ASSURED

ASSURED VISION TOWARDS TRUSTWORTHY "SYSTEMS-OF-SYSTEMS"

ASSURED Webinar:
Towards Practical Solutions for Efficient and Scalable Attestation Capabilities

Dimitris Karras

UBITECH

31/05/2023

www.project-assured.eu

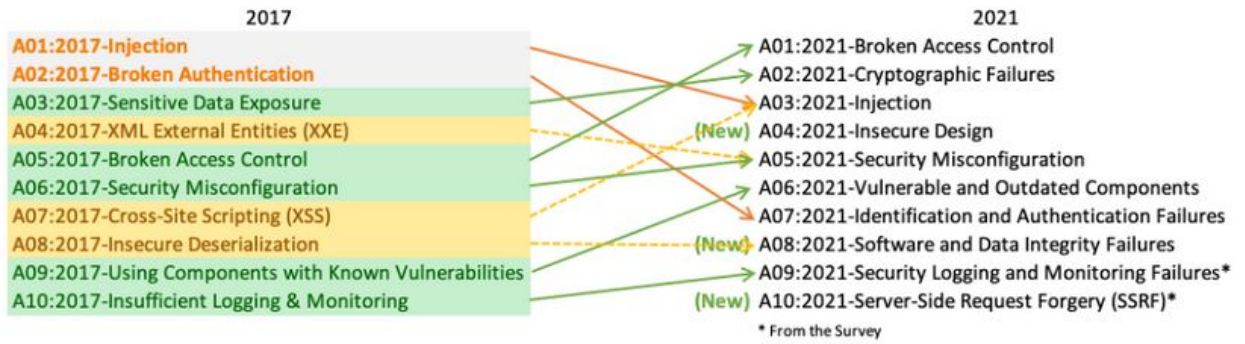
BACKGROUND AND MOTIVATION

As the demand for increasingly autonomous Cyber Physical Systems (CPSs) grows, so does the need for **certification mechanisms during runtime**.

- × Current methods towards validation require exhausting offline testing of every state scenario.
- ✔ Therefore, we aim to provide ***security and privacy guarantees for devices, as well as the system as a whole, during runtime!***

Novel assurance services are needed to ensure that operation does not put the systems or the people operating them in danger:

- Ensure **trusted execution** of (insecure) components
- Safeguard **code updates** against tampering
- Firmware and software **compliance** to execution policies



ENISA threat landscape report – top 10 threats

THE VISION OF ASSURED

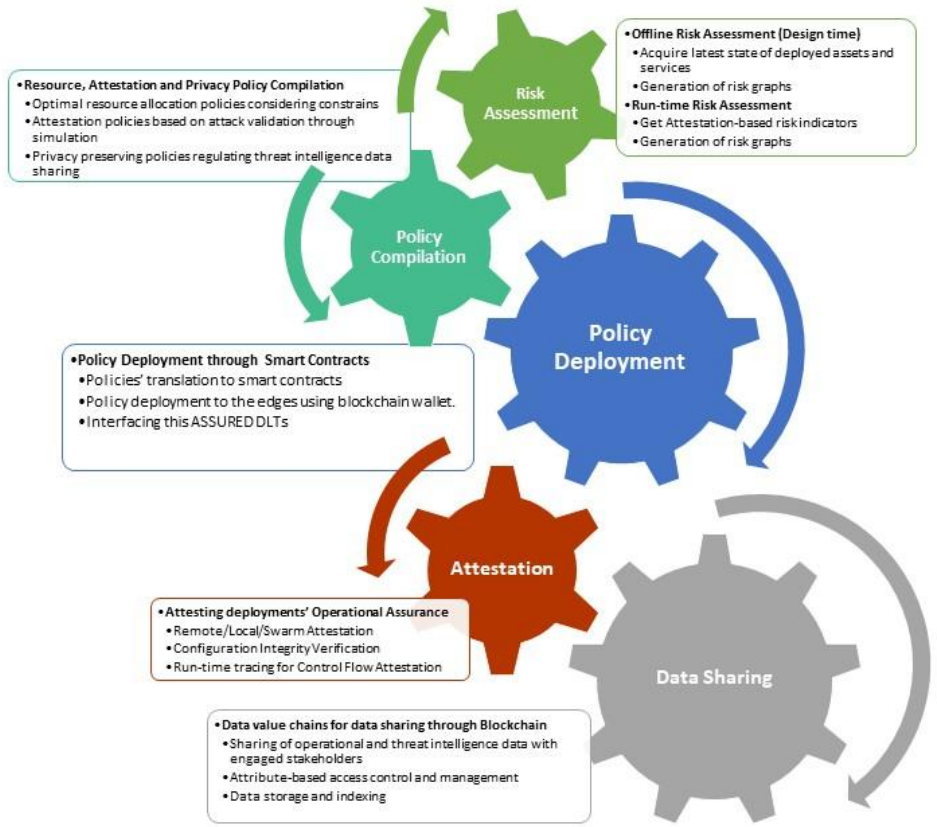
The core vision of ASSURED is the development of a complete framework that can provide **operational assurance** to large-scale Systems-of-Systems (SoS) comprising various **heterogeneous devices**, characterized by different **security and privacy requirements**.

