Binding the Battery to the Pass: An Approach to Trustworthy Product Life Cycle Data by Using Certificates Based on PUFs

Julian Blümke
CARISSMA Institute of Electric, Connected and Secure Mobility (C-ECOS)
Technische Hochschule Ingolstadt
Ingolstadt, Germany
e-mail: julian.bluemke@carissma.eu

Hans-Joachim Hof
CARISSMA Institute of Electric, Connected and Secure Mobility (C-ECOS)
Technische Hochschule Ingolstadt
Ingolstadt, Germany
e-mail: hans-joachim.hof@thi.de

***Abstract*—Reusing batteries of electric vehicles in second life is one pillar of the European Union's Green Deal and its derivatives in order to foster the reduction of greenhouse gases. Product life cycle data plays an important role in improving and simplifying the process of finding the most suitable second life application for a used battery. Such data collected throughout the product's life cycle will be summarized in a digital product pass mandatory for future batteries. Having trustworthy data is a key element of the battery pass in order to provide authentic batteries. This paper presents a concept to securely bind the pass to the battery itself by using physical unclonable functions for creating unique cryptographic keys per battery. Inhomogeneities and cell-to-cell variations in a battery pack enable the use of batteries as physical unclonable functions. The approach combines the cryptographic keys derived from the battery with certificates and makes use of Certificate Transparency promoting trust in the issued certificates. Initial security analysis shows that attacks on product life cycle data and certificates as well as the introduction of manipulated and counterfeit batteries can be detected.**

***Index Terms*—physical unclonable function; Certificate Transparency; electric vehicle battery; battery identity; battery pass; cybersecurity.**

I. Introduction

This paper extends [1]. The European Union's (EU) Green Deal aims to reduce greenhouse gases towards net-zero emissions by 2050 [2]. One of the measures is to lower the use of fossil energy in the transportation sector. Electrically driven vehicles foster this goal and are expected to achieve high sales numbers in the upcoming years: The Faraday Institute forecasts a worldwide demand of more than 5 900 GWh in the year 2040 (2020: 110 GWh) [3]. The rise of Electrical Vehicles (EV) is accompanied by an increasing need for high-voltage batteries. However, batteries degrade during usage and charging. They can only be used in an EV until their capacity degraded to 80% [4, 5]. This will result in a large number of dismounted and unusable EV batteries having a negative economical, ecological, and social impact [6]–[8]. However, these batteries may be still fine for other use cases. To support the recycling and reusing of products and materials the EU introduced the Circular Economy Action Plan containing the reuse of batteries as one pillar [9]. Its goal is to set up applications for a battery's second life either as a complete product in a different environment or dismantled in new products.

The new mass market for EV batteries will also encourage the production of counterfeit batteries. Non-certified or non-qualified batteries can introduce safety risks due to deviations from the specifications of genuine products and especially due to cost-savings in risk-reducing controls and management systems [10]. Reduced capacity and lifetime, overheating, and self-ignition, as well as social aspects like underpaid workers and bad working conditions during manufacturing, are examples of likely effects when using counterfeit EV batteries.

Circular economy and the fight against counterfeiting emphasize a need for authentic batteries that we define as the following: trust in the battery's quality, evidence in the correct implementation of the specification, and traceability of the product life cycle enhance the opportunities for second life applications and lower the risk of introducing low quality and dangerous products into the market. Both, the readiness for circular economy and the circulation of only high-quality batteries, shall be regulated within the new EU-regulation about the treatment of (old) batteries [11] introducing the Battery Passport as an electronic record for batteries of EVs, among others.

This paper presents an approach to inherently bind the digital pass to the physical battery by using certificates based on Physical Unclonable Functions (PUF) managed within the method of Certificate Transparency. The following paragraphs introduce the basic techniques of the presented approach.

Battery Passport: As of today the final adoption of the new regulation by the European Council and the European Parliament is still open [12]. However, no significant modifications of the regulation are expected until then. Therefore, the following requirements can be summarized: The Battery Passport shall be unique for each individual battery and shall consist

2023, © Copyright by authors, Published under agreement with IARIA - www.iaria.org

of data relevant to the battery's model, and static and dynamic data specific to a single battery. The latter shall accommodate performance and durability parameters, the status of the battery, the number of charging and discharging cycles, negative events like accidents, and operating environmental conditions including the temperature and State of Charge (SoC).
The Battery Passport shall be available through an online database. In case of a second life application, the existing data shall be transferred into a new passport and the legacy passport shall be deleted. Test reports shall be available to notified bodies, market surveillance authorities, and the European Commission to enable examination of compliance with the battery-related requirements.

The regulation provides for a physical code as an identifier of a battery. However, we want to solve the identification of a battery by means of PUFs.

Physical Unclonable Function: A PUF uses physical deviations that occur during production to create a unique and unclonable identifier [13]. It is described as a challenge-response-pair (CRP) where a device to be authenticated needs to prove the ownership of the PUF-identifier. According to McGrath et al. [14] a PUF needs to fulfill the following properties: robust, unique, easy to evaluate, challenging to replicate, and impossible to predict. In general, a distinction is made between weak and strong PUFs. Weak PUFs only comprise one or few CRP, which brings the advantage of storing cryptographic keys without requiring non-volatile memory. An example of a weak PUF is the SRAM-PUF: An SRAM memory cell has two stable states that represent 0 and 1. However, before the first write operation has been executed, the cells tend either to 0 or to 1. This undefined state is used to derive a cryptographic key [15].
On the other hand, strong PUFs are defined as having so many CRP that an attacker cannot solve or recover the PUF in a finite time. One example of these types of PUFs is the optical PUF: It consists of a movable laser beam, a scattering medium, and a sprinkle detector (Figure 1). The orientation of the laser beam is the challenge, whereas the sprinkles comprise the response. It is hardly possible to create equal scattering media and therefore, this principle is suitable as a source of randomness [15].

