ASSURED

Enhanced DAA flavors and Trust Revocation in Distributed Environments

Dimitris Papamartzivanos
Stefanos Vasileiadis

Digital Security & Trusted Computing Group

ASSURED Scientific Workshop

Darmstadt, Germany | April 25-26, 2023

www.project-assured.eu

Security & Privacy Enablers

2019

FIDO U2F with TPMs

- ✓ Privacy and Anonymity
- ✓ Proof of Knowledge
- ✓ Direct Anonymous Attestation

2020

Configuration Integrity Verification

- ✓ Multi-tenant Virtual Network Functions (VNFs)
- ✓ Protection even if a tenant/container gets compromised
- ✓ Zero knowledge features for "hiding" the attestation evidence

ESORICS 2020

2021

Efficient and Privacy-preserving Revocation

- ✓ DAA
- ✓ Zero Trust Model
- ✓ Use case in VANETs

WiSec 2021, TDSC 2023

2022

Hardware RoT for SSI's

- ✓ TPM-based Wallet for VC and VP Management
- ✓ HW-based Key protection
- ✓ Proof that the Wallet that produced a VC belongs to the Holder
- ✓ Proof that the Wallet is not compromised

EuroS&P 2022

2022

Secure Element in Blockchain Network

- ✓ Decentralized Attribute-based Access Control
- ✓ Efficient Verification
- ✓ TSS in GO

2022

Zero knowledge Attestation

- ✓ Privacy preservation of attestation evidence
- ✓ Both CIV and CFA
- ✓ Weakening Verifier's trust assumptions

ARES 2022, AsiaCCS 2023

—> Future

Holistic Attacker Model

- ✓ TPM Command Injection

Instantiation in safety-critical application domains

- ✓ Connected Vehicles, Healthcare, Programmable Network Infrastructures

Formally verified security controls on RISC-V architectures

Sustainable Security

- ✓ QR TPM

What's been going on

DAA and Challenges

- Trust computing provides a RoT to prove devices are in a “trustworthy” state.
- Schemes should offer user-controlled security and privacy-preserving
- DAA is an anonymous signature scheme for the purpose of computer platform attestation whilst preserving platform anonymity
- The efficient revocation of trust of an existing member who is no longer legitimate is an important and challenging subject for DAA

DAA and Challenges

- Especially in user-centric and/or safety-critical applications strong requirements are posed:
  - Anonymity
  - Pseudonymity
  - Unlikability
  - Unobservability
- Revocation policies for removing misbehaving nodes from the network when using pseudonym schemes require the resolution of participant's long-term identified.
- In order to address the need for anonymity and accountability in highly distributed environments we need to search for decentralized approaches that shift trust from the infrastructure to the edges.

Enhanced DAA Flavors

- Enhanced DAA with revocation for distributed environments
- Attribute-based DAA (DAA-A) creating Verifiable Presentations for privacy-preserving SSI management.
- Decentralized Attribute-based encryption using DAA key for device state provenance

