Trustworthy Supply Chain Exchange for Product Carbon Footprint

Saad Bin Shams
Cybersecurity & Trust
Siemens AG
Munich, Germany
saad.shams@siemens.com

Andreas Kind
Cybersecurity & Trust
Siemens AG
Munich, Germany
andreas.kind@siemens.com

Florian Ansgar Jaeger
Digital Industries
Siemens AG
Berlin, Germany
florian_ansgar.jaeger@siemens.com

Gunter Beitinger
Digital Industries
Siemens AG
Amberg, Germany
gunter.beitinger@siemens.com

Ionut Alexandru Leonte
Cybersecurity & Trust
Siemens AG
Bucharest, Romania
alexandru.leonte@siemens.com

Maximilian Weinhold
Digital Industries
Siemens AG
Munich, Germany
maximilian.weinhold@siemens.com

Vinh Pham
Cybersecurity & Trust
Siemens AG
Munich, Germany
vinh.pham@siemens.com

***Abstract*— Product Carbon Footprint (PCF) is a systematic measure of the greenhouse gases (GHG) emissions in creating a product. There are several standards for PCF accounting, but sharing the PCF in a verifiable manner is not standardized. The current processes typically rely on sharing digital documents that assert what is typically an estimated and static PCF. In this paper we present our Trustworthy Supply chain eXchange (TSX) approach and compare different technologies that can be used to implement it. Our approach helps the manufacturers to compute the dynamic PCF of products and enables sharing the PCF with other stakeholders by technically solving the confidentiality concerns which led to estimated and static PCFs in the past. We achieve this with the use of the selective disclosure feature in the verifiable credential (VC) technology provided by the AnonCreds VCs. Moreover, the PCF sharing is integrity protected and establishes the authenticity of the PCF data. We use blockchain as an infrastructure that aids in sharing verifiable PCF across organizations and countries. Lastly, our approach has the flexibility to be adopted for any standard of PCF accounting.**

Keywords—Verifiable Credentials, Product Carbon Footprint, Blockchain.

I. Introduction

In recent years action against climate change has come to the forefront. World leaders have stressed the need to limit the global warming temperature increase to 1.5°C by the end of the century in the Paris agreement. Consequently, the topic of measuring the climatic impact of manufacturing products and carbon emissions of corporations is now in the limelight. Product carbon footprint (PCF) is a systematic process of measuring the greenhouse gas emissions of products during its lifecycle. There are many norms and standards for PCF accounting. The foundation is set by the life cycle assessment (LCA) standards such as ISO 14044 [1]. There are other category specific norms that have been introduced as well, such as ISO 14067 and the GHG-Protocol [2]. They partially diverge but due to their wide applicability, they still leave room for interpretation. This is why for comparability reasons, individual industries have defined Product Category Rules (PCRs) or even Product Specific Rule (PSR) (sub specifications of PCRs) [3], where the intent is to provide comparability of the LCA data, more specifically PCF data within homogenous product groups.

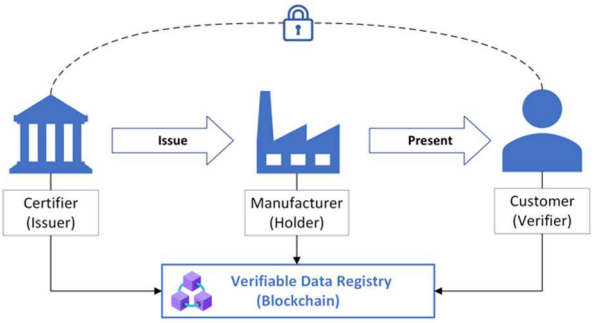

Figure 1: A scenario showing the exchange of verifiable credentials for Product Carbon Footprint (PCF). The Certifier issues a verifiable credential to the manufacturer, who uses it to prove to the customer about the PCF of the product they purchased.

Despite all these norms and standards, carbon emissions reporting is not mandatory for corporations [4]. However, there are indications from regulators that this will change. Governments around the world would be mandating companies to track and report the carbon emissions of their products. Consequently, this creates several problems.