Establishment of Trusted Service Graph Chains in next-generation "Systems-of-Systems" addressing **Security**, **Safety** and various levels of **Trustworthiness** for mixed-criticality services.

Adoption and implementation of the **Zero Trust** concept with the principle "*Never Trust, Always Verify*" for assuring vertical trust for all devices comprising the supply chain.

ASSURED RESEARCH IN TRUSTED COMPUTING, BLOCKCHAIN & LIGHTWEIGHT CRYPTO

Enhanced Operational Assurance	Increase trust to a device output by assessing its configuration & execution state – **Real-time tracing capabilities without impeding performance**
Risk Assessment	Identity risk interdependencies in a service graph chain that can affect the safety of the system
Threat Intelligence Information Sharing	Secure and auditable sharing of operational and attestation data only to authorized & authenticated devices & users – Useful for **Certification**
Decentralized Identity Management	How to ensure that each entity is the one that it claims to be – TC-based Wallet running at each user/device
Safety Zones Detection	Optimal Deployment of security (attestation) policies
Vulnerability Analysis	Protection of cyber-physical systems through run-time attack path analysis



ASSURED COMPONENTS

ATTESTATION ENABLERS

- Attest both the correct configuration & execution of a device
- Different types of attestation tasks depending on the requirements
- Control-flow Attestation, Configuration Integrity Verification, Direct Anonymous Attestation, Swarm Attestation
- Jury-based Attestation for resolving inconsistencies in the provided claims

Innovation:

- Lightweight attestation capabilities
- ML-based CFA
- Orchestration of the different attestation tasks depending on the policies (protection profiles)

RUNTIME TRACER

- Real-time tracing capabilities of the configuration state & control-flow graphs
- SW-based, HW-based, and hybrid
- Lightweight enough to operate in resource-constrained devices

Innovation:

- Does not affect software performance
- Non-intrusive

SSI WALLET

- Bridge for the secure management of cryptographic material & continuous authorization and authentication
- Following the SSI concept
- Capable of producing Verifiable Proofs for device attributes

Innovation:

- Protected under HW-based key (DAA)
- Merging of the SSI and trusted computing benefits

BLOCKCHAIN-BASED CONTROL

- Secure information exchange & data sharing
- Attribute-based Access Control
- Attribute-based Encryption
- Searchable Encryption

Innovation:

- Decentralized ABE
- **Certification capabilities** due to the auditable recording of all data transactions

ASSURED COMPONENTS

RISK ASSESSMENT

- Identification & Calculation of risk interdependency graph
- Based on definition of hw- & sw-assets from the system administrator
- Prerequisite for the calculation of optimized set of security policies

Innovation:

- Consider both **security & privacy** related vulnerabilities
- Attack Path Calculation

POLICY RECOMMENDATION

- Calculation of the optimized set of security policies
- Set of attestation policies
- Scheduling of attestation & computational tasks

Innovation:

- Multifactor constraint problem solving
- Different dimensions – convergence of security, safety, and resource

SECURITY CONTEXT BROKER

- Bridge for interacting with the Blockchain
- Deployment of attestation policies through smart contracts
- Attribute-based Access control capabilities

Innovation:

- Adoption of the gRPC concept for automatic dissemination of events
- Access control based on the use of Verifiable Credentials

ATTACK VALIDATION

- Virtual representation of the physical devices
- Processing of real-time system raw traces for attack path identification
- Simulation & Emulation of various attack vectors

Innovation:

- Device Behavioral Analysis
- Mutation Fuzzing & Concolic Testing

ENVISIONED USE CASES

ASSURED

SMART MANUFACTURING

- Accident prevention for humans working in tandem with machinery (robotic arms)
- Validation against a malicious user attempting modification
- Data integrity and trustworthiness for position of worker (equipped with RFID)

SMART AEROSPACE

- Need to increase the trustworthiness of all internal components of an aircraft
- Need for fast and secure SW updates
- Need for verification in the integration of new products and system level solutions
- Protection against security misconfiguration, vulnerable and outdated components

