The Role of IIoT for Decarbonization shown in the ESTANIUM Network

Gunter Beitinger, Andreas Kind, Maximilian Weinhold, Florian Ansgar Jaeger, Saad Bin Shams

Siemens AG

2023-01-18

CONTENTS

1 OVERVIEW

Effective decarbonization and ESG measures, today, lack transparency of production information in supply chains. For instance, the common practice for calculating upstream emission values based on life-cycle assessment (LCA) databases does not provide actionable and trustworthy product-level emission data.

We developed an IIoT approach to (i) collect direct production values from industrial production facilities and (ii) request indirect production values from suppliers. The approach addresses the need for data sovereignty and protecting confidentiality of production data using an open ecosystem provided by the ESTAINIUM Association.

The ESTAINIUM Association originated from the need to reduce the adverse impact of industrial production on the environment. It was born as association of members that enables them to share the respective product carbon footprint (PCF) along the supply chain in a standardized and trustful way. The technology used not only enables stakeholders to share the PCF but also enables it to be verifiable by the consumer of the product. We call this approach "Trustworthy Supply Chain Exchange" (TSX) and apply it for PCFs. TSX is a necessity when sharing PCFs as single indicator where results are aggregated from primary data across upstream supply chain. Sharing single indicator results enables suppliers to protect confidential process information, but the resulting limitations in transparency require high trust levels.

1.1 INTRODUCTION

The ESTAINIUM Association is a non-profit, non-governmental organisation of entities that are focused on the common goal of alleviating the impact of industrial production. The major component of production-related emissions is *carbon* [1]. Therefore, reducing the production of carbon or compensating its production is imperative to meet the target of cutting emissions by around 45 percent below 2010 levels by 2030 and stay so on track to limit the raise of temperatures to 1.5 degrees Celsius, according to the Intergovernmental Panel on Climate Change (IPCC) [2].

ESTAINIUM works on the governance level to come up with a roadmap for reducing the impact of industrial production on environment, which is the third biggest carbon emitter after coal-fired power station and traffic. This body of work paved the way for an approach called Trustworthy Supply Chain Exchange (TSX), which helps understanding the process of measuring the product carbon footprint (PCF). It laid the foundations for a web application that would help manufacturers in sharing their PCF values with their customers in a verifiable manner. To achieve this, TSX utilizes the verifiable credentials (VC) technology, which is a World Wide Web Consortium (W3C) standard [4]. We apply TSX on PCF data as single indicator where results are aggregated from primary data across upstream supply chain (PCF aggregation).

1.2 PURPOSE

Carbon makes up to 81% of the greenhouse gases released in the environment [1]. The major share comes from CO_2 production, which is the leading cause of global warming. Therefore, it is essential that the production of carbon will be significantly reduced to achieve the goal of *Net Zero* carbon production. Even after extensive studies in today's technologically pervasive world, we still struggle to answer the simple question "What is the carbon footprint of a specific product when it is manufactured?". If the amount of carbon produced during manufacturing cannot be measured, it is very difficult to reduce it.

To close this gap, TSX permits manufacturers to measure the PCF of their goods through standardized calculation methods. Furthermore, it enables them to get their PCF verified through trusted issuers of VC. The shared PCF is also verifiable, and it can be proven that it is released from a trusted issuer.

Once the process of calculating carbon emissions is standardized and transparent, carbon reduction can be achieved in an empirical way. There are several ways of reducing carbon emissions, for example through application of more eco-friendly manufacturing processes or use of renewable energy sources etc. Lastly, manufacturers could compensate their carbon emissions related to a specific product through carbon sinks of an equivalent amount.

1.3 STRUCTURE

In this paper, we will give an overview over the ESTAINIUM Association, TSX and how a trust technology, like verifiable credentials can help sharing PCF data in a verifiable and trustworthy manner to facilitate industry to reach the goal of *Net Zero* carbon emission.

1.4 AUDIENCE

This publication is targeted to interested technology leaders in businesses looking to improve operational efficiency and discover decarbonization and sustainability opportunities.

2 BACKGROUND ON VERIFIABLE DATA SHARING TECHNOLOGY

The goals of TSX can be met in various ways. The most common technique is the adoption of X.509 certificates [5]. To achieve this, PCF certifiers must set up their own Certificate Authority (CA), which is essentially a server that is trusted to issue certificates to requesters. Hence, manufacturers need to reach out to the CA to receive PCF certificates. Another way is the provisioning of a centralized platform, merging manufacturers and certifiers to issue and exchange the PCF to maintain a common ground for data interchange. It is likely that the underlying technology for such a platform would also base on X.509 certificates. Despite the presence of such technologies, the VC technology is much better suited for TSX for PCF.