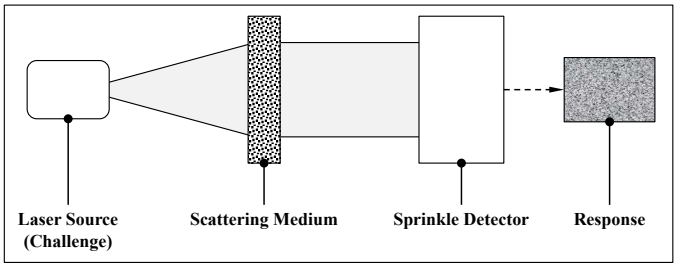

Fig. 1. Process of optical PUF (illustration based on [16])

Regardless of the PUF's type, the general process of deriving cryptographic keys applies to both. Since both the physical source and the measurement process are subject to noise and variabilities, the PUF's response differs slightly, even if the same challenge is used. Therefore, an additional step needs to be done in order to correct these errors [15, 17]. To enhance general security, the random number created from the PUF is hashed using a cryptographic hash function [18]. The process of deriving cryptographic keys from a PUF is shown in Figure 2 in which a fuzzy extractor is used for stabilization and uniformity of the plain PUF response.

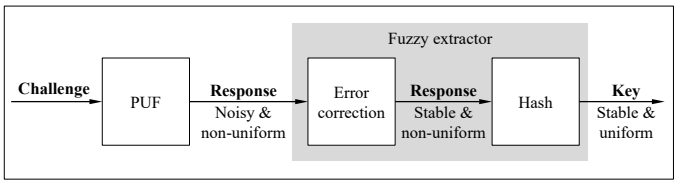

Fig. 2. Process of deriving cryptographic keys from PUF (illustration based on [18])

The two main areas of application of physical unclonable functions are a secret key generation (weak PUFs) and authentication at low cost (strong PUFs) [13]–[15]. The advantages of using PUFs instead of dedicated random number generators are the following: they are simple as they are using existing hardware structures and do not rely on pseudo-random number generators. The secret is only available in a powered mode, which makes it more difficult for attackers to read out the keys, the chance for invasive attacks is reduced, and they are more cost-efficient as they do not need expensive security hardware modules [15].

As introduced later in Section III, the Battery Passport consists of certificates. To enable trust and transparency in the issued certificates, the methods of Certificate Transparency are used.

Certificate Transparency: Certificate Transparency (CT) was originally developed by Google and is about the transparent and trust-worthy issuing of certificates used in the Web PKI [19]. It is summarized in the experimental RFC 6962 [20] and deals with the difficulties of trusting Certificate Authorities (CA) in general: private keys associated with a certificate may be stolen or created in a wrongful way such that encryption itself would not be damaged but an attacker might be able to decrypt the communication without knowledge of the necessary key. A common way to check the trustworthiness of CAs is to examine audits. However, audits often check for formal aspects only than for the correct implementation of technical processes.
The idea of CT is about storing certificates in publicly available append-only logs that can be validated by everyone. Figure 3 shows the steps needed to implement CT: The owner of the domain requests a certificate by the CA, which creates a pre-certificate and sends it to the log. The latter is managed as a Merkle Tree [21]. A Signed Certificate Timestamp (SCT) ensuring that the certificate is added to the log is sent to the CA. The certificate is extended with the SCT and transferred

2023, © Copyright by authors, Published under agreement with IARIA - www.iaria.org

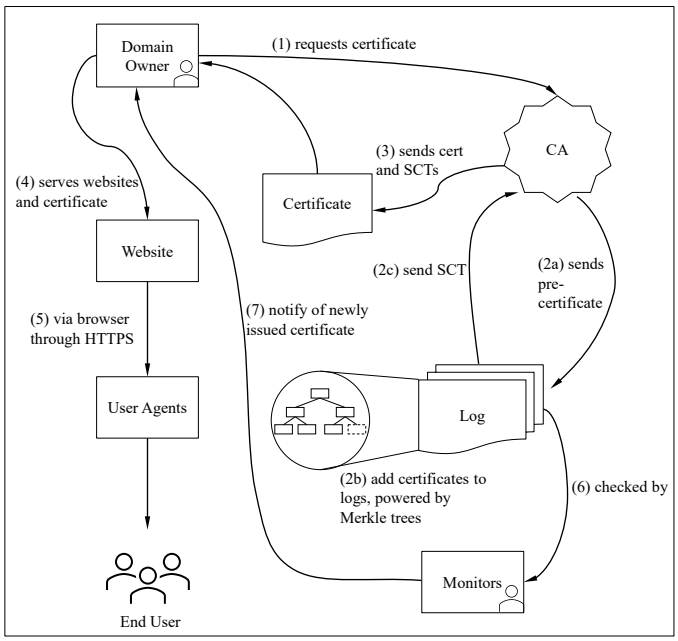

Fig. 3. Implementation of certification transparency (illustration based on [19]).

to the domain owner. From this time on, the domain owner can use it as a normal certificate, e.g., for hosting websites. At the end user's site, the certificate is checked for the existence of SCTs, e.g., during TLS handshake. Some internet browsers require that the certificate is signed with at least two SCTs. The certificate logs are checked periodically by external monitors. The domain owner is informed if there are new and especially odd activities with certificates of its domain.

Furthermore, there are other methods for detecting counterfeit products, e.g., by statistical measures [22], physical inspection, or electrical examination [23]. However, the presented concept is triggered by the EU regulation concerning the battery pass and therefore, the concept of logging and auditing is reasonable.

The remaining paper is structured as followed: Section II describes related work as a basis for a concept for authentic batteries, which is introduced in Section III. A brief security and performance evaluation of the presented approach is given in Section IV. Current and future activities are summarized in Section V.

The conference paper's extensions comprise additional information on the regulation concerning the Battery Passport, a more detailed explanation of PUFs and their characteristics, an overview of research works related to inhomogeneities and cell-to-cell variations in lithium-ion batteries, initiatives on the implementation of the Battery Passport, and an elaborated explanation of the presented approach to combine the physical battery with the Battery Passport.

