SECURE IDENTITIES FOR RENEWABLE ENERGY SOURCES THROUGH SELF-SOVEREIGN IDENTITY AND ATTRIBUTE-BASED ACCESS CONTROL

Moritz Volkmann, Sascha Kaven, Shashank Tripathi, Volker Skwarek
Hamburg University of Applied Sciences, RTC CyberSec

HAW HAMBURG
FTZ CyberSec

RQ: How can an identity and access management (IAM) framework for RES in energy trading using Self-Sovereign Identity (SSI) and Attribute-Based Access Control (ABAC) be designed to ensure privacy and security?

RESEARCH GAP

HAW HAMBURG

- Existing measures for smart grid security are incomplete
  - Reliability of prosumers has to be ensured
  - Delivery and consumption have to be reliable
- Rising identity-related attacks in P2P energy trading
  - About 1200 CVEs with improper authentication in last four years

Smart grid decentralization needs tailored cybersecurity solutions

OUR CONTRIBUTION

HAW HAMBURG

- **Privacy-by-design Identity and Access Management (IAM) framework** for prosumer and RES identity management
- Utilization of **SSI Verifiable Credentials (VCs)** with blockchain technology for identity and certificate management
- **ABAC for fine-grained and situation-dependent trade authorization**

SECURITY-BY-DESIGN APPROACH

HAW HAMBURG

Security-by-design: Designing a system based on **security principles** and building measures to protect **security assets**

Security assets (CIA triad):

Confidentiality:

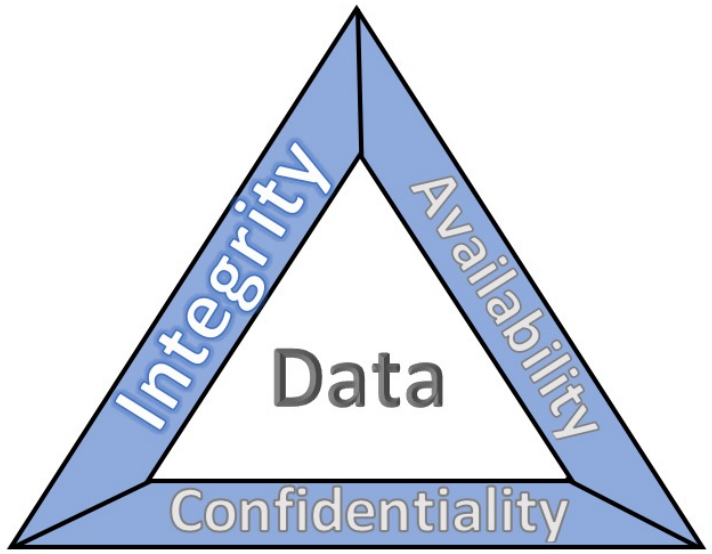
data sniffing, phishing attacks

Integrity:

false data injection attacks, replay attacks

Availability:

denial-of-service attacks

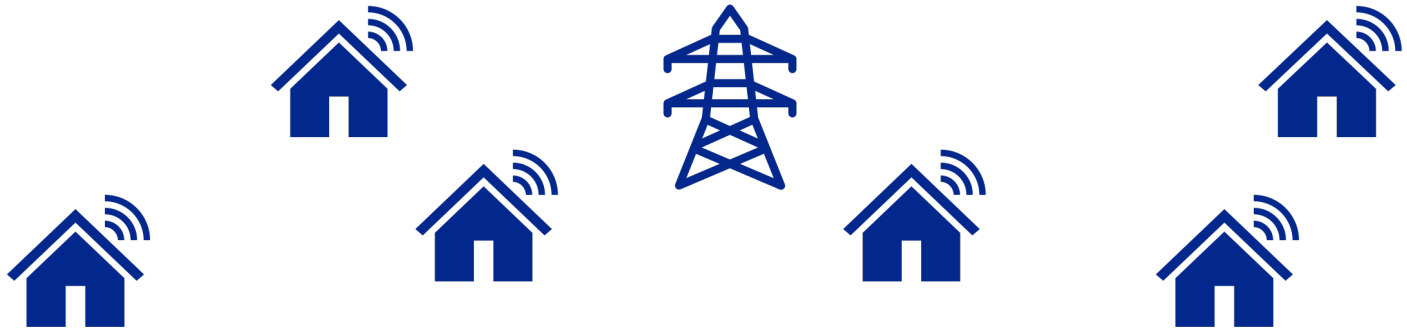


CIA triad according to NIST 1800-26A

Management Plane

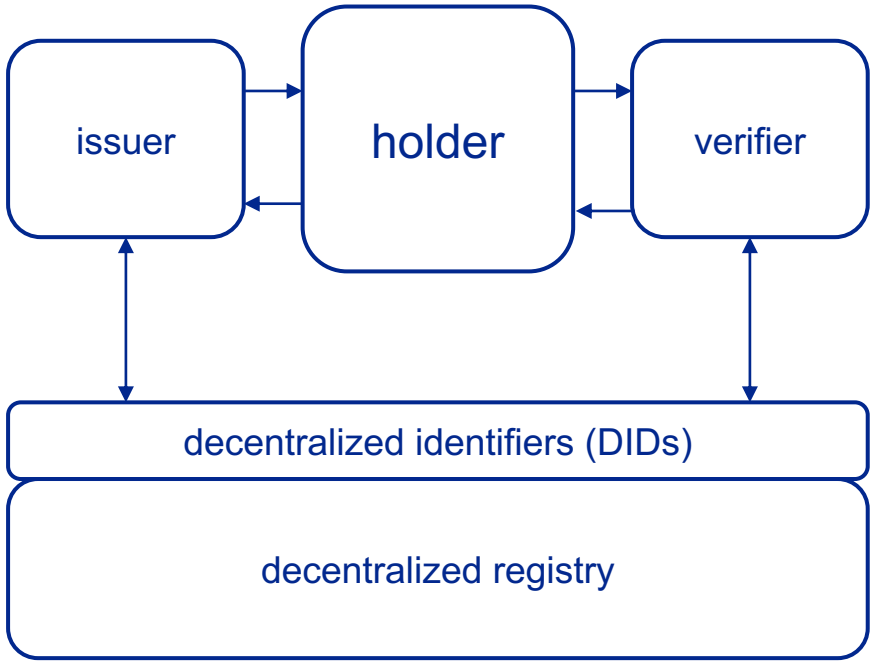
Control Plane

Data Plane

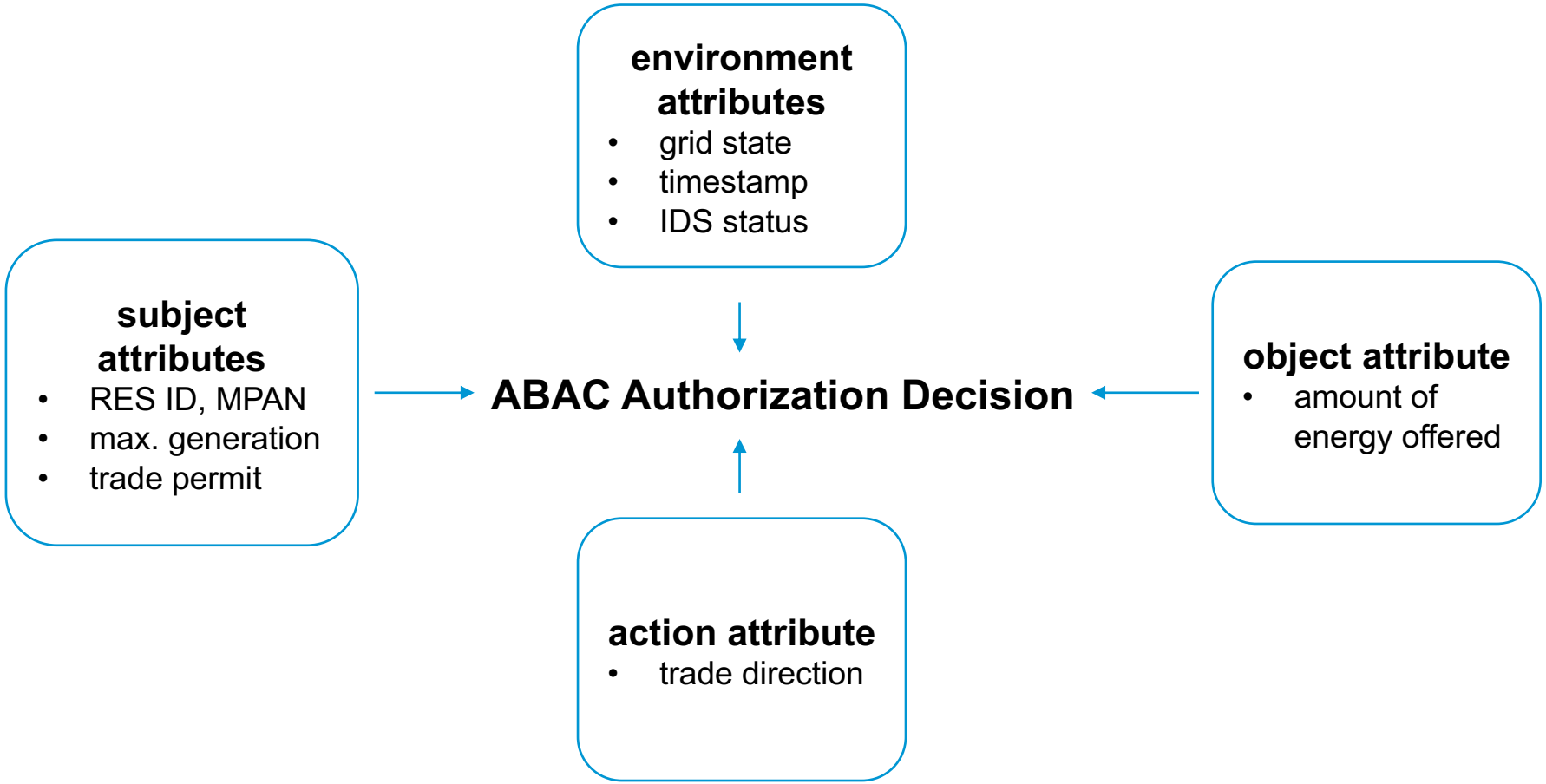


SSI IDENTIFICATION AND AUTHENTICATION

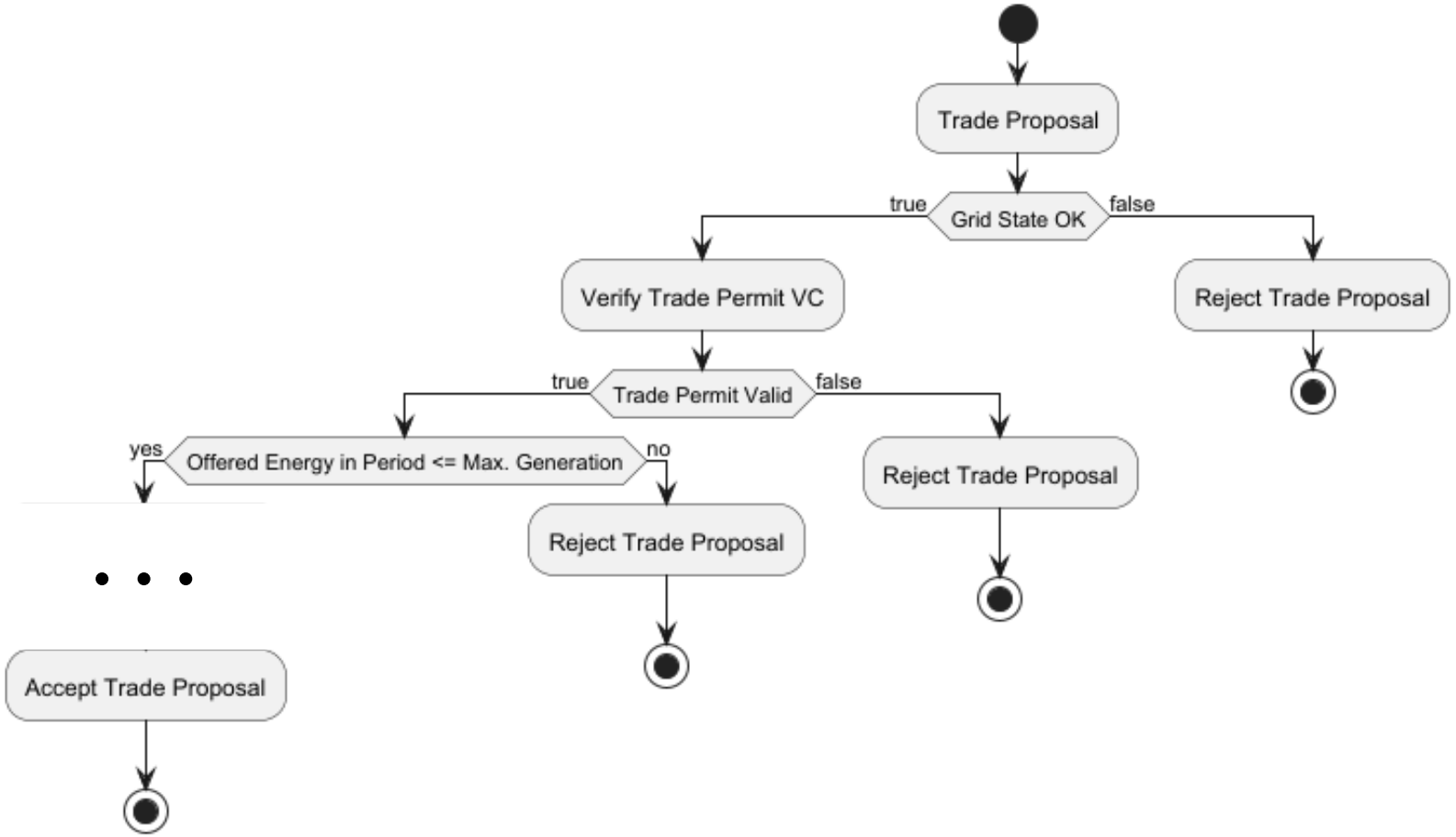
- User-centered identity management approach
- Allows issuance of VCs and verification through ZKP
- Encrypted P2P communication channels
- Selective disclosure
- Revocation of VCs is effective immediately



SSI model according to Preukschat & Reed (2021)


environment attributes
• grid state
• timestamp
• IDS status
subject attributes
• RES ID, MPAN
