ASSURED VISION TOWARDS TRUSTWORTHY “SYSTEMS-OF-SYSTEMS” AND SECURE DATA SHARING

ASSURED Webinar:
ASSURED CYBERSECURITY AND INSIDER THREATS:
BLOCKCHAIN-EMPOWERED MOBILE EDGE INTELLIGENCE
FOR SECURE AND SUSTAINABLE COMPUTING

Dimitris Karras

UBITECH

11/07/2023

www.project-assured.eu

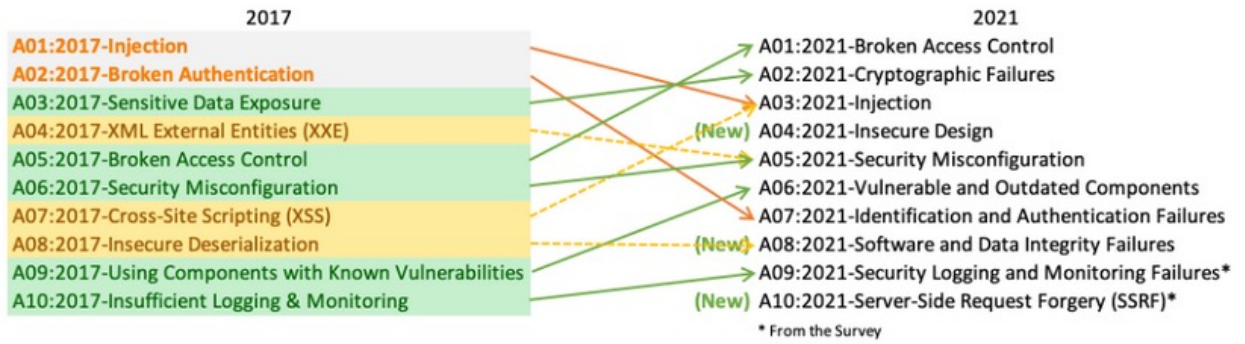
BACKGROUND AND MOTIVATION

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

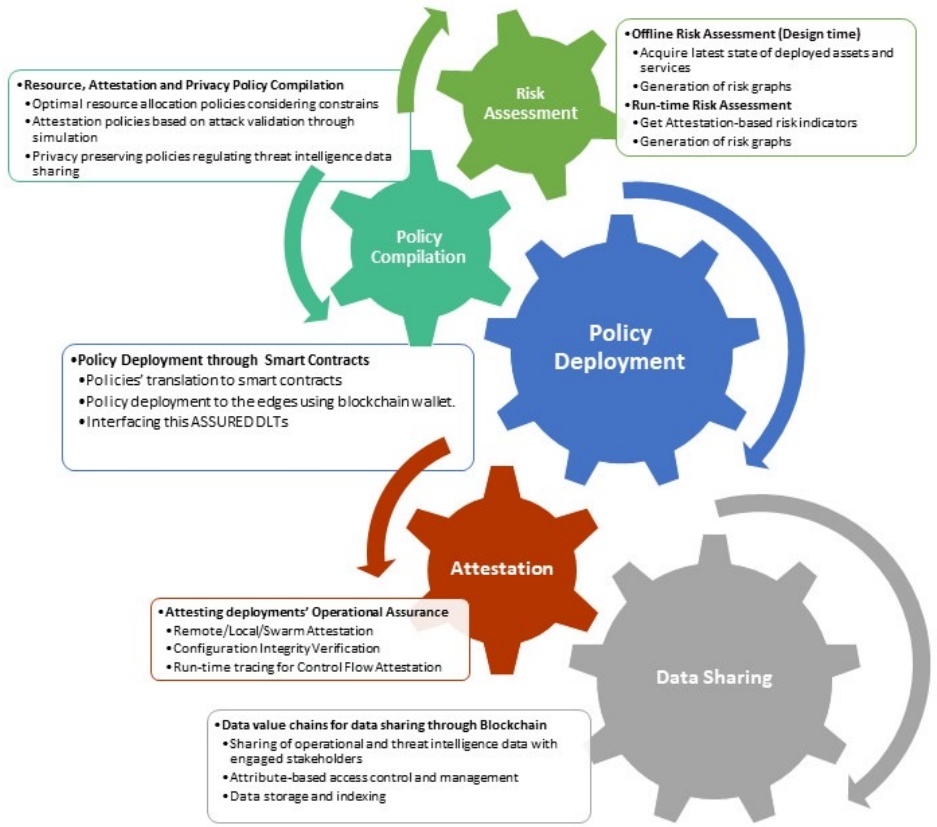
The core vision of ASSURED is the development of a complete framework that can provide **operational assurance** to large-scale Systems-of-Systems (SoS) comprising various **heterogeneous devices**, characterized by different **security and privacy requirements**.