II. Related Work

To the best of our knowledge, the idea of a digital product pass for single products is unique to batteries. Other applications do have static product records or they are only implemented for a group of products and not for single devices. Additionally, the battery pass will be the first pass that is required by law in the EU. The following related research results introduce only comparable parts of the presented concept.

A. Product Passes

The general concept of product passes is not novel. Several initiatives for passports in other domains already exist. Exemplary three implementations are introduced.

The International Material Data System (IMDS) is a collection of life cycle data in the automotive industry. Original equipment manufacturer (OEM) and supplier store information on component and material data of vehicles in the IMDS to reduce the workload and required time of life cycle assessment. The system has been introduced in the year 2000 and is commonly used by more than 50 OEMs and 120 000 suppliers [24].

Reusing building materials is important for a circular economy in the civil industry. The Building Information Management (BIM) based Material Passport shall enable Urban Mining by comprising data on materials across the full life cycle, e.g., of volume and geometry of multilayered components (concrete, insulation, plaster) or assessment of demolition acquisition [25].

The Danish ship manufacturer and logistic company Maersk created a Cradle-to-Cradle passport for enhanced recycling opportunities at the end-of-life of a container vessel. The document contains information on built materials as well as disassembly and recycling activities. This decreases the need for new materials fostering sustainability and reducing overall costs [26].

These initiatives show that product passes can enhance and simplify the assessment of the life cycle and of potentials for reuse and recycling. However, these product passports do not take into consideration dynamic activities and modifications of the product during life.

B. PUFs based on batteries

In [27], Vittilapuram Subramanian and Madhukar Lele describe the calculation of PUF identifiers out of a set of different parameters: pressure drop between two sides of the battery, the batteries natural frequency, the temperature pattern, the open circuit voltage (OCV), or the air leak rate. The created PUF identifier is saved as a physical tag on top of the battery or in the battery management system's memory. However, the identifier can only be calculated in a dismounted state. This method shows the possibility of a battery PUF creation in general.

Zografopoulos and Konstantinou [28] presented a method to authenticate an outstation in a distributed energy storage network. This work takes advantage of the fact that the cells' voltages differ at the same SoC. Both, the outstation and the

2023, © Copyright by authors, Published under agreement with IARIA - www.iaria.org

master station, sanitize a challenge-reply-table with continuously updated measurements presenting a model of every cell. The authentication challenge is formed out of a selection of cells. The SoC and the voltages are measured and sent back to the master station. If the actual measurements match with the values in the challenge-reply-table the outstation is accepted as authentic.

Both works demonstrate that it is feasible to use PUFs on batteries. However, existing works use PUFs as a mechanism to create an identity. We want to extend this to use PUFs to derive keys.

C. Inhomogeneities and cell-to-cell variations in lithium-ion batteries

Durbarry et al. [29] state that variations from cell to cell are the origin of a battery's uniqueness. Differences are noticeable in capacity, current, impedance, open circuit voltage, and so in the SoC [30, 31]. The origins of these inhomogeneities can be split into intrinsic and extrinsic influences.

Intrinsic inhomogeneities: As many parts of the used materials are natural products they are subject to variations. For example, the material used for the electrodes differs in composition, purity, defects, and morphology. An identical manufacturing process is also hardly achievable due to its complexity. Differences may also arise with respect to the production volume [32]. Even if the cells are produced identically, variations between them may also result from uneven cell connections [30]–[32].

Extrinsic inhomogeneities: The environment of the battery pack can also have an influence on differences between cells as well as the pack design: Unmatched cells and asymmetric design can result in inhomogeneous cell utilization. The same applies to an ineffective cooling strategy and external heat sources resulting in local temperature peaks. Finally, cells in serial or parallel architecture lead to differences [29]–[32].

The overall result of inhomogeneous parameters leads to inhomogeneous aging of different cell components and this again amplifies the variations of parameters. Aging accelerates over time [30, 31].

These research works show that significant cell-to-cell variations in lithium-ion batteries exist and are measurable. They also demonstrate the effects of aging on these inhomogeneities, which are mentioned later in Section III-E as one major challenge of the presented concept.

D. Blockchain with PUFs

A common mechanism to implement digital product passes is the use of blockchain [33, 34]. Casino et al. described a blockchain as a "distributed append-only timestamped data structure" [35, p. 56] where no central and trusted authority is involved. Exchanging assets, digital or physical, between two blockchain participants is achieved and recorded with transactions. They have to be validated by other participating nodes using a consensus algorithm in order to prevent corruption or forgery of branches. Blockchains in the sector of supply chain management can increase trust, traceability, transparency, and accountability. They are installed for better visibility and enhanced optimization of a supply chain [35].

Mohanty et al. [36] introduced PUFChain, which is a method that combines blockchain with PUFs within the Internet-of-Everything (IoE) domain where trusted nodes authenticate IoE-data collected from client nodes. The process is divided into three phases: During the enrollment, the client's PUF-CRP are calculated and stored in a secure database. The phases of transactions consist of data collection, PUF response generation, and hashing of both. The data and the hash are added to the blockchain and need to be authenticated by trusted nodes. These nodes recalculate the hash by using the client data and the pre-calculated PUF response retrieved from the database and validate the block if both hashes match. An application of PUFChain in the Internet-of-Energy was given by Asif et al. [37].

An approach to enable trust in the supply chain by tracing was presented by Cui et al. [38]. Newly manufactured devices need to be registered in a blockchain with a unique ID, e.g., a PUF. Device transfers are recorded in the blockchain. The contractual ownership alters only after a transfer confirmation, which is done by calculating the unique device ID of the received device and comparing it with the ID mentioned in the transaction payload. End users can check the device's authenticity by matching the computed ID with the blockchain content.