Firstly, there is no standard way for a manufacturer to share their PCF in a verifiable manner with their customers. Therefore, manufacturers cannot compute dynamic PCF for their products and have to rely on averages and estimates to arrive at static PCF values computed with the help of Excel sheets. A task which is performed by a practitioner experienced in this domain [5]. Currently, corporations typically rely on third party certifiers that provide a certification for the processes of manufacturing and look at the corporations' emissions and compensations holistically to provide estimates on the PCF. Such certifications can be seen as labels on the product that might show that a product is carbon neutral. Whereas, in reality the PCF value is dynamic in nature and changes as the inputs to the process of manufacturing changes over time.

Secondly, the certification documents for PCF include information that is considered to be trade secrets, such as supplier information, which inhibits the companies to share the certified PCF value. Therefore, we need a mechanism to selectively disclose data from the PCF certification. The shared data should be verifiable, which means that its provenance and authenticity can be proven. Moreover, we need to achieve this verifiability amongst multiple companies and across the globe.

Lastly, as highlighted earlier, there are multiple norms and standards for computing the PCF. Hence, we need an approach that is flexible to represent PCF information based on all of these standards for different industries.

A. Contributions

In this paper we present a blockchain based approach that tackles these challenges. In particularly we,

- compare the different technologies that can aid in sharing of PCF in a verifiable manner. Presented in section IV.
- present an approach that helps in establishing an eco-system for sharing dynamic PCF between the stakeholders based on different standards and norms for PCF accounting. Presented in section V.
- present the approach in which the manufacturer can selectively disclose certified attributes in a PCF certification while still maintaining verifiability and confidentiality of the data. Presented in section V-C.

We have also implemented our approach of tracking, sharing, and verifying dynamic PCF as a cloud-based application called SiGREEN [6].

II. Trustworthy Supply Chain Exchange (TSX) and its Requirements

In the previous section we highlight the problems with the current processes of PCF accounting and sharing. To address these challenges, we will present our approach which we refer to as Trustworthy Supply chain eXchange (TSX). The requirements for our approach based on the challenges are as follows.

A. Dynamic nature of PCF

We have seen earlier that currently the calculated PCFs are static in nature. In reality, the PCFs are dynamic, and their value depend on inputs at the time of manufacturing. As an example, the PCF of a product manufactured in winters might be higher than the same product produced in summers because in the winters additional energy might be required for heating. Furthermore, there might be changes in the manufacturing processes that can alter the PCF and it should be reflected in the calculated PCF. The products are manufactured through complex conversions from raw material into finished products that are later distributed to end customers. The network of resources, activities, people and organization involved in turning raw materials into final products is referred to as a supply chain. The flow of materials that go from raw material extraction to manufacturing to distribution to the end customers is referred to as *downstream*. The reverse flow is known as *upstream*. A product usually goes through multiple stages of manufacturing and at each stage additional components can be added together to make a product with more value addition (a simple supply chain with multiple stages of manufacturing can be seen in Figure 3). Therefore, at each stage the PCF of each component is required to compute the PCF at that stage. Any change in the PCF of the component should be propagated through the supply chain. This highlights the significance of the dynamic nature of PCF. Hence, one of the core requirements for the TSX approach is that it supports computation of dynamic PCF.


```
{
  "PCF certificate identifier" : "v1.3",
  "PCF Certification Date" : "05-03-2023",
  "Product Identifier" : "001-002-003",
  "Product Name" : "Computer Motherboard",
  "Bill of Material" : [
        {"Plastic housing supplier" : "Plastic ltd.",
        "Plastic housing PCF per unit" : "2",
        "Unit for PCF" : "kgCO2e"},
        {"CPU supplier" : "Power Management Unit Inc.",
        "CPU PCF per unit" : "3",
        "Unit for PCF" : "kgCO2e"}],
  "Scope 1 contribution" : "10",
  "Scope 2 contribution" : "15",
  "Scope 3 contribution" : "5",
  "Aggregated PCF" : "30",
  "Aggregated PCF unit" : "kgCO2e"
}
```


Figure 2: A simple PCF form shown in the form of a JSON structure (in this figure represents dummy PCF data). It is divided into different attributes and their respective values. Attributes such as "Bill of Materials" is confidential for the manufacturer.