SMART CITIES

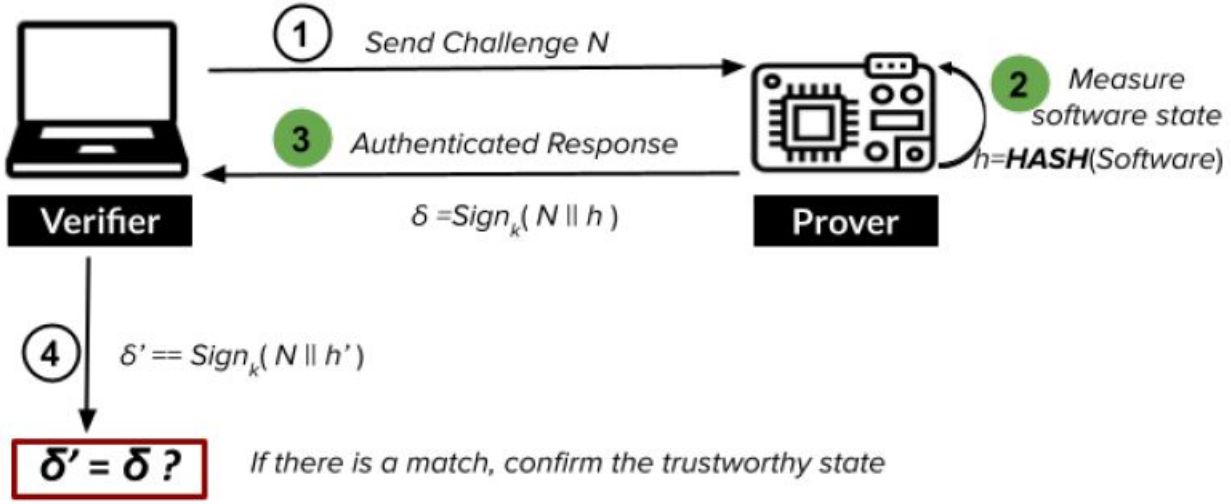
- Use of smoke and gas detection sensors, CCTV cameras
- Strong requirements for anonymity and privacy of users
- Strong authentication and authorization of various stakeholders when accessing sensitive information

SMART SATELLITES

- Collaborative execution of safety-critical processes by multiple satellites
- Lightweight authentication and secure communications
- Integrity of mission critical payloads and secure software updates

USE OF REMOTE ATTESTATION IN ASSURED

- Therefore, we need to provide mechanisms that are able to achieve **security and privacy requirements** in a wide variety of use cases and application domains!



- **Remote Attestation**: The method by which a Prover device authenticates the correctness of its configuration state and/or the execution of software processes, through the issuance of an attestation challenge by a Verifier and the provision of an appropriate response by the Prover.