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

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

MOTIVATION FOR USE OF BLOCKCHAIN

Blockchain: a decentralized and distributed ledger, where a set of blocks containing recorded data are linked between them in a secure manner.

Why do we use Distributed Ledger Technologies (DLT) in ASSURED?

- **Data sharing** is a cornerstone of ASSURED. DLTs provide necessary features that guarantee the level of trustworthiness required for **robust**, **secure**, and **privacy-preserving** data transactions.
- Enables ASSURED to build a **flexible and expendable data sharing network**. Easy to add new users following a secure enrollment process.
- The use of **smart contracts** in tandem with DLTs enables the coordination of activities required for data sharing, governance of the execution of attestations, clear definition of flow of interactions between Provers and Verifiers.

BLOCKCHAIN-RELATED FUNCTIONALITIES OF ASSURED

The Blockchain Infrastructure in ASSURED is used for various purposes:

- To ensure **certifiable** and **auditable** transactions with a high level of **trustworthiness** through the use of **smart contracts**
- To implement identity management mechanisms in tandem with the **TPM-based Wallet** to enable devices to interact with the Blockchain following the notion of **Self-Sovereign Identities (SSI)**
- To enable the use of the Wallet in tandem with the ASSURED lightweight crypto schemes, **Attribute-Based Access Control (ABAC)**, **Attribute-Based Encryption (ABE)**
- To enable secure storage of results of attestation processes in the form of **attestation reports** in order to enable **data and threat intelligence sharing**
- To enable querying for the stored data through the **Dynamic Symmetric Searchable Encryption (DSSE)** scheme

ASSURED BLOCKCHAIN COMPONENTS (1)

The ASSURED framework contains the following components related to the Blockchain Infrastructure:

- **Blockchain Peer:** Hosts chaincode to be executed and interacts with edge devices through TPM-based Wallet for supporting execution of smart contracts, recording, and sharing of attestation reports.
- **Private ledger:** Storage of attestation reports, pointer to ABE-encrypted off-chain attestation data, data associations
- **Public ledger:** Storage of keyword lists that can be used for users to query for attestation reports and data.
- **API layer**: Provides a gateway to bridge connections and communications between devices and Peers (transactions, query requests)
- **Ordering service**: Responsible for organizing submitted transactions in order and creating new blocks.

ASSURED BLOCKCHAIN COMPONENTS (2)

- **Security Context Broker (SCB):** Acts as a trusted bridge between (trusted) Blockchain network and (untrusted) outside world.
- **Membership Service Provider (MSP):** Verifies, at a high level, that a device is permitted to access a ledger.
- **TPM-based Wallet:** Provides strong device authentication and enables interactions between devices and ledger.
- **Smart Contract Composition Engine:** Responsible for receiving optimal set of attestation policies by Policy Recommendation Engine and converting them into form that can be executed by target device(s).
- **Privacy Certification Authority (CA):** Responsible for verifying attributes demonstrated by device during its enrolment to the Blockchain network.
- **Blockchain Certification Authority (CA):** Provides necessary certificate for the TPM-based Wallet to access the ledger.