B. Providing trustworthiness and verifiability

Another important requirement for TSX is to make sure that the PCF calculation is verifiable and trustworthy throughout the supply chain. We should make sure that the PCF data is computed properly, it is integrity protected and is authentic. The manufacturers might have an incentive to under report their PCF so that their products are chosen over their competitor's. It is important that we ensure that the PCF is calculated to the maximum accuracy, and it is not tampered with as it is propagated through the stages of the supply chain. Similar to what we have today, this is ensured with the help of trusted third-party certifiers. At each stage the PCF data is certified and issued by the certifiers. To achieve verifiability, we use cryptographic digital signatures that provide us with integrity protection of certifications and to prove that it is issued from a trusted certifier. Therefore, upon receiving the certified PCF, a verifier can ascertain that the data is vetted by a trusted third-party certifier.

C. Confidentiality in supply chain through selective disclosure

For the TSX approach we want to maintain the confidentiality of data in the PCF certifications throughout the supply chain. As mentioned earlier, currently the companies are not mandated to share their PCF. Therefore, they do this activity to gain better insights in their processes, to improve them for the environment and to be ready to comply to possible incoming regulations. They primarily perform this with the help of a practitioner on a corporate level, computing their corporate carbon footprint and estimating their PCFs. If these PCF certification documents have to be shared, then they must be shared in their entirety with the requesting party. This inhibits the manufacturers from sharing PCF information because the PCF certification document might include confidential information that they are not willing to share with any other party. Example of such information is of the components that goes into making the entire product. This is known as the Bill of Materials (BoM) of the product (as shown in Figure 2). The document contains the information of the suppliers of each component and is a closely guarded secret for each manufacturer and is kept

confidential. Consequently, we end up with estimates of PCFs or static PCFs due to this inability to share the PCF. Hence, we need a mechanism that provides a way to share parts of the PCF certification while still maintaining verifiability of the data.

D. An eco-system of heterogenous industries

Lastly, we want to provide an eco-system where the stakeholders from different industries can come together and share the PCF amongst each other. The approach should be flexible enough to represent data based on standards for different industries. Furthermore, we want mechanisms where the origin of data can be verified across companies and around the globe.

III. Related Work

The current literature in the realm of PCF sharing is not extensive. However, there are still some ideas with a similar goal. Yuting Pan et al. present an approach for carbon trading using blockchain [7]. This paper focuses on carbon trading rather than PCF sharing. Carbon trading is when companies that have a surplus of carbon emissions sell a part of their share to the companies that have exceeded their limit.

Antonio Cruz et al. put forward an approach for PCF tracking [8]. They primarily talk about each company tracking PCFs of their own products. They also propose a smart contract-based platform for traceability of products and organizations. All of this is gathered into a platform, which highlights the contributions of each manufacturer in the final PCF. This is also visually shown in the form of a tree for the end customer, who can then take an informed decision while choosing a product to buy. However, in our context their approach does not satisfy our requirement of confidentiality as explained in section II-C. The platform fails to achieve this requirement because in their approach any party can track which suppliers contributed to making a certain product. Furthermore, the platform provides a user interface for companies to input their own values. Consequently, the PCF calculated is not validated by a third party and the trustworthiness of the data is limited.

Chunhua Ju et al. present an approach to track carbon footprint of organizations on the blockchain [9]. The primary goal of the authors in this paper is to eliminate corruption and to prevent manipulation. It is a hybrid solution, which uses both on-chain and off-chain storing mechanisms. The traceability is done off-chain and the verification is done through on-chain data. The entire application focuses on providing auditing capabilities for tracing and verifying carbon emissions of companies and products when it is shared. The shortcoming in this approach is like the one presented before. Their approach does not warrant the vetting of data from third-party certifiers. Therefore, the PCF information itself would have limited trustworthiness. Furthermore, their approach is inefficient for practical purposes. The paper itself highlights the inefficiency of traceability as the number of interactions from participant increase.