ASSURE

Secure Enrollment

Key Restriction Usage Policies

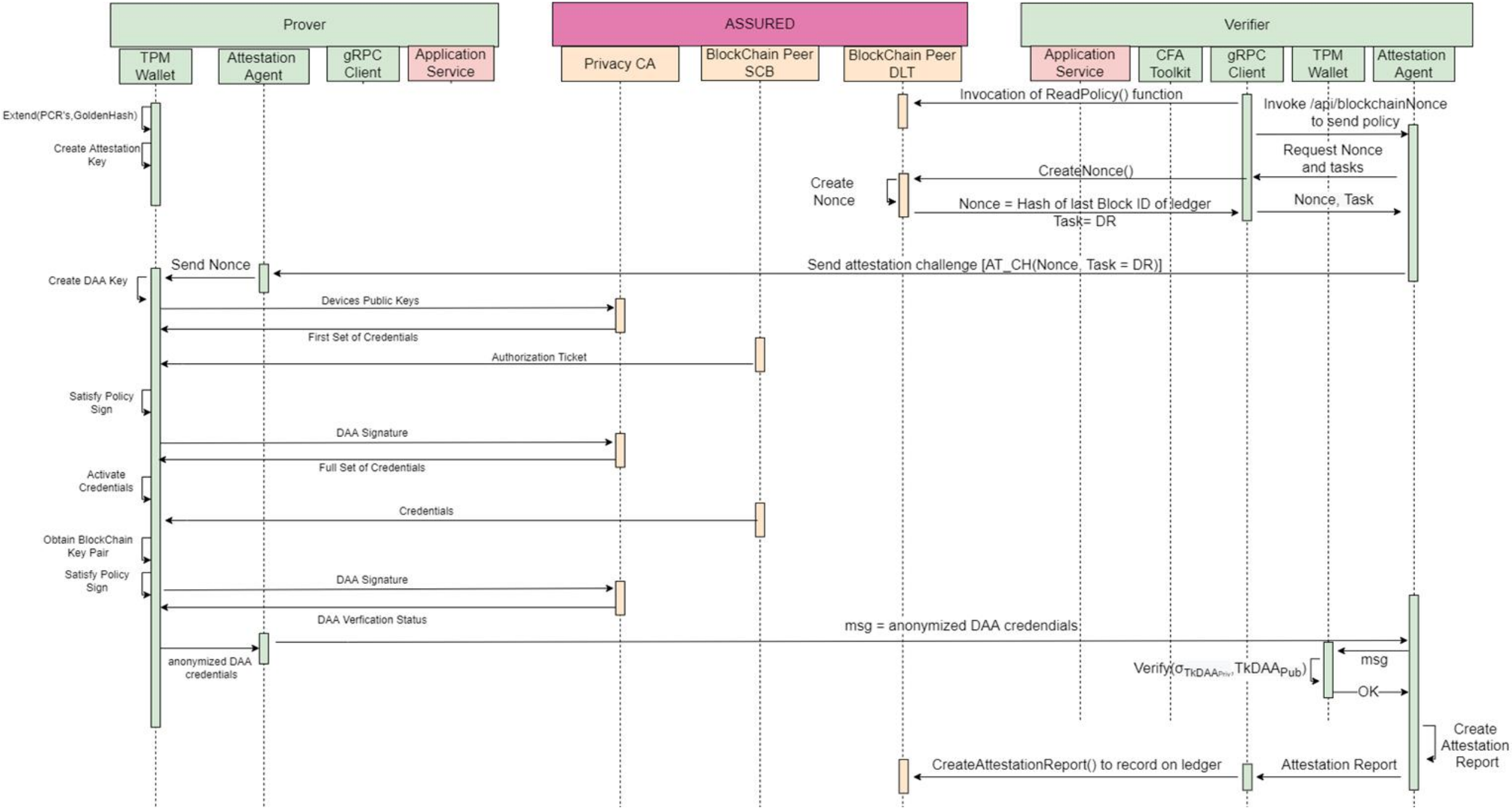
As the TPM is accessible from everyone who has access to the device we need a way to protect the use of our cryptographic keys.

For this purpose we use key restriction usage policies.

- ✓ A key restriction usage policy comes from a trusted third party.
- ✓ Dictate a correct/pre-determined state of the device.
- ✓ Provide proof during runtime for the state of the device.

Secure Enrolment

- **In the concept of the ASSURED project a secure enrolment protocol is designed for the secure creation and binding of keys.**
  - Every device that wants to participate in the network must undergo this procedure.
  - A trusted 3rd party entity (SCB in ASSURED) constructs an authorization ticket using the expected security metrics of the tracer for each device.
  - These metrics are stored to the platform configuration registers to be attested during runtime.
  - The Secure Enrolment is completed by the Privacy CA with which the device collaborates to create the DAA key.


