A Verifiable Credential Framework for Traceable and Scalable Data Sharing: Application to Product Carbon Footprint

Nobuaki Endoh

NTT Space Environment and Energy Laboratories, NTT, Inc., Tokyo, Japan
Email: nobuaki.endou@ntt.com

***Abstract*—Verifiable Credentials (VCs) technology is gaining traction as a means of transmitting trustworthy credentials in the digital world. One is its leading use cases currently being explored is sharing Product Carbon Footprint (PCF) data among companies in a supply chain. Advancing the application of VCs is expected to reveal technical challenges and opportunities for improvement, thereby fostering further technological development. This paper proposes a new model to enable data to be securely and efficiently shared using VCs. In our model, we propose two schemes that are independent and combinable. The first scheme is to share data that includes a watermark in a verifiable form. This scheme's main advantage is that it allows shared data to be tracked and revoked. The second scheme is to make data sharing scalable in a manner in which downstream-product companies can verify that the data was created by certified upstream-product companies. To assess feasibility, we design, implement, and evaluate our proposed system for sharing PCF data. The results show that the proposed model significantly enhances security and efficiency. The proposed schemes, inspired by the challenges in sharing PCF data, are designed with general applicability, enabling them to be adapted to a wide range of scenarios.**

***Keywords*—security, verifiable credentials, sustainability**

I. Introduction

To reduce CO_2 emissions, companies in a supply chain are increasingly sharing Product Carbon Footprint (PCF) data among themselves [1, 2]. In a product supply chain, sharing PCF data, such as CO_2 emissions, makes it possible to analyze products and raw materials that significantly impact CO_2 emissions, as well as to examine production methods that result in lower emissions. This is expected to lead to reduced CO_2 emissions. For example, in the automotive industry, where there is a strong movement to share PCF data, Catena-X has become a standard PCF verification framework [3].

PCF data sharing becomes more effective when more companies participate. Because disparate methods of data sharing are inconsistent and inefficient, there is a move toward standardization. For standardization of technical aspects, standards organizations have developed a method of integrating web Application Programming Interfaces (APIs) based on OpenID Connect (OIDC) [1, 2]. Moreover, a Verifiable Credentials (VCs) based method is being considered for more trustworthy data, convenience, and compatibility with web technologies [3, 4].

The sensitive nature of PCF data, which encompasses critical details like raw materials and production methodologies, necessitates secure data sharing mechanisms. In addition, a trustworthy PCF data sharing scheme is needed to verify that the shared PCF data has been calculated appropriately since PCF data values vary depending on the calculation method and that the shared PCF data has not been spoofed or tampered with [1–3].

VCs offer a promising approach to these challenges since they are tamper-evident and trustworthy credentials that can be verified with technologies such as digital signatures. Similar to a passport in the physical world, this technology aims to transmit credentials in the digital world, making them more secure and convenient to use. VCs are also attracting attention as a fundamental technology for the shift from a centralized to a decentralized identity management model in which individuals control their own identity across any number of authorities, called Self-Sovereign Identity (SSI) [5]. VC standard specifications are being developed such as data model specifications by the W3C [6] and protocol specifications by the OpenID Foundation [7, 8]. Due to their benefits, VCs are being explored for a wide range of use cases, including verification of identity, professional qualifications, academic credentials, and vaccination certificates [9, 10]. GAIA-X is a European initiative for a federated data infrastructure that emphasizes data sovereignty and trust [11]. Within this ecosystem, VCs are employed for secure and tamper-evident data exchange, supporting use cases such as PCF data sharing, and providing the foundation for sector-specific ecosystems like Catena-X [3]. Nevertheless, the ecosystem is still in an early stage of development, and its frameworks and applications continue to evolve. Furthermore, existing VC-based data-sharing frameworks face unresolved technical challenges when applied to large-scale industrial PCF data sharing. In particular, they

Manuscript received November 18, 2025; revised December 22, 2025; accepted March 25, 2026; published June 26, 2026.

struggle to balance scalability and trust, as full per-product data certification becomes impractical at scale, and they provide limited mechanisms to trace and contain unauthorized data use after legitimate disclosure.

This paper proposes a new system model using VCs for data sharing in which, (1) the Certified Provider (CP) scheme shifts the certification target from individual data records to provider capabilities, significantly improving scalability while preserving trust guarantees, and (2) the Trace (TR) scheme introduces a novel integration of watermarking with verifiable credentials through a Matching Table, enabling post-disclosure traceability and selective revocation. By combining these mechanisms, the proposed method simultaneously addresses the critical scalability and post-disclosure accountability challenges that have not been jointly resolved in prior VC-based data-sharing systems. The contributions of this paper are as follows:

We propose a new system model of VC-based data sharing that enables data to be shared securely and operationally efficiently with general applicability. It serves as an extension which is consistent with current standards and able to address recognized challenges. We suggest a scheme using VCs for sharing data that contains watermarks. This allows traceability and flexibility of the data to be shared. Furthermore, it enables VCs of the data to be identified and revoked. We present a scheme that can verify that data is shared by legitimate certified companies. This can reduce the burden on certifier organizations and make the system practical.