IV. Technology comparison for TSX

There are several technologies present that enables the sharing of verifiable data between partners. To have an organized discussion the technologies can be divided into two categories. One is the infrastructural technology that provides a framework for sharing verifiable data, the other is of data containers that hold the actual PCF data. We will first present the infrastructural technologies and then take a deeper look into the data containers.

A. Infrastructural technologies

1) Public-Key Infrastructure (PKI)

A PKI provides public keys of entities and a mechanism to verify their authenticity using public-key certificates including a possibility to check their revocation status [10]. The technology has been around for decades and is standardized in ITU T X.509. When we talk about creating an eco-system of heterogenous stakeholders for sharing the PCF then reaching a consensus on which PKI instances to trust becomes challenging [11]. According to the requirements of the TSX approach laid out in section II, we need to find a way where multiple companies can share verifiable PCF data across organizations around the globe. Consequently, in a PKI-based approach, as the number of companies grow, establishing trust across multiple PKIs become difficult. Furthermore, the handling of certificate validation paths and revocation information can become complex. Where both are required to create an efficient and secure ecosystem for sharing verifiable PCF.

2) Hyperledger Indy (HLI)

HLI is one of the projects under the umbrella of Hyperledger Foundation [12]. It is an identity and privacy focused blockchain technology. Like a PKI, it can serve as the root of trust and as a mechanism for distributing the public keys of entities. However, in contrast to a PKI, it achieves this by storing them in a publicly readable *verifiable data registry*, which is realized in the form of a blockchain. Furthermore, it provides a cryptographic revocation mechanism that is privacy preserving and uses public cryptographic accumulators. This enables the users to prove the revocation status of VCs without revealing their details to others. In comparison, a PKI typically relies on certificate revocation lists and reveals more details about certificates and their holders. Moreover, in the HLI blockchain all participants of the network operate an HLI node and have a common trusted blockchain where all the public keys are stored. Therefore, the stakeholders share a common trust domain and thus avoid political and cumbersome discussions on how to establish trust in PKI instances. However, reaching a common understanding on trust establishment and on operating HLI nodes securely is still needed. There are multiple HLI network instances running today. One of such networks is the IDunion network in the European Union, which is working towards recommendations on these open points. These must be adopted by all the operators to keep the entire network secure.

B. Data containers

1) X.509 certificates

There are two main types of X.509 certificates, both of which are handled by PKI. Public-key certificates (PKC) are very commonly used to securely relate identities with their public keys. Attribute certificates (AC) can be used to relate entities with their attributes. The latter have seen only limited use in industry. Using X.509 certificates as data containers for verifiable PCF is possible, however there are a few issues

associated with them. The format of PKC is strict and is meant to share and verify public keys of an entity. The optional X.509v3 extensions can be used to represent PCF data, but we do not need to use the main feature of PKCs which is the included public key. For ACs, no public key is mandatory to be included, and we can represent any attribute that might be needed to represent the PCF data. Unfortunately, for both these types of certificates it is required to share the entire certificate, including the identity of the holder, with the receiving party. As we pointed out in the requirements in section II-C, sharing the entire certificate is not desirable because some of the included information might be confidential for the manufacturer.

2) AnonCreds Verifiable Credentials

Verifiable Credentials (VCs) are a new technology for sharing verifiable data that are being standardized at W3C [13]. VCs are like the physical credentials a person stores in their wallet such as a driver's license, but they are digital representations of the same data. VCs require software applications called wallets to store this digital form of credentials. AnonCreds VCs are the type of VCs which are inherently supported by HLI (introduced in IV-A). AnonCreds VCs, like all VCs, relies on a trust triangle which is shown in Figure 1. The issuer of VCs stores its public keys in the *verifiable data registry (blockchain),* and it uses the corresponding private key to digitally sign the issued VC to the holder. The holder stores the VC in its wallet. Upon request from the verifier, the holder prepares the presentation for the verifier in the form of a verifiable proof. Once the verifier receives the verifiable proof, it reads the verifiable data registry to get the public keys of the issuer it trusts and then validates the data presented in the verifiable proof. With this process the verifier can ascertain that the information presented is not tampered by the holder and that the data presented in the verifiable proof is coming from the trusted VC issuer.