Prover
ASSURED
Verifier
TPM Wallet
Attestation Agent
gRPC Client
Application Service
Privacy CA
BlockChain Peer SCB
BlockChain Peer DLT
Application Service
CFA Toolkit
gRPC Client
TPM Wallet
Attestation Agent
Extend(PCR's,GoldenHash)
Create Attestation Key
Invocation of ReadPolicy() function
Invoke /api/blockchainNonce to send policy
Request Nonce and tasks
CreateNonce()
Create Nonce
Nonce = Hash of last Block ID of ledger
Task= DR
Nonce, Task
Send Nonce
Send attestation challenge [AT_CH(Nonce, Task = DR)]
Create DAA Key
Devices Public Keys
First Set of Credentials
Authorization Ticket
Satisfy Policy Sign
DAA Signature
Full Set of Credentials
Activate Credentials
Credentials
Obtain BlockChain Key Pair
Satisfy Policy Sign
DAA Signature
DAA Verfication Status
msg = anonymized DAA credendials
anonymized DAA credentials
msg
Verify($\sigma_{TkDAA_{Priv}}$, $TkDAA_{Pub}$)
OK
Create Attestation Report
CreateAttestationReport() to record on ledger
Attestation Report

Key Restriction Policies Update

For our security schemes to be viable in a real case scenarios we need to provide a secure way for the device to get updated.

- A trusted 3rd party needs to construct a fresh authorization ticket specifically created for the state of the updated device.
- The new security metric will be stored again in the Platform Configuration Registers.

Attestation On Runtime

When challenged the Device:

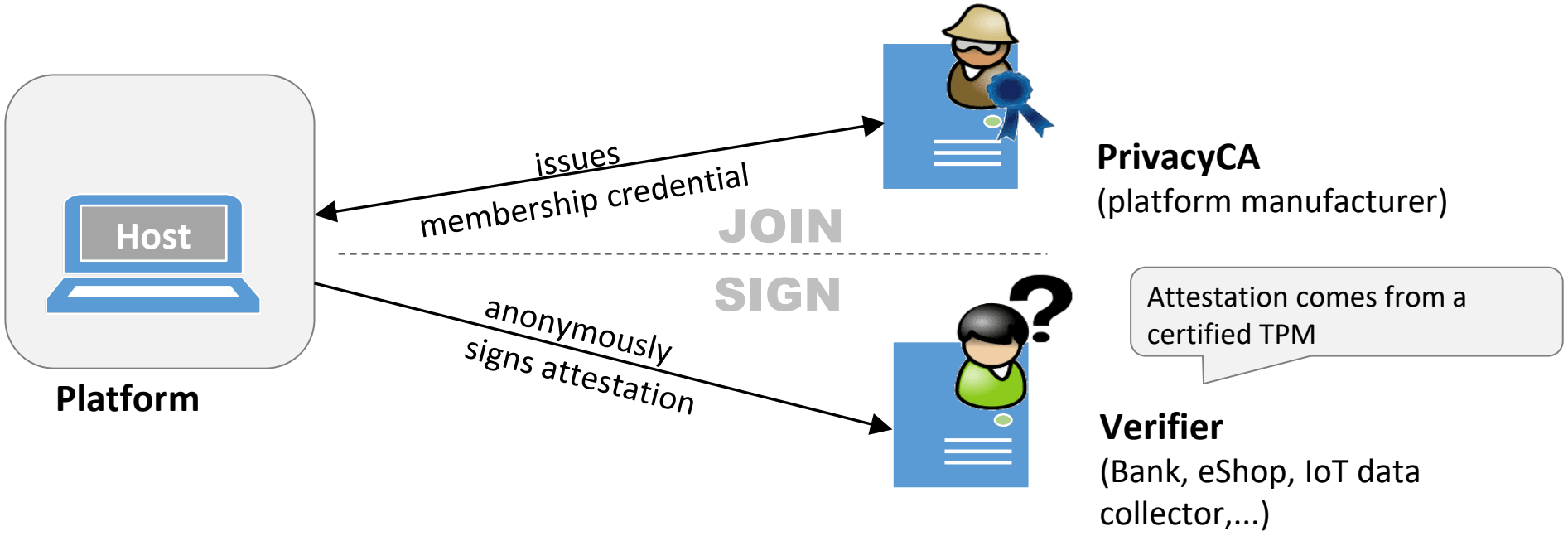
1. Loading from the Platform Configuration Registers the hashed representation of a “healthy” device.
2. Request from the tracer the live configuration of the attested binary.
3. Compute the real time representation of the device and go through a verification procedure against the authorization ticket provided by the 3rd trusted party