BLOCKCHAIN-RELATED SCHEMES

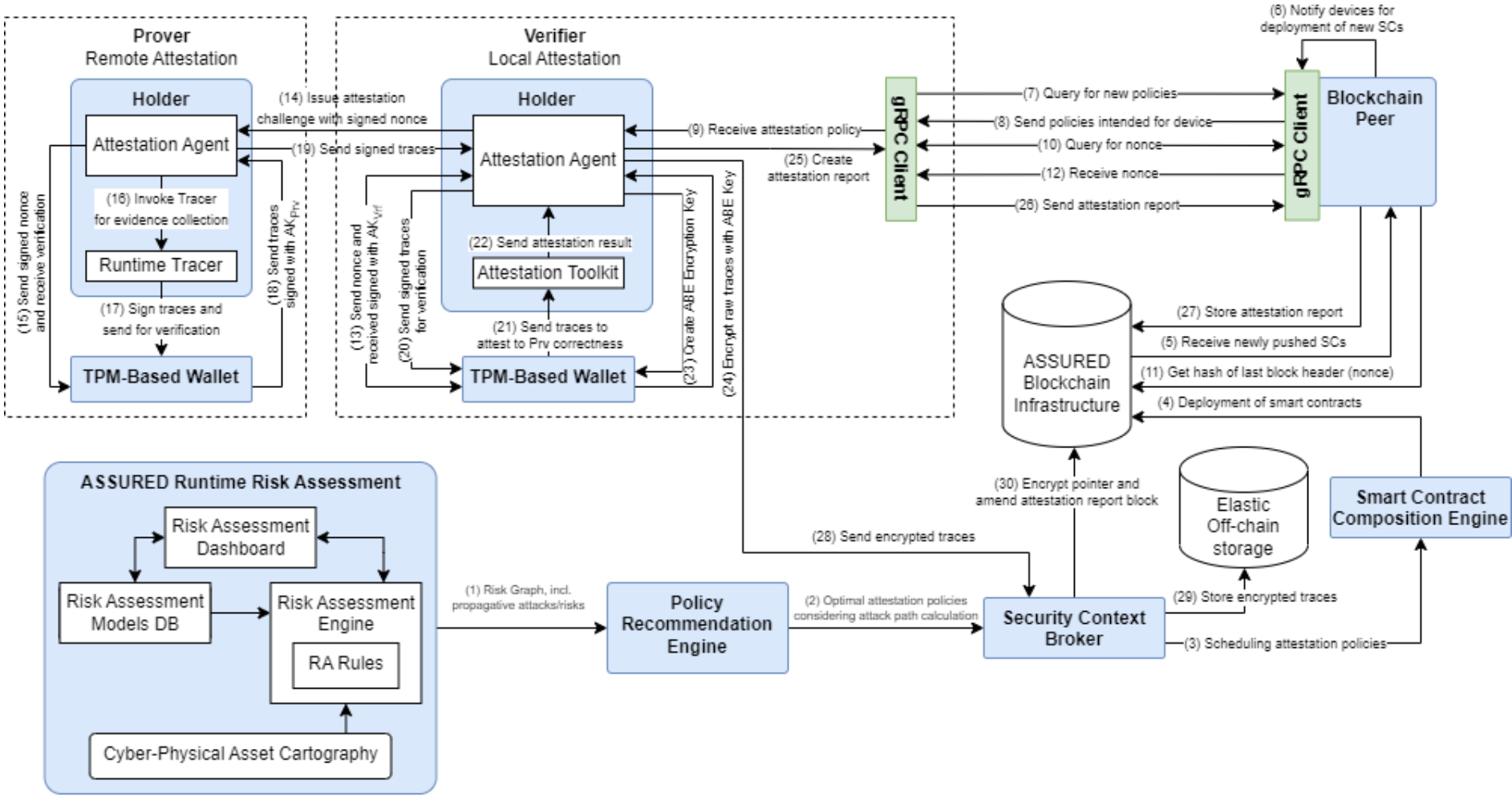
The ASSURED framework contains various schemes that leverage the Blockchain Infrastructure:

- **Secure Enrollment:** Creation of Blockchain certificate that enables device interactions with the ledger, cryptographic material and keys that enable use of lightweight crypto schemes.
- **Two-layer access control:**
  - *Membership Service Provider (MSP):* Verifies whether device has access permissions to a particular ledger.
  - *Attribute-Based Access Control (ABAC):* Verifies granularity of access through creation of a Verifiable Presentation (VP).
- **Attribute-Based Encryption (ABE):** Encrypts operational data or raw traces as attestation data so they can be stored in Elastic off-chain storage facility and can only be decrypted by devices that can demonstrate possession of required attributes through a VP.
- **Dynamic Symmetric Searchable Encryption (DSSE)**: Enables querying for attestation reports and data stored off-chain, based on a set of keywords on the public ledger.. Device must demonstrate required attributes VP in order to obtain access to requested data.

POSITIONING OF BLOCKCHAIN IN ASSURED

Blockchain as pat of the ASSURED workflow:

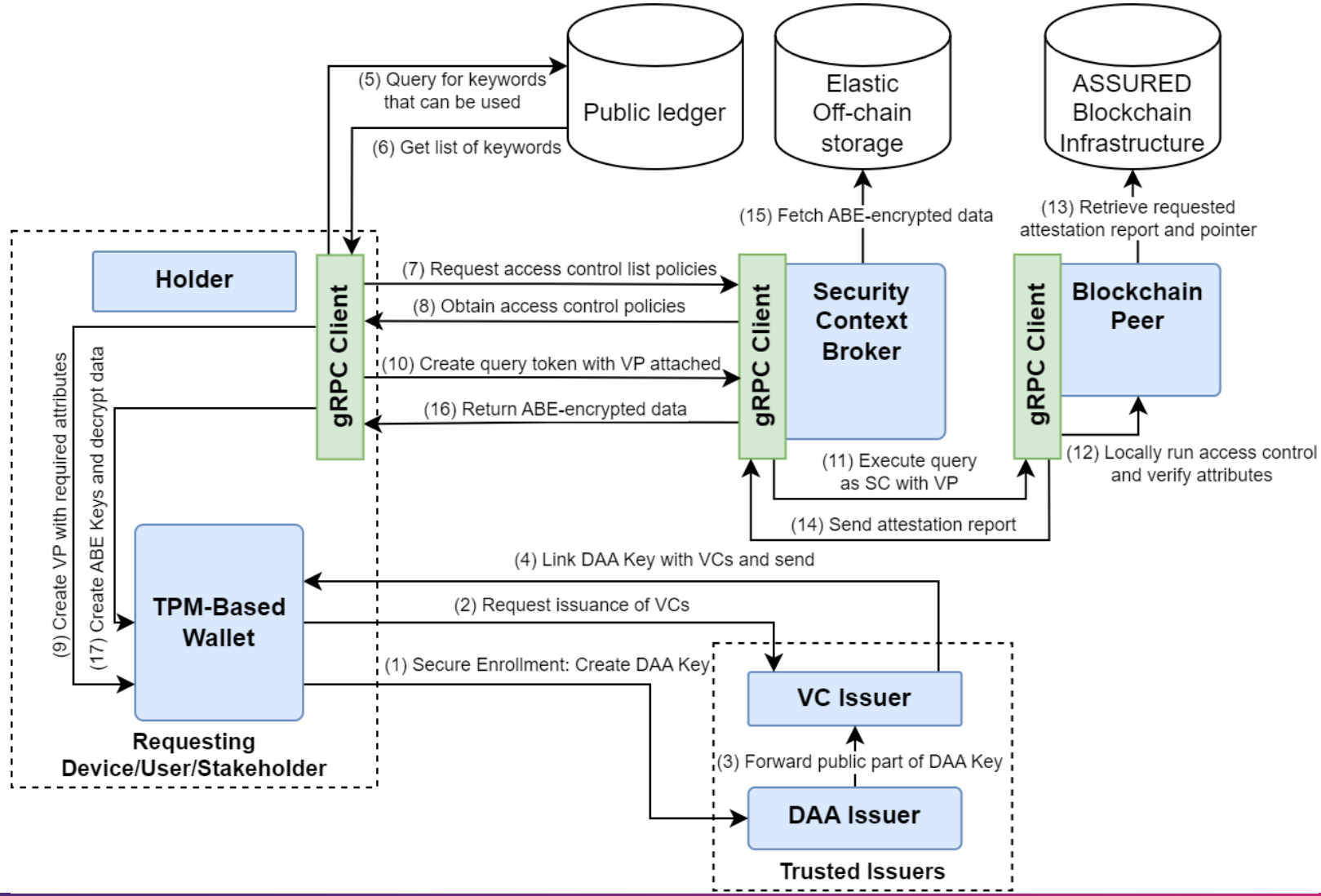
- Security policies are converted to **smart contracts (SCs)** and stored on the ledger.
- SCs are pushed to the **Blockchain Peer**, and devices are notified of their deployment. Device receives policy through gRPC client.
- Attestation task is performed. Result is sent to ledger through BC Peer as **attestation report.**
- Attestation evidence is ABE-encrypted and stored off-chain. SCB receives **location pointer** and amends corresponding attestation report. Keyword list is stored on **public ledger**.



QUERYING FOR ENCRYPTED DATA

Querying for attestation reports and ABE-encrypted data:

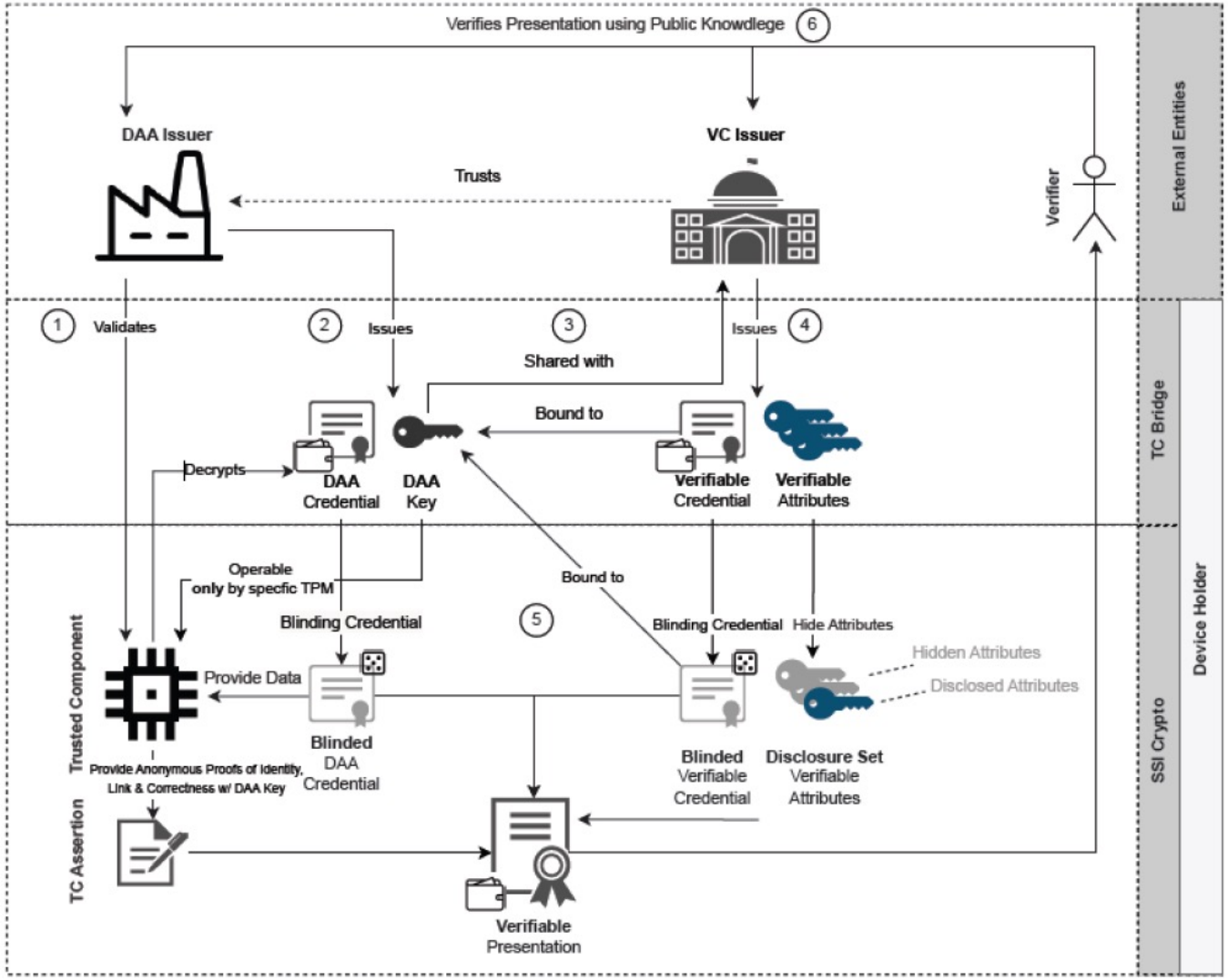
- **Secure enrollment:** Device uses TPM-based Wallet to issue VCs and create DAA Key (linked between them).
- Device queries **public ledger** for available keyword list for querying.
- Device selects keyword and SCB retrieves **access control policy** with required attributes.
- Device creates **VP** with required attributes and sends it to SCB.
- SCB verifies correctness of VP. If correct, attestation report and data is returned and decrypted



THE ASSURED TPM-BASED WALLET

Functionalities provided by the ASSURED TPM-based Wallet:

- **Device Binding and Key Registration**: Use of a hardware-protected key, build into the device TPM. Key restriction usage policy guarantees that only this device can use the key. Created during secure enrollment process.
- **Obtaining a Verifiable Credential (VC):** Issued by the Privacy CA and contains device attributes. Binded to the Wallet.
- **Obtaining a Verifiable Presentation (VP):** Created by the Wallet and containing a subset of attributes contained in VC. Used in ABE, ABAC, DSSE schemes to prove possession of required device attributes.



KEY TAKEAWAYS AND OPEN TOPICS

ASSURED Blockchain services offer significant benefits, but constraints need to be considered:

- Designed schemes are **agnostic to the type of Blockchain framework used**, but implementation was performed using **Hyperledger Fabric**. *How do implemented schemes behave using different Blockchain infrastructures?*
- Adoption of Blockchain Peer is a milestone towards creation of **secure oracles** to bridge the gap between on-chain and off-chain data. To this end, *we performed enhancements to the Go interfaces to facilitate communications with the TPM.*
- Moving towards the adoption of **Self-Sovereign Identities (SSI)** through the use of decentralized identifiers in accordance with the principle of selective disclosure. Supported through TPM-based Wallet.

THANKS

PROJECT-ASSURED.EU

@Project_Assured

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