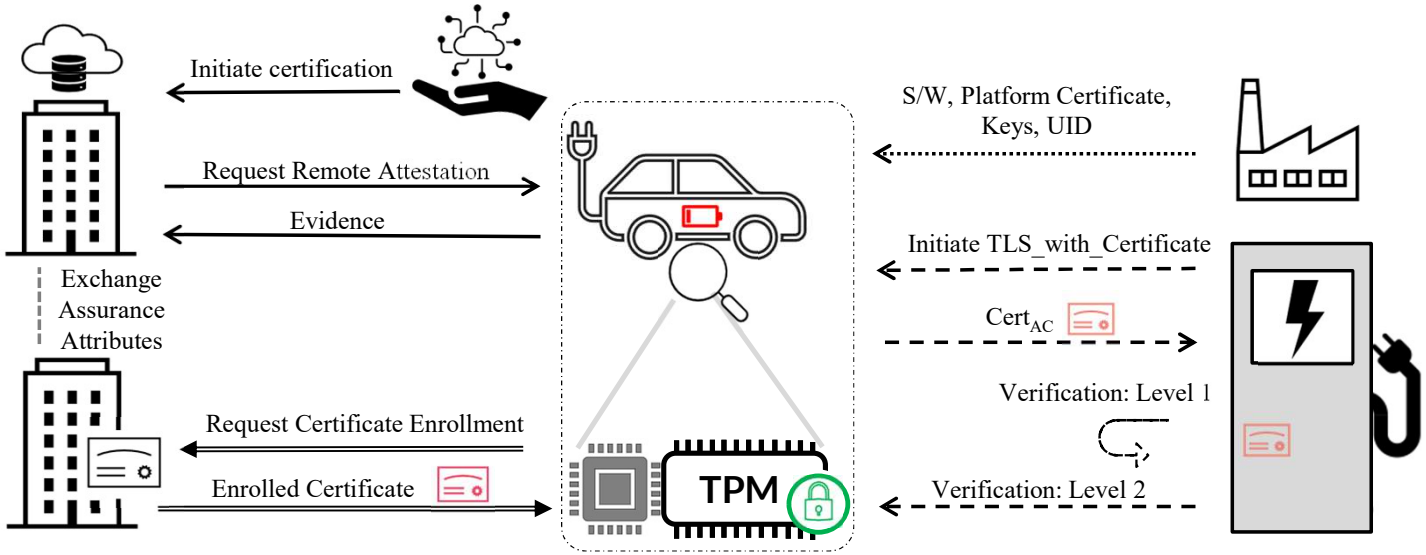
- Time-of-check Time-of-Use (TOCTOU) is a race condition between the time the devices was attested and the current state.
- Using TPM, an **attester** (IoT device) generates *integrity key* (**IK**)**,** an asymmetric keypair IK_{priv} and IK_{pub} , using the *PCRSelection* (hashes of software).
- The *PCRSelection* ensures that **IK** will not be valid if the software state of the device changes (a.k.a., TPM Sealing)
- IK is strictly connected with the state of IoT device and detects TOCTOU discrepancy if software is updated

