IARIA

CARISSMA

Institute of Electric,
Connected and Secure Mobility

Authentic Batteries: A Concept for a Battery Pass Based on PUF-enabled Certificates

Authors: Julian Blümke,
Prof. Dr.-Ing. Hans-Joachim Hof

Presenter: Julian Blümke
julian.bluemke@carissma.eu

SECURWARE’22, Lisbon (PRT), 18.10.2022

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 963540.

Technische Hochschule Ingolstadt

Julian Blümke

- **Research Group *Security in Mobility* at CARISSMA Institute of Electric, Connected and Secure Mobility**
- **Research Topic: Security of Battery Management Systems**
- **Vita**

2018 – 2021	Master of Science in Computer Science
2013 – 2017	Bachelor of Science in Aviation and Vehicle IT
2017 – 2021	Software Engineer at Airbus Defence & Space
2013 – 2017	Trainee at Airbus Defence & Space

- **Current Research Project: MARBEL**
  - Manufacturing and assembly of modular and reusable Electric Vehicle battery for environment-friendly and lightweight mobility
  - New compact, modular, weight-optimized, and high-performance battery pack with longer life, and greater energy efficiency in charging use and energy use

Agenda

- **Background and Problem Description**
- **Concept for Authentic Batteries**
  - Data for battery pass‘s records
  - Security Considerations
  - Related Work
  - Security Architecture
  - Challenges
  - Security Assessment
  - Efficiency of Data Transfer and Verification
- **Conclusion and Future Work**

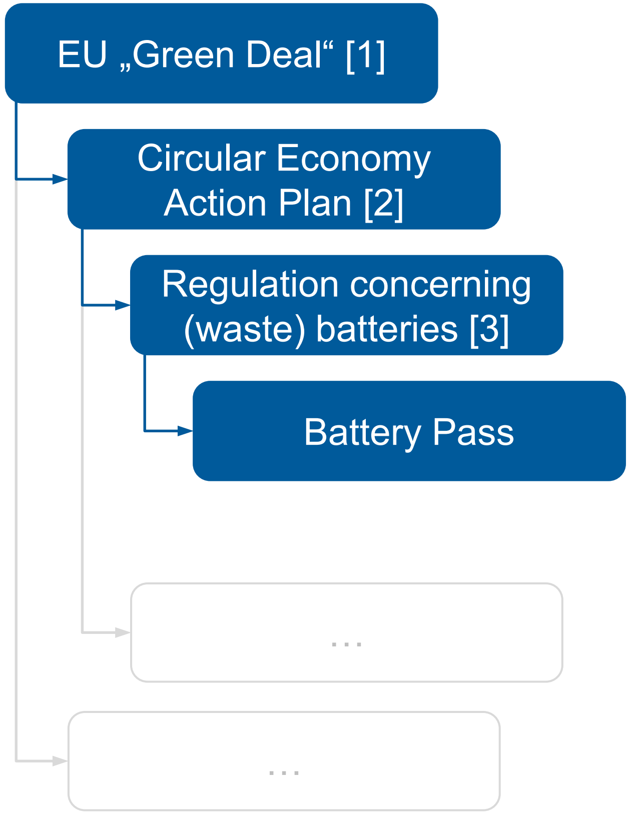
Background and Problem Description

- **Circular economy: reducing greenhouse gases by reusing batteries**
- **Collecting PLC data for easier assessment of best fitting second life applications**
- **Battery Pass mandatory for future batteries**
- **Additional: Counterfeit batteries due to new EV battery mass market [4]**