Whereas blockchain is a popular method for storing tamper-proofed data, we decided to use a different approach. In our opinion, the system consists of trusted partners: A generally trusted collaboration across the supply chain of EV batteries has to exist already, meaning that contracts describing a trade relationship are in place. One major motivation for using blockchain methodology is to create a network between parties that do not trust and know each other. Both are not applicable to the application presented in this concept. Therefore, decentralized distribution of data is not necessary and so, a central database fits the requirements and can be hosted, e.g., by the EU enforcing the battery regulations. In a blockchain, consensus mechanisms shall ensure the correctness of new transactions. In this specific application, these mechanisms are useful only to a limited extent as they will only perform a proof of formal attributes of a transaction, i.e. a new record added to the Battery Pass. A blockchain party validating a new block cannot check the validity and legitimacy of, e.g., a new temperature maximum or a degradation of the capacity. This is only possible with direct access to the battery system itself. As a summary, using a blockchain will add extra effort without having additional advantages. The key functionality of generating trusted and tamper-proofed data records can also be achieved by using the methods of Certificate Transparency.

E. Initiatives working on Battery Passport

The new EU regulation concerning the Battery Passport is expected to be mandatory within the next years. Therefore,

2023, © Copyright by authors, Published under agreement with IARIA - www.iaria.org

several initiatives for the battery pass's implementation exist. Due to the early phase of these projects, only introductory content has been published and so, an assessment of the architectural concepts is hardly possible. However, a brief overview of existing projects is given.

The Global Battery Alliance (GBA) is a collaboration platform consisting of more than 120 partners and organizations and puts the focus on a sustainable supply chain in the battery industry. It was founded at the World Economic Forum (WEF) in 2017. The GBA published proof-of-concept pilots for a Battery Passport at the Annual Meeting of the WEF 2023 [39]. The pilots contain information on a specific battery: EV manufacturer, battery producer, battery cell producer, cell type, chemistry, capacity, and other parameters are shown as well as information on materials including the origin of raw materials. The focus of the pilots is on ESG (environmental, social, and corporate governance) data. Whereas the underlying architecture and processes are not known so far, the proof-of-concept pilots give an insight into a potentially implemented Battery Passport.

A project closely related to the GBA is called *Battery Pass*, which is a consortium formed by companies from the automotive, battery recycling, and data processing industries [40]. It is funded by the German Federal Ministry for Economic Affairs and Climate Action and shall make use of the automotive information exchange system Catena-X. A report [41] guiding through the new EU regulation's content relevant to the battery passport has been published. It introduces the consortium's interpretation of the requirements and outlines an overview of the possible data stored in the Battery Passport. This project aims to give guidelines for interpreting and implementing the EU regulation and therefore, it should be kept in view. A demonstrator is expected to be published in 2024.

III. Concept for authentic batteries

A. Introduction

The general aim of our method is to have one single source of truth containing information about the battery's life cycle including the manufacturing process, product acceptance tests (PAT), measures of quality control, and usage history. Tracing materials and processes fosters consumers' trust in the battery and enables an easier and more precise assessment of the batteries' status for recycling or reusing.

The data of the life cycle record is stored in a database that can be restricted in order to control the read and write access of the supply chain parties involved. Access control also protects the parties' intellectual property (IP). It is mandatory to have a secure binding between the life cycle record and the battery itself ensuring the correspondence between both. The secure binding is established by the use of certificates in combination with PUFs that provide unique identifiers for each battery.

B. Data for battery pass's records

Data is added to the battery pass during manufacturing, product testing, and quality control. This data brings added value to the end user, as the user receives information on a remarkable downgrade of, e.g., the state of health (SoH) or capacity and on minimum and maximum temperatures, voltages, and currents. The latter parameters are important to assess the battery's health for a second life application. The data acquisition building the life cycle record is split into three phases (see Figure 4).

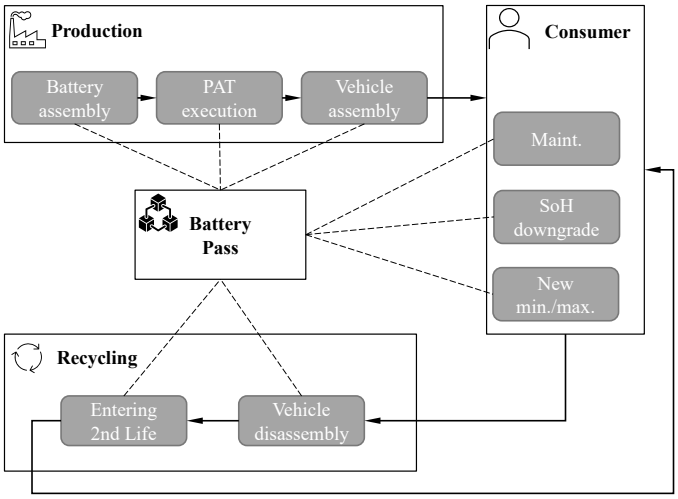

Fig. 4. Battery pass as life cycle record.

Assembly and initial product testing takes place during the production stage at the battery OEM. Information about the manufacturer, working conditions, date of production, and results of acceptance tests are stored in the battery pass. It may be split into battery cell OEM and battery pack OEM having similar data. Afterwards, the battery is transferred to the vehicle's OEM to be built into the intended vehicle. Again, information about the vehicle manufacturer, working conditions, and the vehicle including the vehicle identification number (VIN) are stored in the record. The storage of information concerning the working conditions shall enable a socially acceptable supply chain, which goes along the new EU regulation.

We are assuming the car to be delivered to the consumer directly after production. At this stage, the battery will be used in its intended environment of the first life. Significant changes in the battery's quality will be logged in the life cycle record. These changes include temperature, voltage and current maxima and minima, and SoH and capacity downgrade. The collection of data at this stage is of high relevance in order to execute a sophisticated life cycle assessment of the battery before entering a second life.

The preparation of the second life is divided into two steps: First, the battery is dismounted from the vehicle and the date and the implementing company are stored in the life cycle record. This marks the end of the first life. The activity of entering the second life contains events like firmware or configuration updates required for a new environment or applications, quality tests, and maintenance activities. Again, the battery will be transferred to a consumer. We assume an

2023, © Copyright by authors, Published under agreement with IARIA - www.iaria.org

environment in which the life cycle record can be sanitized. Therefore, the stage of the second life equals the consumer stage. Depending on the new area of application other or additional data than before may be stored in the battery pass.