2.1 INTRODUCTION TO VERIFIABLE CREDENTIALS

Credentials are a part of our daily lives; driver's licenses are used to assert that we can operate a motor vehicle, university degrees can be used to assert our level of education, and government-issued passports enable us to travel between countries or more recent discussion regards a vaccination pass. These credentials provide benefits to us when used in the physical world, but their use on the Web continues to be elusive [4]. Verifiable Credentials technology aims to leap this hurdle in the digital world. In the physical world, a credential might consist of information related

- to identifying the subject of the credential, such as a name,
- to the issuing authority,
- to the type of credential, and
- to specific attributes or properties being asserted by the issuing authority about the subject.

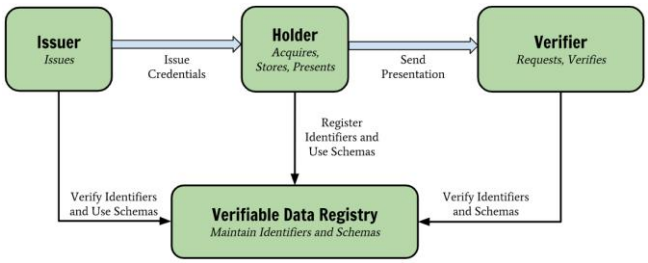

Figure 1. An image showing different parties in the sharing of the verifiable credential and the underlying verifiable data registry that holds the public data, which is used as an anchor for the publicly trusted information. According to *[4]*.

A verifiable credential can represent the same information as a physical credential. The addition of technologies, such as digital signatures, makes verifiable credentials more tamper-evident and more trustworthy than their physical counterparts. It contains claims, which are statements

about a subject. A subject is a thing about which claims can be made. Claims are expressed using subject-property-value relationships. As an example, a claim about the subject “Jane Doe” can have the property “alumni of” with the value “University A”. Lastly, credentials hold proofs, which typically holds information about the cryptographic signatures of the issuer. In our simple example, the issuer would be “University A”. Therefore, the credential would be signed by the private key of the issuer, which can be verified by the issuer’s public key.

There are three different parties involved in the VC data model, which is presented by W3C (see Figure 1) [4]. These are the *issuer, holder,* and *verifier*. A *holder* is a role an entity might perform by possessing one or more verifiable credentials and generating verifiable presentations from them. Examples of holders include students, employees, and customers. An *issuer* is a role an entity performs by asserting claims about one or more subjects, creating a verifiable credential from these claims, and transmitting the verifiable credential to a holder. Examples of issuers include corporations, non-profit organizations, trade associations, governments, and individuals. A *verifier* is a role an entity performs by receiving one or more verifiable credentials, optionally inside a verifiable presentation, for processing. Examples of verifiers include employers, security personnel, and websites.

A *verifiable data registry* is a role a system might perform by mediating the creation and verification of identifiers, keys, and other relevant data, such as verifiable credential schemas, revocation information, issuer public keys, and so on, which might be required to use verifiable credentials.

2.2 PUBLIC KEY CRYPTOGRAPHY (PKC)

To digest the concept of TSX for PCF, it is important to get an overview over the concept of PKC [6]. PKC is the branch of cryptography that enables entities to sign digital documents or issue certificates to other entities asserting attributes about them. The digital signatures and the author of a certificate can be verified through mathematical algorithms.

PKCs create two keys as core components that belong to an entity. These keys are essentially large numbers that enable the signing and verification process of signatures. One of the keys is known as the *public key* the other is known as the *private* (or *secret*) *key*. As the name suggests, the private key is stored in a secure location, whereas the public one is placed in an area that is publicly accessible to everyone.

An entity uses its private key to sign a digital document, which is then sent to a requesting party, depending on the requirement of the application. The party holding the digitally signed document can present the document to a verifying party that considers the contents and then proceeds to verify the signature placed on the document by applying the public key. Thereby, the *integrity* of the document is ensured by a mathematical process and *authenticates* that the document was issued by a trusted entity. The verifier achieves this knowledge by getting the public key of the issuer through a trusted source, the so-called verifiable data registry, and then runs verification algorithms to achieve trust in the presented document.

No other public key can verify the integrity and authenticity of a document other than the mathematical pair of that private key. It is evident that the security of the private key storage is of utmost importance and is kept secure in a wallet application. Furthermore, another important aspect to consider is the storage location of the public key. This is answered by Hyperledger Indy [7], which serves as the trusted public storage for information that needs to be available publicly and provides with a mechanism to ascertain the most recent publicly trusted information.