Verifiable proofs with AnonCreds VCs solve the challenges of confidentiality presented in section II-C, with the feature of selective disclosure. This enables the holder of an issued VC to control which attributes from within that VC the verifier can or cannot see, when providing a verifiable proof. Thus, maintaining confidentiality and cryptographic verifiability of VCs. Additionally, AnonCreds VCs provide zero-knowledge proof-based mechanisms to prove the value of the PCF to be above or below a certain threshold value instead of revealing the actual value itself. Lastly, another benefit of using this technology is that they provide flexibility in the format of the data that can be shared because there are no strict requirements on what the format of the VC should be. The stakeholder can define a format that is relevant for their use case. Hence, this aids in creating sophisticated formats of the VCs based on various PCF accounting norms and standards introduced in section I and the requirement in section II-D.

3) Selectively Disclosable JSON Web Tokens (SD-JWTs)

SD-JWTs are another form of VCs which we believe are important to compare in the context of data containers for verifiable PCFs. These are a relatively new specification which are being standardized in IETF [14]. SD-JWTs are essentially JWTs that provide the feature of selectively disclosing the attributes to a verifier. The attributes that need to be selectively disclosed are processed by the issuer by adding a salt to the attribute name and value. The individual attributes are hashed and replaced in the original JWT. These attributes are known as a selectively disclosable claim. The entire SD-JWT goes through this process and is then sent to the holder along with the respective salts of each attribute which are referred to as disclosures. The holder shares the entire SD-JWT with the verifier where the attributes are in the hashed form. When the holder wants to disclose any attribute to the verifier then they share the disclosure (salt, attribute name and value) for the specific attribute. The verifier can recalculate the hash to verify that the raw value of the attribute is in the shared SD-JWT.

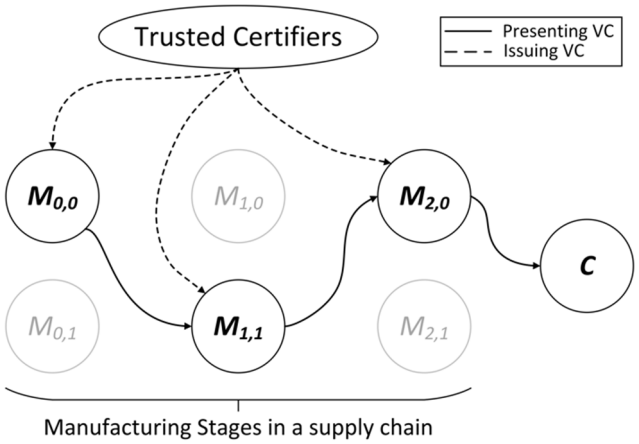

Figure 3: A simplified supply chain showing different stages of manufacturing. Each stage's manufacturer requests a verifiable credential for its PCF from the trusted certifiers. It is then shared in a verifiable manner with the downstream manufacturer. The downstream manufacturer uses the shared PCF and adds their own contribution to the PCF, requests a VC for it and the chain continues to the end consumer 'C'.

The use of SD-JWTs provides us with the benefit of selective disclosure, the flexibility of using any accepted asymmetric cryptographic algorithms for cryptographic verifiability, and the flexibility in their format depending on the application. However, the problem they pose is that they are currently not supported by either of the infrastructures that we have presented in IV-A. Theoretically they can work with either of the infrastructural technologies and would also support the requirements for TSX. However, they are still in the draft phase within IETF and requires more work before they can be used in productive use cases.