• max. generation
• trade permit
ABAC Authorization Decision
object attribute
• amount of energy offered
action attribute
• trade direction

ABAC AUTHORIZATION



IMPLEMENTATION

HAW HAMBURG

- SSI system with Hyperledger Indy blockchain and Aries agents for identification and authentication
- ABAC system using Authzforce framework for authorization
- Implemented features:

Holder	Issuer	Verifier
request trade permit VC	issue VC	verify VC
request RES VC	update VC	verify claims of VC
create digital presentation	revoke VC	--

- Simulated test with prosumer agents for evaluation
  - Component & integration tests
  - Performance tests

How the proposed IAM framework ensures protection of security assets:

Confidentiality:

- Encrypted communication channels
- Conditional validation of attributes

Integrity:

- VCs with ZKP
- Revocation of malicious actors' trade permits
- Unique session identifiers and timestamping

Availability:

- Efficient ABAC authorization process
- ABAC ruleset accounting for real-time grid status & IDS
- Decentralized IAM

FEATURED PROJECTS & FUTURE WORKS

HAW HAMBURG

PEAK (finished 2024)

ABAC456

- Future testing in real-world scenarios in follow-up Projects
- Implementation in real-world markets in Germany by 2030.

CONTACT

HAW HAMBURG

https://linktr.ee/moritz_volkmann

moritz.volkmann@haw-hamburg.de