2.3 HYPERLEDGER INDY

Of the many projects by the Linux Foundation around trust technologies, Hyperledger Indy focuses on digital identities and VCs. After initial contribution by the Sovrin Foundation [7], interest in this project has expanded exponentially with several industry experts contributing and evolving the infrastructure for modern digital identities and credentials.

The verifiable data registry for the VC that TSX utilizes is a blockchain, where copies of data are distributed across several blockchain nodes. The decentralized ledger would serve as the source of trust for publicly available information. The reason to keep it public is to enable anyone to read the information related to public keys of the entities or read the credential schemas, which can be verified by anyone. Information about credential revocation is also pushed onto the distributed ledger so that everyone can access the latest information. In summary, the decentralized ledger acts as a point of trust, from where the authorized entities can read the information needed for verification. However, no actual PCF data is stored in the decentralized ledger.

2.4 DIGITAL WALLETS FOR VERIFIABLE CREDENTIALS

A *wallet* is a software application, which runs on a computing hardware that enables the *subject* to hold the VCs that are issued to it. A wallet can hold multiple credentials from different issuers. It also can search for the credential attributes, which would satisfy the *verifier's* request for authentication.

There are different ideas evolving for wallet application. Some are designed for smart phones, while others focus on cloud platforms. For more information refer to the Hyperledger Aries Project, which is at the forefront of developing wallets for applications based on Hyperledger Indy [8].

2.5 MOTIVATION TO USE THE VC TECHNOLOGY

Talking about a centralized platform, includes the reliance on a single party controlling the platform. This does not distribute trust over multiple parties and is not accepted in industries anymore. For this reason, such a centralized approach is avoided.

Using the X.509 certificates to provide verifiable PCFs is a strong contender. However, there are few shortfalls: Firstly, the setup of the Certificate Authority (CA) for each certifier is an added IT cost which they might not want to undertake. Secondly, there needs to be an application layer

on top of the certificates to aid in the exchange. ESTAINIUM association could undertake standardization for such a layer, however, it would be a huge effort.

Hence, the Verifiable Credential technology seems to be more suitable, as Hyperledger Indy provides an out of the box application layer that supports data exchange. The certifiers only need to be listed as trusted issuers in the verifiable data registry without the need to run any additional IT infrastructure to issue VCs for PCF. Furthermore, the VC technology is an open standard with opensource libraries available. Potentially, any interested party can develop their own application and be ready to receive VCs and exchange PCF with drastically reduced efforts as compared to the techniques.

3 BACKGROUND ON PCF ACCOUNTING

There exist a variety of norms and standards, which provide guidance for PCF accounting. The basis are life cycle assessment (LCA) standards such as ISO 14044 [9]. With PCFs being a single score impact category extract from a Lifecycle Assessment, more impact category specific norms such as the ISO 14067 [10] or documents such as the GHG-Protocol for PCF accounting were defined. They partially diverge due to their wide applicability, but still leave enough room for interpretation. Hence, for comparability reasons, individual industries defined the Product Category Rules (PCRs) or even Product Specific Rules (PSRs) and derived requirements (sub specifications of PCRs). They intend to provide a high comparability of LCA results for PCFs within homogeneous product groups. The European initiative Product Environmental Footprint (PEF) tried to tackle this challenge. All these documents assume a conventional assessment of PCFs, with one practitioner modelling the entire value chain, including the process steps outside the practitioner's foreground system. Therefore, the practitioner must make assumptions with industrial averages or request life cycle inventory data from suppliers. For confidentiality reasons, suppliers are commonly reluctant to share this data. The WEF white paper "Share to Gain" [11] makes it even clearer. For successful collaboration in the context of data sharing, stakeholders need an understanding how to promote value together. Three factors are identified as key for success, all covered by the TSX approach. First, a clear value proposition for data sharing, second a mutually beneficial agreement and third the use of secure technologies and common standards are required. PCF aggregation solves this issue, with a practitioner connecting a PCF of an upstream supplier to their life cycle inventory – instead of an emission factor from a database. Initiatives such as Pathfinder (WBCSD) and others are currently defining PCF aggregation specific standards with data exchange formats for intra-value chain exchange of PCFs and fit frameworks. Apart from formats and rules for the calculation of PCFs, third party verification of results is an essential part of TSX. Scalable auditing mechanisms for PCFs on company level enable significant cost savings compared to individual PCF verifications. A standard for PCF programs of companies to be audited would enable a significant scaleup and increase in trust among sharing network participants.