C. Motivation to use HLI with AnonCreds VCs

HLI with AnonCreds VCs is a complete technology solution from the Hyperledger Foundation which is available for productive use. They work together to provide a holistic infrastructure that can be used to share PCF data in a verifiable and privacy-preserving manner. HLI provides a mechanism to distribute and share public keys via the blockchain. Compared to PKI, it aids in reducing the organizational and political challenges that might arise when working with multiple stakeholders in the ecosystem from heterogenous industries. The HLI blockchain nodes can be operated by multiple stakeholders to create a common ledger that stores public information for verification of VCs for PCF. Consequently, the blockchain helps in providing an infrastructure that enables the sharing of verifiable PCF data across companies and countries.

AnonCreds VCs provide the data container capabilities to share verifiable PCF. Furthermore, they are flexible to support any format defined by the standards and norms for PCF accounting presented in section I. Additionally, AnonCreds VCs provide the features of selective disclosure, which satisfies the requirement for providing data confidentiality for the manufacturers in our TSX approach.

V. Our Approach

For the TSX approach it is imperative that all parties in the supply chain can share their carbon emissions for the product that they manufacture with ease. There are three main types of stakeholders within the TSX approach. Firstly, there are the manufacturers who want to share the PCF with other stakeholders. Secondly, there are the certifiers that serve as the trusted third party within the system. They vet the processes and calculation of the PCF at each step of the supply chain. Lastly, we have the consumers of the verifiable PCFs. They can be either the next stage manufacturers or the end customer of the product.

A. Mapping of TSX stakeholders to roles in VC ecosystem

As pointed out earlier, there would be different stakeholders becoming part of the TSX network with 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 as shown in Figure 1.

There are primarily three stakeholders in the TSX approach. When mapped to the VC data model in Figure 1. The stakeholders are as follows:

- *Certifiers*: VC Issuers
- *Manufacturer*: VC Holder
- *Downstream Manufacturer / Customer / Auditing Authority*: VC Verifier

Certifiers are the ones that issue the VC for the PCF to the *manufacturers*. The certifiers, like in the real world, serve as the trusted third parties in the TSX approach that vets the manufacturing processes and provides a VC for PCF. This ensures that the PCF received by the *downstream manufacturer*, which is aggregated along the entire supply chain, is trustworthy at each stage.

The *manufacturers* are the holders of the PCF VCs. It is important to note that all the manufacturers would have to share their PCF data to their *downstream customers* and request PCF data from the *upstream suppliers*. The VCs are primarily issued by the *certifiers*. However, in case the manufacturer does not have a valid and certified PCF of a product to serve the request of its customer it would have the option to issue a VC itself to fulfill the request while it initiates the process of getting a certified PCF. Such VCs are *not* considered to be as trustworthy because they would be assertions by the manufacturers themselves.

The verifier's role can be taken by multiple stakeholders in the TSX approach. The most common one would be the *customers* of products. The customer can also be the next stage *downstream manufacturer* that uses a component to create a product themself. Therefore, the manufacturer would also be the verifier of the PCF information at some stage of the production in the entire supply chain. Lastly, the verifier can also be an auditing authority or a governmental agency that could request PCF data in a spot check or even when providing compliance certifications to manufacturers and companies.

B. VC issuance and PCF calculation

In order to fully explain how the credential issuance process works we will explain it from the reference of a manufacturer, which extracts the raw materials to create a product for the next stage of production. We will use the notation $M_{k,i}$, where k refers to a particular stage in the supply chain and i refers to a specific supplier at a particular stage. This can be visualized in the Figure 3 which shows a simplified supply chain. On the left side we have the manufacturers that extract the raw materials and create a product that is used in the next stage to create a value-added product. This continues until the product reaches the final consumer of the product.

Taking the supply chain shown in Figure 3 as an example, let's assume that the last stage manufacturer $M_{2,0}$ receives the request from the customer C to share the verifiable PCF. When $M_{2,0}$ receives the request for a PCF credential it would check if it already has an issued VC for the product in its wallet. If the credential is already present in its wallet, then the process is straightforward. $M_{2,0}$ would use the already present VC, choose which attribute it wants to share from the VC, create a verifiable proof from it and share it with the customer.