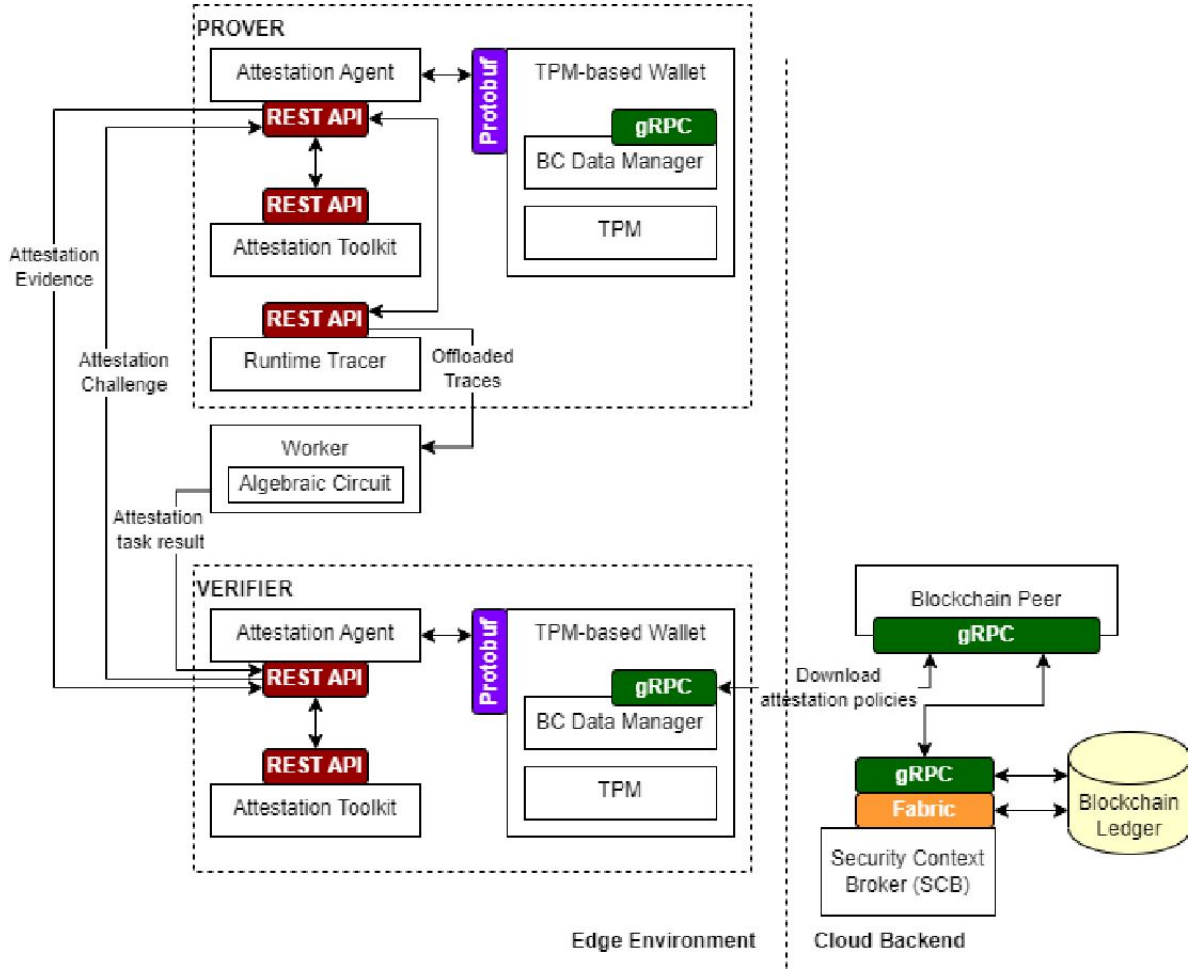
KEY FEATURES OF REMOTE ATTESTATION IN ASSURED

- Provision of high **security, privacy, and trustworthiness guarantees** throughout the operational lifecycle of a device through the use of **trusted computing** technologies.
- Design and implementation of **local attestation mechanisms** for the verification of the correct state of a device locally, by setting up **key restriction usage policies** as part of the secure enrollment process.
- Towards privacy-preserving attestation, this also enables the Prover to only send a signature to the Verifier to perform attestation without disclosing the state of the Prover.
- ASSURED is the first project of its kind to provide **Machine Learning-assisted CFA**, in order to detect deviating behavior of software processes.
- Combination of attestation with **certification and auditability** features through Blockchain technologies, since all attestation policies are depicted as **smart contracts**, deployed and enforced through the ledger, and **attestation reports** are stored afterwards.

HIGH-LEVEL ARCHITECTURE

Core components:

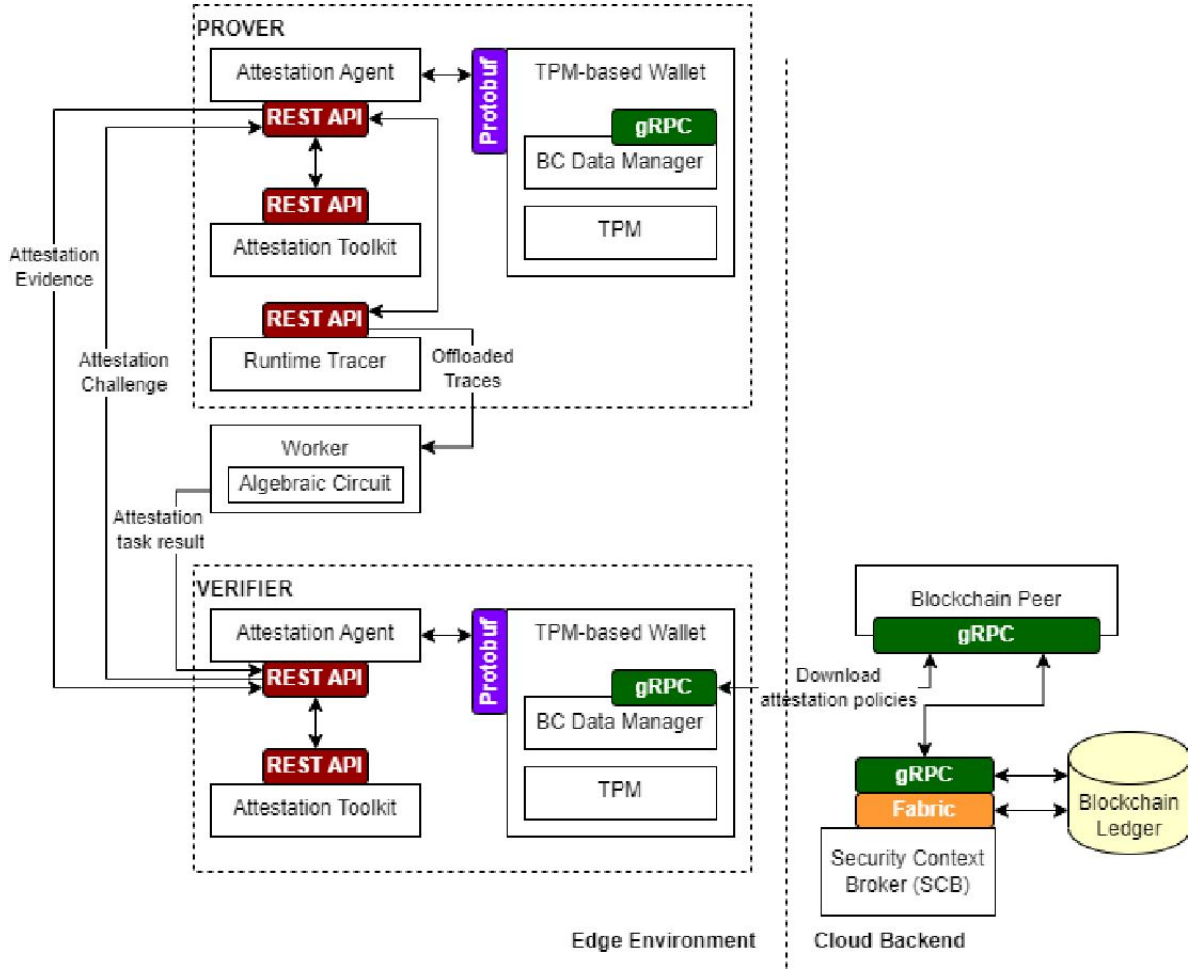
- **Prover:** Device that proves correctness of configuration state or SW execution. Contains:
  - **TPM-based Wallet:** Storage of attestation keys and cryptographic material
  - **Runtime Tracer:** Collection of attestation evidence (configuration, control flow)
  - **Attestation Toolkit:** Execution of remote attestation logic
  - **Attestation Agent:** Orchestration of attestation process, communication with Wallet, Tracer, Toolkit. Interfacing with REST API, Protobuf.
- **Verifier:** Device that verifies correctness of Prover. Contains the same components. Downloads policies from the ledger, recording of attestation reports
- **Worker:** Offloading of verification tasks in zero knowledge (CEA)



HIGH-LEVEL ARCHITECTURE

Core components:

- **Blockchain Ledger**: Deployment of attestation policies, attestation reports
- **Blockchain Peer**: Intermediate party between device and ledger
- **SCB**: Responsible for the orchestration of various actions:
  - Zero-touch configuration of device attestation keys
  - Maintenance and approval of acceptable node configuration
  - Secure device enrollment
  - Storage and retrieval of attestation reports
  - Device secure update during runtime



ASSURED Attestation Toolkit

- **Configuration Integrity Verification (CIV):** Verifies correctness of device configuration
- **Control Flow Attestation (CFA):** Verifies correctness of software process execution – Core Artefact
- **Direct Anonymous Attestation (DAA):** Enables privacy-preserving attestation, enhanced with traceability and revocation features.
- **Swarm Attestation:** Simultaneous attestation of multiple devices with novel signature features, using the above attestation mechanisms (CFA, CIV, DAA).
- **Revocation capabilities:** Capability for the revocation of the DAA credential of a device that is suspected to be compromised.

MOVING FORWARD – NEW CHALLENGES

ASSURED has taken major steps forward regarding the convergence of security and safety in supply chains and embedded systems, yet new challenges are brought forth:

- **Distributed:** Next-generation systems must be seen as inherently and increasingly Federated Safety-Critical Systems that are not owned by a single entity.
- **Bottom Up:** Data and system components must be in a position to make strong statements about their runtime integrity.
- **Defensive:** Consideration of strong adversaries that can manipulate interaction with the secure element, and design of more generic attestation schemes.
- **Safety:** Interdependent requirements characterized as complex, multi-dimensional, transversal, uncertain, and with different potentially contradictory requirements.

THANKS

PROJECT-ASSURED.EU

@Project_Assured

ASSURED project is funded by the EU's Horizon2020 programme under Grant Agreement number 952697