These currently established standards of measuring the environmental impact of industrial production will become the foundation of the TSX for PCF calculations. They will be used in unison with the VC technology to enable sharing of PCF data between companies and stakeholders.

3.1 AIM OF THE TSX FOR PCF

TSX does not necessarily require new standards to be written from scratch. Nonetheless, further efforts to align the existing ones will improve the PCF quality. Interoperability can be made transparent by either requesting additional parameters when documenting a PCF or limiting the choices of practitioners with PCF accounting. A common level of ambition must be identified, which is practical and still feeds the purpose of giving people and companies an effective option to track, reduce and compensate their emissions. Currently, TSX's goal is to enable sharing of PCF data in supply chain and later other ESG data, too.

The major participation in the TSX network will come from industry and the certifiers or accreditation bodies. The industrial partners would be aiming to reduce their adverse impact on the planet. The certifiers or accreditation body would be the trust anchors that verify the PCF of the manufacturers in a supply chain.

4 CORE APPROACH

The approach to create a digital way of calculating and communicating PCF values is called TSX for PCF. For that, it is imperative that all parties in the supply chain can share their contributions with ease. Once we have streamlined the process of sharing PCF values, we envision that it would be much easier for companies to reach the goal of *Net Zero* carbon emissions. Furthermore, we focus on the core approach for TSX for PCF that other parties can adopt to fulfil the need to measure, share, and compensate carbon emissions.

4.1 MAPPING TSX FOR PCF PARTICIPANTS

The VC model is a powerful way to share the PCF values between parties within a supply chain, particularly because of their nature of being cryptographically verifiable. This brings an important aspect of trust into the system, which is also a requirement from a business perspective. We envision different stakeholders becoming part of the TSX network and having different roles depending on their business objectives. To utilize VC technology, we need to map different stakeholders from the TSX network to the different roles within the VC Model.

Certifiers can validate the PCF values of other stakeholders as third-party certification bodies, thereby bringing trust into the ecosystem. Consequently, they take the role of VC issuers. The manufacturers and their suppliers are holders of verifiable credentials. Whenever manufacturers want to calculate the PCF of a product, they contact their suppliers for a credential with the PCF values and adjoining data, which are the required input values to calculate the PCF. The supplier would share the requested information in form of a verifiable credential. The manufacturer adds the respective PCF value to the calculation of the PCF. It is important to note that the manufacturer would also play the verifier role once it has received the credentials from its suppliers. Furthermore, exclusive verifiers in the network can act as additional role, which can be taken by auditing authorities, or end customers that buy the product and need to make an informed decision about the PCF before purchase.

4.2 TRUST ASSUMPTIONS FOR TSX FOR PCF

We have seen that there are multiple parties in the entire eco-system for TSX for PCF, which can broadly be classified into certifiers, manufacturers, suppliers, auditing authorities and end customers. The roles of the VC model are evident as explained in the previous section. However, we need to have some trust assumptions.

Certifiers are the trusted third parties and other participants trust them to ensure proper behaviour within the TSX network. They are the trust anchor that vet the manufacturer's processes and aid in issuing credentials that can be trusted by everyone within the TSX network. Certifiers are also trusted to follow the applicable standards and regulations in the LCA of products for PCF calculation.

The verifiers, whether they are manufacturers, the end customer, or some auditing authority assume that the certifiers are trustworthy. Furthermore, the credential owners are assumed to trust the certifiers for producing correct credentials, and that it reflects the true PCF value.

Additionally, it is assumed that the PCF values are linked to the corresponding real-world product and provide its accurate PCF. Lastly, for TSX for PCF, we also assume that the verifiable data registry is up-to-date, and integrity protected, and only authorized entities can post on the verifiable data registry.

5 EXEMPLARY APPLICATION OF CREDENTIAL ISSUANCE AND SHARING

VC technology is core element of the TSX for PCF process. Once a manufacturer starts building a product for its customers, it is commonly built with products from other suppliers. Figure 2 shows an example product of a Programmable Logic Controller (PLC), which requires among other things a plastic housing, which is sourced from one or more suppliers.