The format of the battery pass's data is not defined here. However, the JSON data format may be reasonable as it is widely used and easy to read and process.

C. Security Requirements

The security demands for the presented concept are mainly derived from the high-level requirements of the Battery Pass as presented in Section I. The following security-related aspects shall be considered:

- The battery pass and its records shall be bound to the physical battery. This guarantees that the records are only valid for one specific battery.
- It shall be possible to detect a manipulated battery pass. Shaping of data towards, e.g., less charging cycles or better historic environmental conditions, may increase the resale value of an EV and therefore, these malicious activities must be prevented.
- The circulation of counterfeit batteries having a stolen or no battery pass shall be recognized as well.
- Updates of the records shall only be possible from the battery itself or from a system that has access to the battery. This ensures the validity of the data without the possibility of data being added by a third party not involved in the process.
- Trust and transparency shall be treated to foster the battery pass's acceptance by the user and in general a successful assessment of second life applications.
- It shall be possible to restrict access to the data records of the Battery Pass to a limited number of users or user groups in general. This ensures the enforcement of the GDPR (general data protection regulation) and the protection of intellectual properties.

D. Security Architecture

The technical implementation of our method is based on signed battery data whereas the keys are derived from the battery's PUF. Figure 5 shows the overall process of adding data and verifying the battery's identity. We are assuming the process of deriving a key from the PUF has already been carried out. As elaborated in the section on related work (Section II), this assumption is reasonable.

The general implementation is split into four phases: In the enrollment phase, the keys and an initial certificate are created. It is followed by the creation and storage process of a new data record. In this phase, the battery is the only active part, apart from storing the certificate in the log. In the third phase, the battery is not involved anymore, as the verification of a record can be carried out by using only the entries of the database and the certificate stored in the log. To verify the identity of the battery, the battery must prove possession of the private

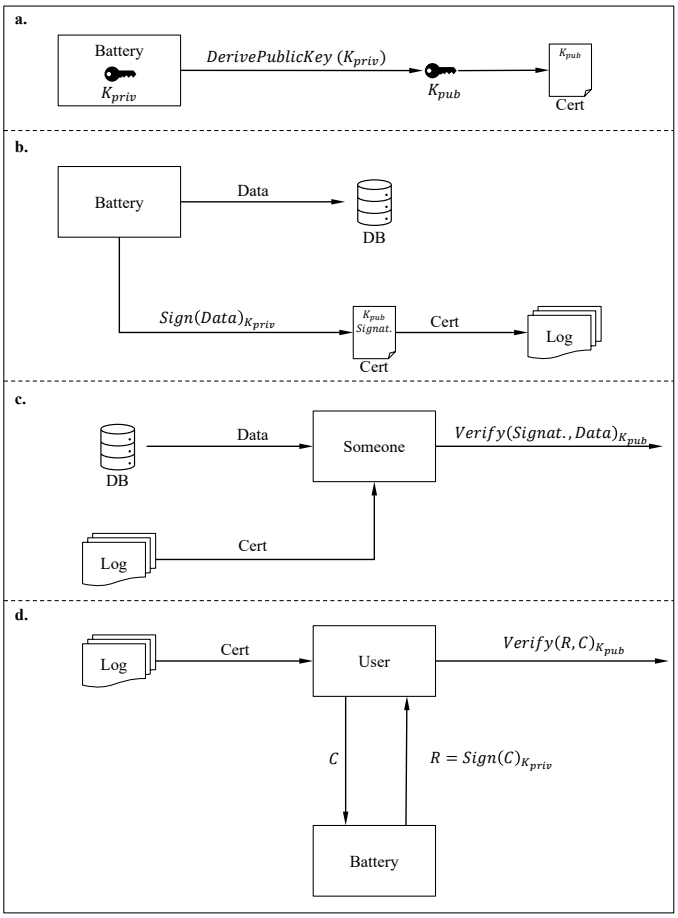

Fig. 5. Implementation of digital pass with certificates. **a.** Enrollment phase **b.** Update of battery records **c.** Verify that the certificate belongs to records **d.** Verify that the battery belongs to the certificate.

key to a user, which is comprised in the fourth phase. The four phases introduced are outlined in the next paragraphs. Except for the first phase, the stages do not have to be processed one after another. The activities can be executed independently.

The first phase is to enroll a private and public key and an initial certificate. As mentioned earlier we assume that a key has been derived from the battery's PUF. This key is the private key and will never leave the battery. A public key is calculated from the private key and added to an initial certificate. At this stage, the certificate may contain only metadata. However, battery-related data will be added in the next step that immediately follows the enrollment phase in order to fill the Battery Pass with relevant data.

The most functional part of the method is adding and updating the data of the battery. The relevant data is described in Section III-B. If new data is generated it will be sent to a central database containing historic and current data of this specific battery (Figure 5b). In the battery or more precisely in the battery management system the data is signed with the private key derived from the battery's PUF. Only the signature is added to a battery-specific certificate also containing the

2023, © Copyright by authors, Published under agreement with IARIA - www.iaria.org

public key. If a certificate already exists for the battery a reissuing is needed and the old one has to be revoked. The certificate itself is attached to an append-only log. We are relying on Certificate Transparency, which is a commonly used method developed by Google to store and handle identity certificates in a trusted and verifiable way, which has been introduced in Section I. Whereas the log itself does not fulfill any functional requirement, it provides additional trust and transparency into the certificate as it can be validated and monitored by external and public parties.
One could argue to add the battery data to the certificate introducing the advantage of having one single document containing all relevant information about the battery. However, having this, the battery's data is publicly available, and therefore, IP may be revealed as well as the opportunity for malicious analysis of production statistics and performance of a battery OEM. A dedicated database can be restricted to a reduced number of users. This is also in line with the EU regulation concerning the definition of the Battery Pass, presented in Section I. Test reports certifying the quality of the battery shall only be accessible to a certain group of users.