Now let's take a deeper look at the scenario where the VC is not present in its wallet. The first task that $M_{2,0}$ performs is to reach out to its direct suppliers ($M_{1,1}$ in Figure 3) and ask for the PCF of the components that were bought from them. Similarly, $M_{1,1}$ requests its suppliers for verifiable PCF in the form of VC until we reach the supplier that creates a product directly from the extracted raw material. Once $M_{1,1}$ receives the PCFs as a VCs from all of its suppliers, it can request a VC from the trusted certifiers that it can use to fulfill the request of its customer $M_{2,0}$.

Once $M_{2,0}$ has verified all of the VCs of PCF of each component, they proceed to add all the verified PCF and add in their own emissions to reach the aggregate PCF for manufacturing their product. On a high level the total PCF for the product can be calculated with the following formula:

$$\boldsymbol{PCF}\ (\boldsymbol{product}) = \sum \boldsymbol{PCF}_{\boldsymbol{Component\ from\ supplier}} + \sum \boldsymbol{PCF}_{\boldsymbol{Own\ manucaturing}}$$

Here the $\sum \boldsymbol{PCF}_{\boldsymbol{Component\ from\ supplier}}$ denotes to the PCFs of the components that goes in making the product. Strictly speaking, this means requesting the PCF for each component directly from its suppliers. In the latter part of the presented formula, $\sum \boldsymbol{PCF}_{\boldsymbol{Own\ manucaturing}}$, denotes to the carbon emissions from the manufacturer $M_{2,0}$. These include the emissions from the manufacturing processes at the factory, the emissions that are a result from the purchased energy supply for the factory to run and it would also include carbon emissions of services that are used by the manufacturer. These are typically indirect carbon consumptions that go into manufacturing a product.

Once the manufacturer $M_{2,0}$ has the PCF calculated for the product they then share this information with a third-party certifier. The certifier validates the information and issues a VC to the manufacturer. The manufacturer can store this VC in their wallet and upon request share the verifiable proofs with the verifier, to share the PCF of their products.

C. Verifiable credential sharing

Verifiable credentials are shared through the process called "*Verifiable Presentation*". Once the

manufacturer receives the request to share the PCF for a certain product it produces, it would go through its wallet to search for a credential that satisfies the request. As pointed out earlier, the manufacturer has the option to select a subset of attributes to share from the VC that can satisfy the request of the verifier. From the VC, it generates a verifiable proof which is then shared with the verifier. The customer or the verifier can also ask to share certain additional attributes that it might need to enhance its trust in the PCF values of the product. In the event of a clash where the manufacturer is reluctant to disclose those attributes, then the zero-knowledge proof feature of AnonCreds can be utilized. An example of such a scenario could be where the customer wants to know the PCF of a specific component within the product of the manufacturer. If the manufacturer does not want to disclose that exact PCF then the customer can instead request the manufacturer to prove that that PCF is below a numerical value of interest for the customer. That way, the component's exact PCF remains confidential. Lastly, during the process of creating the verifiable proof the manufacturer also includes proof of non-revocation. This shows the customer that the VC that was issued to the manufacturer is still valid and has not been revoked by the issuer of the VC.

VI. Conclusion

In this paper we presented our TSX approach and its manifestation. We propose the use of HLI with AnonCreds VCs to tackle the challenges of verifiable PCF sharing. With the use of this technology, we can provide certified and verifiable PCF sharing across companies and countries using different standards. We have an eco-system-based approach where the manufacturers in the supply chain can compute the PCF of their products and share it with their customers, without revealing confidential information. Furthermore, the TSX approach helps in transferring the dynamic nature of the PCF throughout the supply chain.

The sharing of PCF becomes easier with our proposed TSX approach. As the regulations come in it would provide an incentive to the manufacturers to reduce the PCF of their products to receive tax benefits. They can achieve a lower PCF by, either choosing components with lower PCFs or by improving their manufacturing processes.