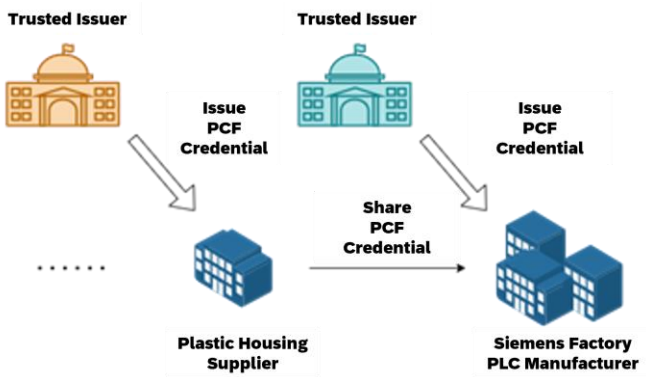

Figure 2. The figure shows the process of sharing PCF credentials with a customer that uses a product in its manufacturing process. The VC for a PCF is issued by *trusted issuing authorities* that make sure that the PCF is being calculated according to the defined processes.

The list of all components describing the final product is referred to as the *Bill of Materials (BoM)*. When the manufacturer calculates the PCF of its PLC, it iterates through the BoM, reaches out to the suppliers, and ask for the PCF of each component. The supplier receives the request to share

the PCF of the sold component and reaches out to a trusted issuer within the TSX network. The issuer then takes the request for a VC for the product and validates that the process requirements are followed for calculating the PCF. It creates a VC for the product and cryptographically signs the VC so that its origin can be approved and shown that it indeed is coming from a trusted source within the TSX network.

After VC creation, the issuer sends the VC for the PCF to the requesting party. Upon receiving the VC, the supplier stores it in the digital wallet and therefore fulfils the customer's request. According to our example and to Figure 2, this refers to the PCF of the PLCs plastic housing.

Upon receiving the VC for the PCF of the supplier, the manufacturer can verify that the trusted issuer signed the VC. Once the public key is retrieved from the data registry provided by Hyperledger Indy, it is used to determine the integrity of the VC and it is ascertained, if a trusted issuer in the TSX network in fact issues the VC. This process of receiving and sharing the VC for PCF is repeated with all suppliers of PLC components listed in the BoM. This enables the manufacturer to calculate the PCF for all components. The manufacturer measures the energy consumption as well as the heating carbon footprint generated by the assets of its own shopfloor. All these carbon emissions are then aggregated to calculate the PCF. After completion, the manufacturer reaches out to a trusted issuer to get a VC for the PCF of the finished PLC, which it can share with customers.

6 CONCLUSION

The existence of climate change is undeniable. Hence, it is important that we join forces to keep our planet inhabitable for future generations. The vision of ESTAINIUM as an association that promotes the use of IIOT technology, such as verifiable credentials, helps us achieve this by enabling manufacturers to be sustainable in their processes and to manage and reduce the impact of industrial production on our climate. Therefore, TSX as an approach for measuring and sharing PCF data through the VC technology can help us in achieving the goal of *Net Zero* carbon production since data is shared for a greater purpose than just to monetarize it. Despite many uncertainties with centralized and closed ecosystems, the TSX concept delivers an approach for successful data sharing due to its inbuilt trustworthiness and interoperability.

7 REFERENCES

[1] Agency, United States Environmental Protection. Overview of Greenhouse Gases. Greenhouse Gas Emissions. [Online] *https://www.epa.gov/ghgemissions/overview-greenhouse-gases*.

[2] IPCC, 2018: Global Warming of 1.5°C. [Online] *https://www.ipcc.ch/site/assets/uploads/sites/2/2019/06/SR15_Full_Report_Low_Res.pdf*

[3] https://www.edie.net/news/11/Boris-Johnson-pledges-action-on--coal--cars--cash-and-trees--at-COP26/

[4] World Wide Web Consortium (W3C). Verifiable Credentials Data Model 1.0. [Online] 2019. *https://www.w3.org/TR/vc-data-model/*.

[5] Gerck, Edgardo. "Overview of Certification Systems: x. 509, CA, PGP and SKIP." (1997).

[6] Diffie, Whitfield. "The first ten years of public-key cryptography." Proceedings of the IEEE 76.5 (1988): 560-577.

[7] Sovrin Foundation. Frequently Asked Questions. What is Hyperledger Indy? [Online] *https://sovrin.org/faqs/*.

[8] The Linux Foundation. Hyperledger Aries. Github. [Online] *https://github.com/hyperledger/aries*.

[9] Finkbeiner, Matthias, et al. "The new international standards for life cycle assessment: ISO 14040 and ISO 14044." The international journal of life cycle assessment 11.2 (2006): 80-85.

[10] García, Rita, and Fausto Freire. "Carbon footprint of particleboard: a comparison between ISO/TS 14067, GHG Protocol, PAS 2050 and Climate Declaration." Journal of cleaner production 66 (2014): 199-209.

[11] World Economic Forum. In collaboration with Boston Consulting Group. „Share to Gain: Unlocking Data Value in Manufacturing. January 2020