In order to check the validity of the data in accordance with the corresponding certificate, access to the data and the certificate is needed. Using the public key stored in the certificate the signatures can be verified (Figure 5c). In this context, another opportunity to avoid disclosure of IP may be possible by letting the signatures be checked by the database itself and letting it deliver a summary of data not revealing IP.

In the last phase, it is checked that the certificate belongs to the battery as described in Figure 5d. Therefore, a challenge-response mechanism is used where the user sends a challenge consisting of a random number to the battery. The challenge is signed using the battery's private key and the response is sent back to the user. If the received signature can be verified using the corresponding public key it is proven that the certificate belongs to the battery as the private key is directly derived from the battery's PUF.

To reduce the risk of stolen or reproduced keys by an attacker the derived key may be stored in a Hardware Security Module (HSM), e.g., placed on the Battery Management System (BMS). However, the cost-efficiency of HSMs in the context of industrial applications with large quantities having high pressure on costs has to be evaluated [42].

E. Challenges

The main challenge of the presented method is the derivation of keys from the battery's PUF. It is required that the keys do not change over time. However, due to the aging of cells and the battery pack the PUF and so, the keys may change. The validation steps mentioned above cannot be executed anymore resulting in a failure of the complete method. The same applies to genuine repairs or maintenance activities of the battery. Single cells will not be exchanged probably, but battery packs. This would result in a new PUF and so in invalid existing private and public keys.
To overcome both, two approaches might be appropriate: First, using a model forecasting the cell and battery aging in order to create static cryptographic keys. And second, if an imminent change is foreseeable having a mechanism to modify the existing keys, e.g., with pre-calculated challenges and a hash chain for tracking expired keys.
Instead of using the battery's cells to create unique identifier, one could also use the surrounding electrical components as an origin for physical unclonable functions. The entropy might be enough to create cryptographic keys as there are many components built into one battery pack. These components do not age in the same way as cells do.

The creation of the PUF shall only be possible using the measured data available to the BMS installed in the vehicle. Measurements that are only obtainable under laboratory conditions cannot be used for these calculations. However, in-situ measurements reduce the opportunities to retrieve cell-to-cell variations as stated by Prosser et al. [43]. Therefore, it has to be analyzed if it is possible to measure the mentioned inhomogeneities sufficiently within the BMS and if these parameters offer enough entropy to be applied to cryptographic applications.

Challenges also arise in the general use of the battery pass. Standardization across companies is mandatory to enable comparability of batteries. This also applies to the update procedure of the battery pass. Questions concerning the frequency and the resolution of record updates have to be answered.

IV. Evaluation

A brief analysis of the security and efficiency aspects of the presented approach is given in the following section. It is evaluated if the concept meets the requirements outlined in Section III-C. The approach is also examined with regard to its efficiency.

A. Security Analysis

The assumed model of the adversary is presented, followed by an evaluation of the individual requirements.

Adversary Model: We assume that the attacker has read and write access to the database. As the certificates are stored publicly following the methods of Certificate Transparency the adversary can also read certificates. However, the attacker cannot read or re-create the battery's private key as we assume that the physical access to the battery and its related components is restricted or destroys the physical characteristics resulting in a modified PUF.

Binding battery pass and battery: The data of the battery stored in the database is signed using a private key that is derived from the components of the physical battery. The signature itself is saved in a certificate, which is the actual battery pass. Therefore, the physical battery and the battery pass are distinctly linked.

2023, © Copyright by authors, Published under agreement with IARIA - www.iaria.org

Detection of manipulated battery pass: Manipulation of a battery pass can be possible in two ways: First, manipulation of data in the database and second, manipulation of the certificate. Data manipulation will be recognized if the signature is verified. Signature verification should be a mandatory step when working with these batteries, e.g., for an assessment of the second life applications. A manipulation of the certificate can be detected by the monitoring instances within Certificate Transparency. However, if an attacker can calculate a signature using a key he controls and if he can add the signature and the corresponding public key to the certificate, a manipulated battery pass cannot be detected by only verifying the signature. To overcome this effect, it must be checked if the physical battery, i.e. the private key, belongs to the public key stored in the certificate.

However, in general manipulation or deletion of data can result in financial and ecological damage as it is the basis for further use of the battery. If the data is deleted, assumptions based on statistical measures have to be consulted, which may result in a worse assessment of the state of health.

Circulation of counterfeit batteries: If an attacker duplicates the certificate in order to sell a counterfeit battery with a pseudo-valid certificate, the attack may not be recognized until the link between the certificate and the battery is verified. Whereas the signature for the data is valid, the challenge-response as mentioned in Section III-D will fail: The public key stored in the certificate does not match the private key of the battery as the public key is a derivative of the private key. Therefore, the decrypted response will not match the initial challenge.

Update of battery pass only with access to battery: In theory, records can be added to the database without having access to the battery. As we assume that the attacker has access to the database values can be added or deleted arbitrarily. Even a signature can be created by an attacker. However, the signature cannot be validated correctly as the key used for signing the data does not match the public key used to validate the signature. The signature will be validated correctly only if the private key derived from the battery is used. Therefore, a valid update of the battery pass is only possible with physical access to the battery. Nevertheless, the validation must be done actively and continuously in order to prevent the theoretical opportunity of adding data without access to the battery. The monitoring feature of Certificate Transparency supports this requirement.

Generating trust and transparency: Trust and transparency for user's acceptance and for trustworthy assessment of second life applications is created with the use of cryptographic keys on the one hand and on the other hand with the use of Certificate Transparency where certificates can be validated by external parties.

Several attack scenarios have been described. None of them can be executed on their own as there need to be attacks on multiple system parts to be successful. However, it also showed that a continuous verification of the different links between certificate, data, and battery is mandatory to ensure the system's security. Nevertheless, a complete and in-depth security analysis will be executed in the future to strengthen the given statements.