→ Need for authentic batteries

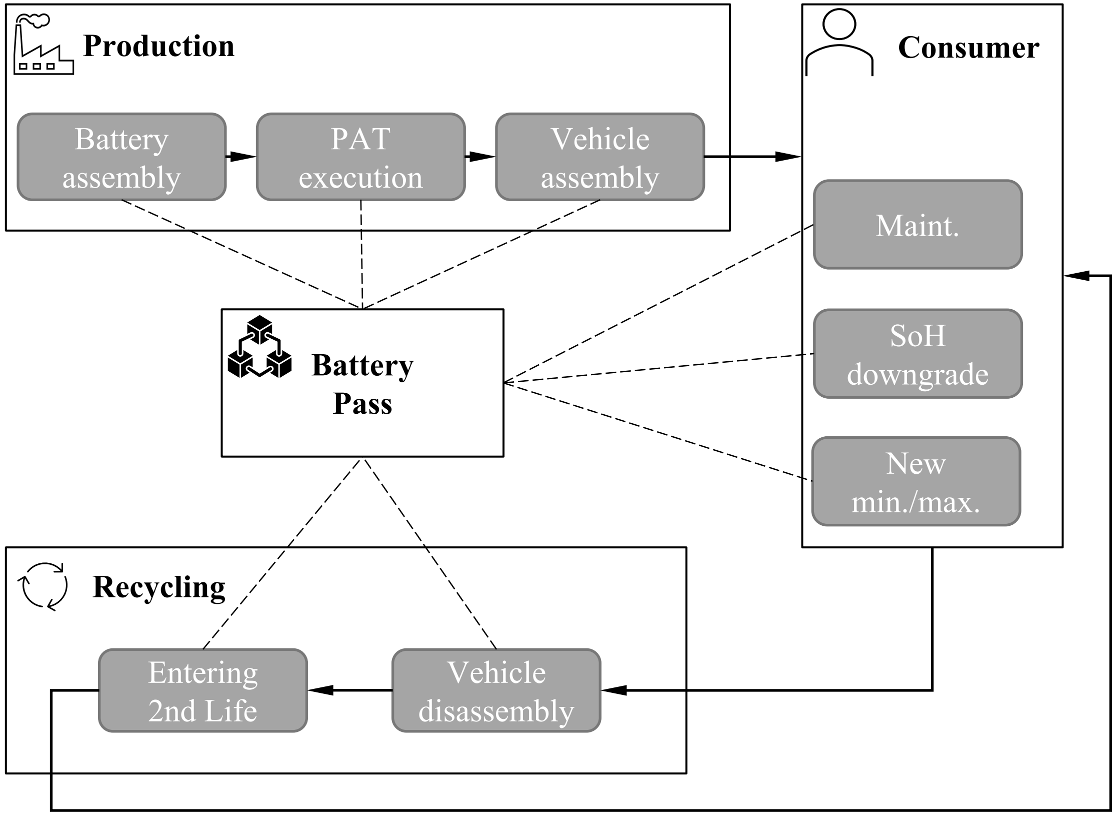
  - Trust in battery‘s quality
  - Evidence in correct implementation of specification
  - Traceability of PLC

- **Key element: Secure binding between physical battery and battery pass**


EU „Green Deal“ [1]
Circular Economy Action Plan [2]
Regulation concerning (waste) batteries [3]
Battery Pass
…
…

Concept for Authentic Batteries

Data for battery pass‘s records



Concept for Authentic Batteries

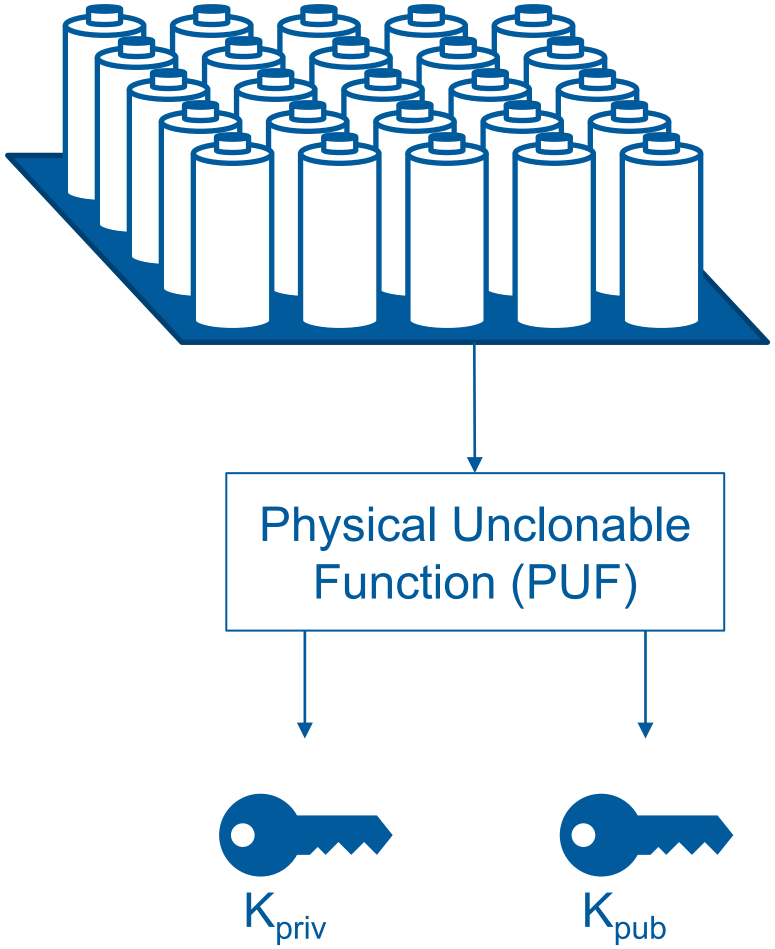
Security Considerations

Requirements

- Distinct binding of battery pass and physical battery
- Detection of manipulated battery pass
- Detection of counterfeit batteries
- Update of battery pass only with access to battery
- Generation of trust and transparency