The use of the proposed technology gives the flexibility to choose any PCF accounting standard. Therefore, the stakeholders can define their own formats of the PCF VCs. This enables stakeholders from heterogenous industries to participate in the eco-system. Further discussions and improvements regarding the standards of PCF accounting is being done in many consortiums where Estainium association is one of them [15]. It is important to note that the TSX approach places no strict requirements on the use of a specific technology. As new requirements and technologies come forward. Other technologies can also be adopted to provide a more technology agnostic eco-system. Lastly, another benefit of presenting this approach is that it can also be adapted to share other Environmental, Social and Governance data in a verifiable manner.

TSX as an approach for measuring and sharing PCF data can help us in achieving the goal of net-zero carbon production, reduce the impact of manufacturing on the climate and help us achieve the targets laid out by the Paris agreement. We have an implementation of the TSX approach in a software application called SiGREEN that aims to help companies verify, track and share their PCF [6].

VII. Future work

As we have shown in the paper, there are different technologies available that can possibly support our presented TSX approach. We have presented a blockchain based approach which currently satisfies the presented requirement. We will continue to evolve the requirements and evaluate different technologies. When certain technologies support our defined requirements, we would incorporate them in our TSX approach as well.

References

[1] M. Finkbeiner, A. Inaba, R. Tan, K. Christiansen, and H.-J. Klüppel, "The new international standards for life cycle assessment: ISO 14040 and ISO 14044," *The international journal of life cycle assessment*, vol. 11, pp. 80–85, 2006.

[2] R. Garcia and F. Freire "Carbon footprint of particle board: a comparison between ISO/ts 14067, ghg protocol, pas 2050 and climate declaration," *Journal of cleaner production*, vol. 66, pp. 199-209, 2014.

[3] V. Subramanian, W. Ingwersen, C. Hensler, and H. Collie, "Comparing product category rules from different programs: learned outcomes towards global alignment," *The International Journal of Life Cycle Assessment*, vol. 17, pp. 892–903, 2012.

[4] Ecosystem Marketplace, "Mandatory sustain- ability reporting moves closer to reality," https://www.ecosystemmarketplace.com/articles/mandatory-sustainability-reporting-moves-closer-to-reality/, accessed: 2023-08-11.

[5] Greenhouse Gas Protocol, "Calculation tools and guidance," https://ghgprotocol.org/calculation-tools-and-guidance, accessed: 2023-08-11.

[6] Siemens-AG, "SiGREEN," https://app.sigreen.siemens.com, accessed: 2023-08-11.

[7] Y. Pan, X. Zhang, Y. Wang, J. Yan, S. Zhou, G. Li, and J. Bao, "Application of blockchain in carbon trading," *Energy Procedia*, vol. 158, pp. 4286–4291, 2019.

[8] A. M. R. da Cruz, F. Santos, P. Mendes, and E. F. Cruz, "Blockchain-based traceability of carbon footprint," in *Proceedings of the 22nd International Conference on Enterprise Information Systems (ICEIS)*, 2020, pp. 1–10.

[9] C. Ju, Z. Shen, F. Bao, P. Weng, Y. Xu, and C. Xu, "A novel credible carbon footprint traceability system for low carbon economy using blockchain technology," *International Journal of Environmental Research and Public Health*, vol. 19, no. 16, p. 10316, 2022.

[10] J. Weise, "Public key infrastructure overview," *Sun BluePrints OnLine, August*, pp. 1–27, 2001.

[11] W.T. Polk and N.E. Hastings, "Bridge Certification authorities: Connecting B2B public key infrastructures", in *PKI Forum Meeting Proceedings*, 2000, pp. 27-79.

[12] Hyperledger-Foundation, "Hyperledger Indy," https://www.hyperledger.org/use/hyperledger-indy, accessed: 2023-08-11.

[13] World-Wide-Web-Consortium, "Verifiable credentials data model v1.1," https://www.w3.org/TR/vc-data-model/, accessed: 2023-08-11.

[14] Internet Engineering Task Force, "Selective disclosure for jwts," https://datatracker.ietf.org/doc/draft-ietf-oauth-selective-disclosure-jwt/, accessed: 2023-08-11.

[15] Estainium-Association, "What we do," https://www.estainium.eco/en/what-we-do/, accessed: 2023-08-11.