If the Verification is successful the TPM can sign the attestation data.

Direct Anonymous Attestation

A special kind of group signatures that uses blinded credentials, authorized by a certification authority, to anonymously sign data.

- Main Research Topics
  - Attribute Based DAA
  - Enhanced DAA with revocation capabilities



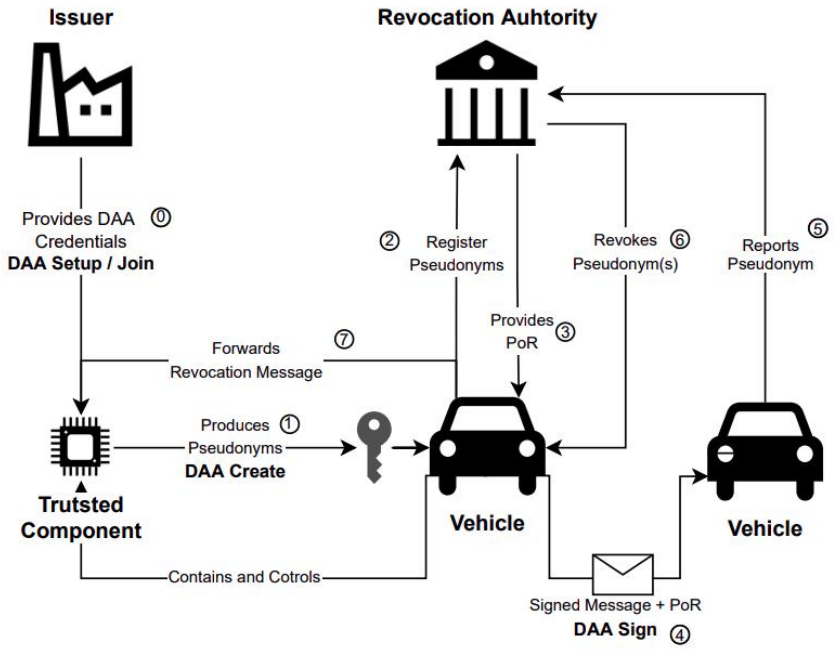
Enhanced Direct Anonymous Attestation

During JOIN phase of the DAA key creation we leverage the Non-Volatile memory of the TPM to link its content with the DAA key.

- After the initialization of the NV RAM of the TPM on a non-revoked state, the NV RAM gets locked from every party apart from the Revocation Authority.

The representation of the NV index is registered to the Revocation Authority.

- Upon detection of misbehavior:
  - The Revocation Authority uses the registered NV Index representation and changes the content of the NV RAM to a revoked state making the key unusable.



Experimentation Results

Phase	Result (Mean Value)
Authorization Index Creation	0.614
Revocation Index Creation	0.25
Final Policy Creation	0.062
Revocation Index Activation	1.109
Revocation	0.812

- Experimentation Set Up
  - Hardware TPM SLB9672
  - Raspberry PI 4 8GB
  - DAA Key and 63 Pseudonyms
  - Full implementation with pytss

THANKS

PROJECT-ASSURED.EU

@Project_Assured

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

Enhanced Direct Anonymous Attestation