Concept for Authentic Batteries

Derivation of cryptographic keys from PUF



Concept for Authentic Batteries

Related Work

PUFs based on batteries

Bosch, 2022 [6]

Calculation of PUF identifiers out of a set of different parameters (pressure drop between two sides of the battery, the battery‘s natural frequency, temperature pattern, OCV, air leak rate)

Zografopoulus, 2020 [7]

Authentication of energy storage network outstation by taking advantage of the fact that the cells‘ voltages differ at the same SoC

Blockchain with PUFs

Mohanty, 2020 [8]

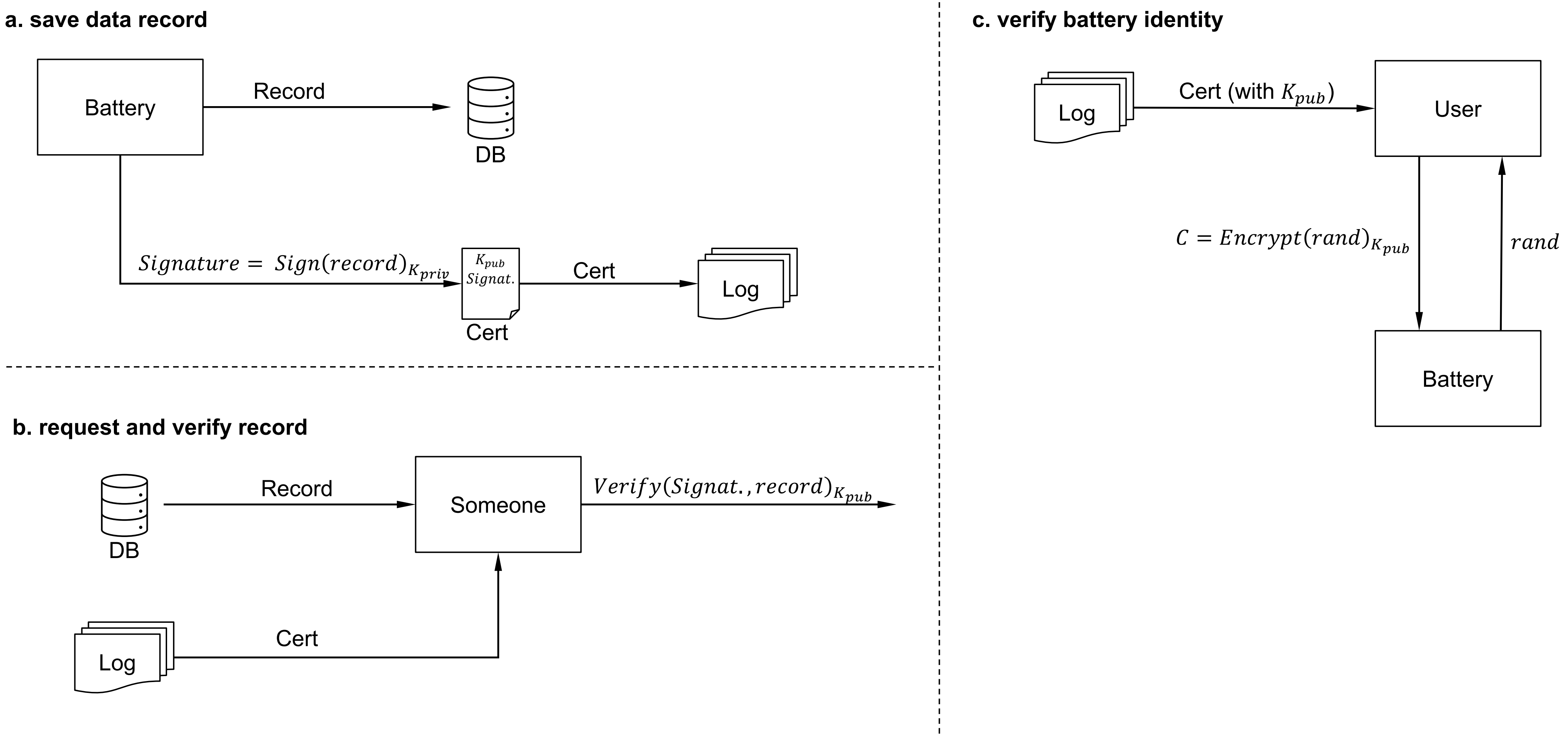
PUFChain: trusted nodes authenticate data collected from client nodes by comparing pre-calculated PUF-CRPs with CRP saved in transaction