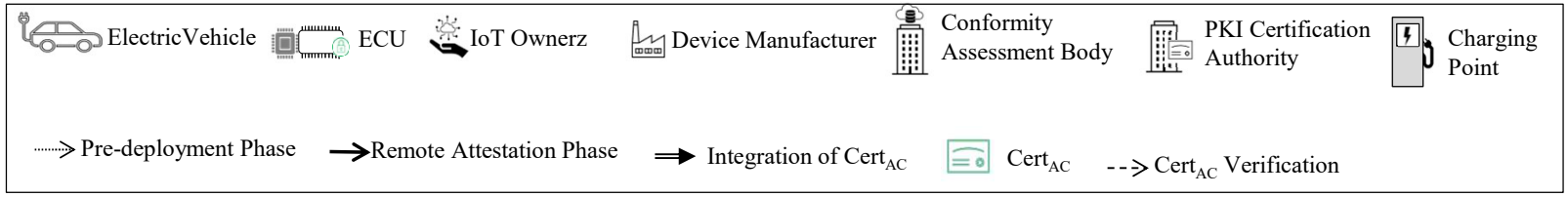
Realtime Verification of Assurance



13

AutoCert – The Process





Implementation & Evaluation

Proof-of-Concept implementation with

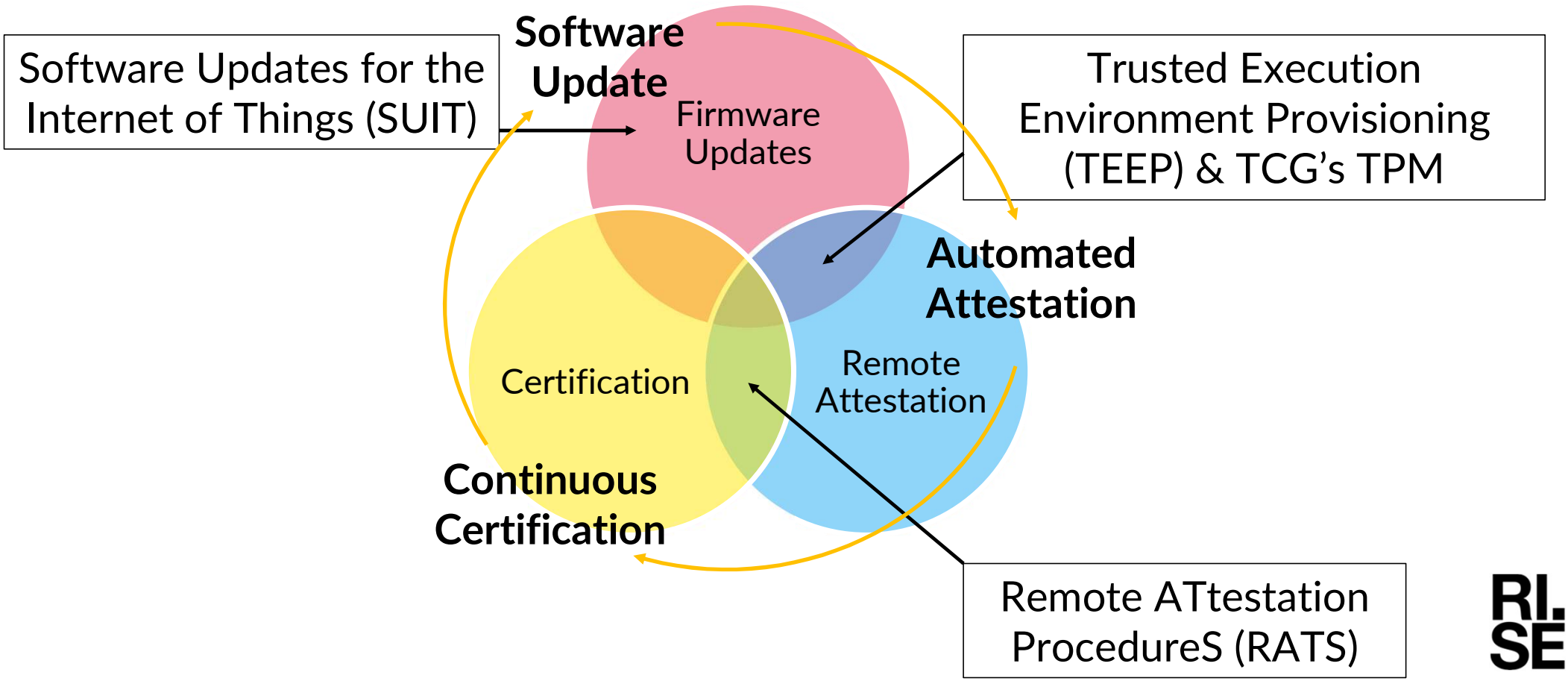
AutoCert: Automated TOCTOU-secure Digital Certification for IoT with combined Authentication and Assurance". In: *Computers & Security* journal (2023)

OPTIGA TPM Evaluation Kit (Infineon)

A result

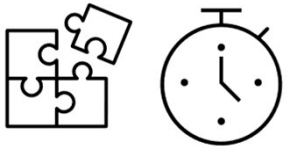
Average latency of each TPM function on the OPTIGA TPM evaluation platform.

New Standardization Efforts at IETF



Conclusion

- An IoT device software state can be automatically attested, verified, and certified
  - Provides TOCTOU security between remote attestation and certification
  - Combines IoT assurance with PKI digital certificate (Authentication-Assurance Certificate)
  - Remote attestation mechanism based on standards (RATS)
  - Standardized way for distribution of certificate (PKI)



Match b/w remote attestation & certificate Issuance, TOCTOU-secure

Avoid storing additional certificate

Standard compliance

VEDLIoT
Very Efficient Deep Learning in IoT

RI.
SE

Thanks

https://shahidaza.net