B. Efficiency of Data Transfer and Verification

In the current EU project MARBEL (Manufacturing and assembly of modular and reusable Electric Vehicle battery for environment-friendly and lightweight mobility [44]) the efficiency of data transfer with a state-of-the-art BMS has been analyzed in a proof-of-concept. Tests have been made with a frequency of data transfer ranging from 5 Hz to 200 Hz sending single MQTT (Message Queuing Telemetry Transport protocol) messages. Authentication and encryption were established using the Transport Layer Security (TLS) protocol adding a security-related overhead to every message. The average message size summed up to 90 bytes, which corresponded to a measured maximum data rate of 144 kBits/s. The findings from these tests appear to support the assumption of an efficient data transfer. However, a continuous stream of battery data might not be required as the degradation of the battery's SoH is a slow process. Data may be also buffered over a defined time and sent in blocks.
Data will be verified on servers that can be highly optimized. Therefore, it is expected that the verification can be carried out efficiently as well.

V. Conclusion and Future Work

Circular economy and the fight against counterfeiting emphasize a need for authentic products. Digital product passes are one example to increase trust and transparency in a product's life cycle. Within the next years, a digital product pass will be mandatory for all EV batteries entering the EU's market. This paper presented an approach to inherently bind the battery with the pass by using certificates with PUFs. Variations from cell-to-cell exist and therefore, it seems feasible to derive cryptographic keys from a battery-based PUF. The certificates are managed and validated within the environment of Certificate Transparency. Challenges arise in the inconsistency of PUFs due to cell aging and in the availability of measurement controls in the BMS. An initial security analysis showed that the presented method enables traceability of and trust in the product life cycle data and detectability of counterfeit products and passes.
Future work includes an analysis of cell parameters usable for a PUF directly retrievable within the BMS. An assessment of the random data in terms of entropy is also to be done as well as further investigations on the consistency of PUFs in the context of EV batteries. The results will be used to create a proof-of-concept followed by a performance and in-depth formal security analysis in order to evaluate the functionality and the security measures of the presented method. Other mechanisms for detecting counterfeit electronic products will be analyzed and set into comparison to PUFs.

2023, © Copyright by authors, Published under agreement with IARIA - www.iaria.org

ACKNOWLEDGMENT

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

We want to thank our research colleagues for supporting us during the concept creation. We also want to acknowledge the research group of Prof. Dr. rer. nat. Hans-Georg Schweiger for discussions about the topic of PUFs for batteries.

REFERENCES

[1] J. Blümke and H.-J. Hof, "Authentic Batteries: A Concept for a Battery Pass Based on PUF-enabled Certificates," in *SECURWARE 2022*, G. O. M. Yee, Ed. Wilmington, DE, USA: IARIA, 2022, pp. 77–81.

[2] 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 [Accessed: 01.06.2023]

[3] "Lithium, Cobalt and Nickel: The Gold Rush of the 21st Century." [Online]. Available: https://faraday.ac.uk/get/insight-6/ [Accessed: 01.06.2023]

[4] E. Wood, M. Alexander, and T. H. Bradley, "Investigation of battery end-of-life conditions for plug-in hybrid electric vehicles," *Journal of Power Sources*, vol. 196, no. 11, pp. 5147–5154, 2011.

[5] E. Hossain, D. Murtaugh, J. Mody, H. M. R. Faruque, M. S. Haque Sunny, and N. Mohammad, "A Comprehensive Review on Second-Life Batteries: Current State, Manufacturing Considerations, Applications, Impacts, Barriers & Potential Solutions, Business Strategies, and Policies," *IEEE Access*, vol. 7, pp. 73 215–73 252, 2019.

[6] L. A.-W. Ellingsen, G. Majeau-Bettez, B. Singh, A. K. Srivastava, L. O. Valøen, and A. H. Strømman, "Life Cycle Assessment of a Lithium-Ion Battery Vehicle Pack," *Journal of Industrial Ecology*, vol. 18, no. 1, pp. 113–124, 2014.

[7] J. F. Peters, M. Baumann, B. Zimmermann, J. Braun, and M. Weil, "The environmental impact of Li-Ion batteries and the role of key parameters – A review," *Renewable and Sustainable Energy Reviews*, vol. 67, pp. 491–506, 2017.

[8] C. Thies, K. Kieckhäfer, T. S. Spengler, and M. S. Sodhi, "Assessment of social sustainability hotspots in the supply chain of lithium-ion batteries," *Procedia CIRP*, vol. 80, pp. 292–297, 2019.

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

[10] 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.

[11] 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 [Accessed: 01.06.2023]

[12] Council of the EU, "Council and Parliament strike provisional deal to create a sustainable life cycle for batteries," Press release, 2023. [Online]. Available: https://www.consilium.europa.eu/en/press/press-releases/2022/12/09/council-and-parliament-strike-provisional-deal-to-create-a-sustainable-life-cycle-for-batteries/ [Accessed: 01.06.2023]

[13] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *Proceedings of the 44th annual Design Automation Conference*, ser. ACM Conferences, S. P. Levitan, Ed. New York, NY: ACM, 2007, p. 9.

[14] T. McGrath, I. E. Bagci, Z. M. Wang, U. Roedig, and R. J. Young, "A PUF taxonomy," *Applied Physics Reviews*, vol. 6, no. 1, p. 011303, 2019.

[15] C. Herder, M.-D. Yu, F. Koushanfar, and S. Devadas, "Physical Unclonable Functions and Applications: A Tutorial," *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1126–1141, 2014.

[16] C. Mesaritakis, M. Akriotou, A. Kapsalis, E. Grivas, C. Chaintoutis, T. Nikas, and D. Syvridis, "Physical Unclonable Function based on a Multi-Mode Optical Waveguide," *Scientific reports*, vol. 8, no. 1, p. 9653, 2018.