Cui, 2019 [9]

Enabling trust in supply chain by tracing devices in blockchain with a unique ID (e.g. PUF)

Concept for Authentic Batteries

Security Architecture



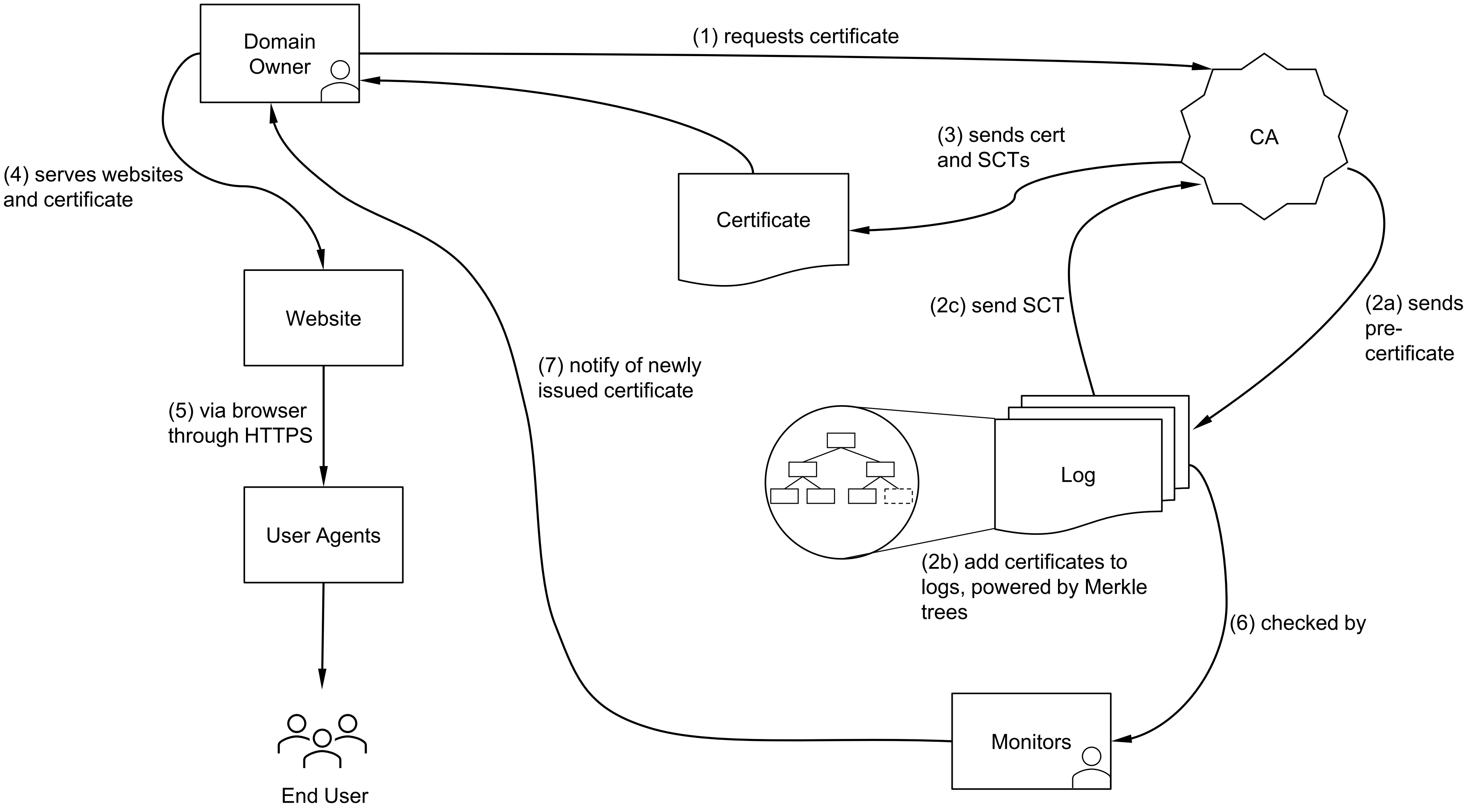
a. save data record

b. request and verify record

c. verify battery identity

Concept for Authentic Batteries

Background: Certificate Transparency



Domain Owner
(1) requests certificate
CA
(3) sends cert and SCTs
Certificate
(4) serves websites and certificate
Website
(2c) send SCT
(2a) sends pre-certificate
(7) notify of newly issued certificate
(5) via browser through HTTPS
Log
User Agents
(2b) add certificates to logs, powered by Merkle trees
(6) checked by
Monitors
End User