[17] M. Hiller, "Key Derivation with Physical Unclonable Functions," Dissertation, Technische Hochschule München, München, 2016. [Online]. Available: https://nbn-resolving.de/urn/resolver.pl?urn:nbn:de:bvb:91-diss-20161219-1311665-1-7 [Accessed: 01.06.2023]

[18] A. Scholz, L. Zimmermann, A. Sikora, M. B. Tahoori, and J. Aghassi-Hagmann, "Embedded Analog Physical Unclonable Function System to Extract Reliable and Unique Security Keys," *Applied Sciences*, vol. 10, no. 3, p. 759, 2020.

[19] Google, "Certificate Transparency: How CT works," 2022. [Online]. Available: https://certificate.transparency.dev/howctworks/ [Accessed: 01.06.2023]

[20] B. Laurie, A. Langley, and E. Kasper, "Certificate Transparency," 2013. [Online]. Available: https://www.rfc-editor.org/info/rfc6962 [Accessed: 01.06.2023]

[21] R. C. Merkle, "A Digital Signature Based on a Conventional Encryption Function," in *Advances in Cryptology — CRYPTO '87*, C. Pomerance, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 1988, pp. 369–378.

[22] K. Huang, Y. Liu, N. Korolija, J. M. Carulli, and Y. Makris, "Recycled IC Detection Based on Statistical Methods," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 34, no. 6, pp. 947–960, 2015.

[23] U. Guin, K. Huang, D. Dimase, J. M. Carulli, M. Tehranipoor, and Y. Makris, "Counterfeit Integrated Circuits: A Rising Threat in the Global Semiconductor Supply Chain," *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1207–1228, 2014.

[24] F. B. de Oliveira, A. Nordelöf, B. A. Sandén, A. Widerberg, and A.-M. Tillman, "Exploring automotive supplier data in life cycle assessment – Precision versus workload," *Transportation Research Part D: Transport and Environment*, vol. 105, p. 103247, 2022.

[25] M. Honic, I. Kovacic, P. Aschenbrenner, and A. Ragossnig, "Material Passports for the end-of-life stage of buildings: Challenges and potentials," *Journal of Cleaner Production*, vol. 319, p. 128702, 2021.

[26] T. Adisorn, L. Tholen, and T. Götz, "Towards a Digital Product Passport Fit for Contributing to a Circular Economy," *Energies*, vol. 14, no. 8, p. 2289, 2021.

[27] 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.

[28] 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.

[29] M. Dubarry, C. Pastor-Fernández, G. Baure, T. F. Yu, W. D. Widanage, and J. Marco, "Battery energy storage system modeling: Investigation of intrinsic cell-to-cell variations," *Journal of Energy Storage*, vol. 23, pp. 19–28, 2019.

2023, © Copyright by authors, Published under agreement with IARIA - www.iaria.org

[30] M. Baumann, L. Wildfeuer, S. Rohr, and M. Lienkamp, "Parameter variations within Li-Ion battery packs – Theoretical investigations and experimental quantification," *Journal of Energy Storage*, vol. 18, pp. 295–307, 2018.

[31] K. Rumpf, M. Naumann, and A. Jossen, "Experimental investigation of parametric cell-to-cell variation and correlation based on 1100 commercial lithium-ion cells," *Journal of Energy Storage*, vol. 14, pp. 224–243, 2017.

[32] D. Beck, P. Dechent, M. Junker, D. U. Sauer, and M. Dubarry, "Inhomogeneities and Cell-to-Cell Variations in Lithium-Ion Batteries, a Review," *Energies*, vol. 14, no. 11, p. 3276, 2021.

[33] M. Kouhizadeh, J. Sarkis, and Q. Zhu, "At the Nexus of Blockchain Technology, the Circular Economy, and Product Deletion," *Applied Sciences*, vol. 9, no. 8, p. 1712, 2019.

[34] T. K. Agrawal, V. Kumar, R. Pal, L. Wang, and Y. Chen, "Blockchain-based framework for supply chain traceability: A case example of textile and clothing industry," *Computers & Industrial Engineering*, vol. 154, p. 107130, 2021.

[35] F. Casino, T. K. Dasaklis, and C. Patsakis, "A systematic literature review of blockchain-based applications: Current status, classification and open issues," *Telematics and Informatics*, vol. 36, pp. 55–81, 2019.

[36] 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.

[37] R. Asif, K. Ghanem, and J. Irvine, "Proof-of-PUF Enabled Blockchain: Concurrent Data and Device Security for Internet-of-Energy," *Sensors (Basel, Switzerland)*, vol. 21, no. 1, 2020.

[38] 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.

[39] Global Battery Alliance, "Battery Passport Pilot," 2023. [Online]. Available: https://www.globalbattery.org/action-platforms-menu/pilot-test/ [Accessed: 01.06.2023]

[40] Battery Pass, "Advancing the implementation of the battery passport in Europe and beyond: Towards a truly sustainable and circular battery life through digital value chains," 2023. [Online]. Available: https://thebatterypass.eu/ [Accessed: 01.06.2023]

[41] Battery Pass consortium, "Battery Passport Content Guidance." [Online]. Available: https://thebatterypass.eu/assets/images/content-guidance/pdf/2023_Battery_Passport_Content_Guidance.pdf [Accessed: 01.06.2023]

[42] Y. Xie, Y. Guo, S. Yang, J. Zhou, and X. Chen, "Security-Related Hardware Cost Optimization for CAN FD-Based Automotive Cyber-Physical Systems," *Sensors (Basel, Switzerland)*, vol. 21, no. 20, 2021.

[43] R. Prosser, G. Offer, and Y. Patel, "Lithium-Ion Diagnostics: The First Quantitative In-Operando Technique for Diagnosing Lithium Ion Battery Degradation Modes under Load with Realistic Thermal Boundary Conditions," *Journal of The Electrochemical Society*, vol. 168, no. 3, p. 030532, 2021.

[44] MARBEL Project, 2023. [Online]. Available: https://marbel-project.eu/ [Accessed: 01.06.2023]

2023, © Copyright by authors, Published under agreement with IARIA - www.iaria.org