Illustration based on [5]

Concept for Authentic Batteries

Security Assessment

Requirements	fulfilled by
Distinct binding of battery pass and physical battery	using keys derived from PUF
Detection of manipulated battery pass	verification of signatures
Detection of counterfeit batteries	verification of signatures
Update of battery pass only with access to battery	updating signature only with PUF
Generation of trust and transparency	using crypto. keys and Certificate Transparency

➔ Just a static and superficial analysis. Future work will contain an in-depth security analysis.

Concept for Authentic Batteries

Challenges

Cell aging / Repairs

PUF may change
→ Validation steps will fail

Standardization

Standardized data formats and processes across companies mandatory

Update process

Frequency and resolution of record updates need to be defined

Solution approaches:

1) Model to forecast cell and battery aging in order to create static cryptographic keys
2) If an imminent change is foreseeable having a mechanism to modify existing keys

Concept for Authentic Batteries

Efficiency of Data Transfer and Verification

- **Data Transfer**
  - During the MARBEL project state-of-the-art BMS has been analyzed in a Proof-of-Concept
  - Tests with a frequency of data transfer ranging from 5 Hz to 200 Hz sending single MQTT messages
  - Authentication and encryption established using TLS
  - Average message size: 90 Bytes → max. data rate 144 kBits/s

  ➔ Findings appear to support an efficient data transfer
- **Verification**
  - Data will be verified on servers → high-performance optimization possible

  ➔ It is expected that verification can be carried out efficiently

Conclusion

Circular economy and product counterfeiting increase **need for authentic products**

Battery pass one example to **achieve trust and traceability** of a product

Presented concept:

- Managing battery‘s life cycle record by using **certificates**
- Binding between battery identity and battery pass achieved with **PUFs**

Future Work

Implementation of a **Proof-of-Concept**

Performance analysis and in-depth formal **security analysis**

Investigations on **PUF consistency**

Any questions?

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 963540.

References

[1] European Commission, “Regulation (eu) 2021/1119 of the European parliament and of the council of 30 june 2021 establishing the framework for achieving climate neutrality and amending regulations (ec) no 401/2009 and (eu) 2018/1999 (‘european climate law’): European climate law,” 2021. [Online]. Available: http://data.europa.eu/eli/reg/2021/1119/oj

[2] European Commission and Directorate-General for Communication, Circular economy action plan: for a cleaner and more competitive Europe. Publications Office, 2020.

[3] European Commission, “Proposal for a regulation of the European parliament and of the council concerning batteries and waste batteries, repealing directive 2006/66/ec and amending regulation (eu) no 2019/1020,” 17.03.2022. [Online]. Available: http://data.consilium.europa.eu/doc/document/ST-7317-2022-INIT/X/pdf

[4] A. B. Lopez, K. Vatanparvar, A. P. Deb Nath, S. Yang, S. Bhunia, and M. A. Al Faruque, “A security perspective on battery systems of the internet of things,” Journal of Hardware and Systems Security, vol. 1, no. 2, pp. 188–199, 2017.

[5] Google, “Certificate transparency: How ct works,” 2022. [Online]. Available: https://certificate.transparency.dev/howctworks/

[6] K. Vittilapuram Subramanian and A. Madhukar Lele, “A system and method for generation and validation of puf identifier of a battery pack,” Patent WO2 022 023 280A2, 2022.

[7] I. Zografopoulos and C. Konstantinou, “Derauth: A battery-based authentication scheme for distributed energy resources,” in 2020 IEEE Computer Society Annual Symposium on VLSI (ISVLSI). IEEE, 2020, pp. 560–567.

[8] S. P. Mohanty, V. P. Yanambaka, E. Kougianos, and D. Puthal, “Pufchain: A hardware-assisted blockchain for sustainable simultaneous device and data security in the internet of everything (ioe),” IEEE Consumer Electronics Magazine, vol. 9, no. 2, pp. 8–16, 2020.

[9] P. Cui, J. Dixon, U. Guin, and D. Dimase, “A blockchain-based framework for supply chain provenance,” IEEE Access, vol. 7, pp. 157 113 – 157 125, 2019.