To assess the proposed schemes, we implement a prototype system and evaluate its performance and estimated operation cost. Security of the proposed schemes is also analyzed.

The rest of this paper is organized as follows: In Section II, we discuss related works. In Section III, we present our system model. In Section IV, we describe the results of evaluations of our proposed model. In Section V, we conducted security analysis of our system model. Finally, we give the conclusion and future work in Section VI.

II. Literature Review

This section describes the previous studies related to data sharing systems using VCs and other related technologies.

A. Supply Chain and Product Lifecycle Management

In the context of supply chain and product lifecycle management, several studies have leveraged VCs to ensure reliability.

Shams *et al.* [12] proposed an approach called Trustworthy Supply Chain Exchange (TSX) for sharing verifiable PCF data across supply chains. To enable PCF data to be verifiably and confidentially shared, TSX combines Hyperledger Indy (HLI), which is a blockchain-based technology, and AnonCreds VCs, which are a type of VC that allows attributes to be selectively disclosed and ensures data privacy. In the TSX approach, manufacturers calculate PCF for their products, obtain a certified VC from a trusted third-party certifier, and store the VC in their digital wallet. Manufacturers share PCF data upon request from a customer (or downstream manufacturer). Manufacturers can selectively disclose specific PCF attributes while maintaining the confidentiality of sensitive information.

Garcia *et al.* [13] proposed a decentralized digital product passport scheme using SSI constructs (DIDs and VCs) to encode product information. Specifically, they model each product's Digital Product Passport (DPP) as a collection of VCs storing its attributes, and show that issuing successive VCs at each lifecycle stage (manufacturing, transfer, repair, etc.) creates a transparent, verifiable chain of custody across the supply chain.

B. Carbon and Energy Trading

VCs and distributed ledger technologies have been widely applied in the context of carbon and energy trading to ensure secure data exchange.

Mandaroux *et al.* [14] proposed digitalizing the European Union Emissions Trading System (EU ETS, a major pillar of the EU energy policy to reduce Greenhouse Gas (GHG) emissions) by using Distributed Ledger Technology (DLT), enabling the verification of authenticity and provenance, proof of ownership, and lifecycle traceability of carbon certificates and assets. Their platform allows VCs to be used to validate emission allowances, real-time tracking of trading of participants' emissions, and the audit trail reporting of the decentralized trading records. However, the challenges of DLT consensus mechanisms include scalability and high energy consumption. In addition, their framework assumes that all information is freely shared among stakeholders, but in practice, users could have various data security concerns that might necessitate additional effort to protect data privacy.

Rasool *et al.* [15] proposed a framework to facilitate creating and validating prosumer-driven verifiable green energy certificates. Their framework integrates the cost-effective DLT of IOTA Tangle with the public blockchain of Concordium that offers SSI support for prosumer-driven certificates, but it is not cost-effective for directly storing certificates. To overcome this, they propose managing certificates as VCs through local registries on the IOTA platform while securely anchoring them in Concordium. Their framework balances trust and operational efficiency to enhance feasibility for real-world deployments.

Kim *et al*. [16] addressed secure, sustainable data sharing in vehicular energy trading. Their blockchain-based Vehicle-to-Vehicle (V2V) energy trading protocol for electric vehicles uses Decentralized Identifiers (DIDs) and VCs to protect privacy. Neither Electric Vehicle (EV) owners' identities nor transaction details are publicly exposed; instead, completed trades are recorded as VCs in their scheme. Only authenticated parties can later prove the validity of these VCs without revealing sensitive data.

C. Comprehensive Surveys

To understand the broader landscape and inherent limitations of VC technologies, comprehensive surveys and systematic reviews have been conducted.

Mazzocca *et al.* [9] comprehensively surveyed DIDs and VCs in terms of implementations, application domains, and regulations. They analyzed available implementations and conducted an in-depth review of how these technologies have been employed across different use-case scenarios. They listed challenges such as standardization, seamless integration, digital wallet, application domains, security and privacy that hinder these technologies adoption in real-world scenarios and suggested future research directions.

Satybaldy *et al*. [10] presented a comprehensive systematic literature review of SSI including VCs, offered a detailed taxonomy, and identified and analyzed open challenges. They described the open challenges that emerged during their investigation in both technical and governance stacks. They mapped challenges to an architectural framework that integrates technology with human accountability across legal and social layers and classified challenges into development stages. They also classified the challenges into specific categories such as interoperability, security, privacy, and scalability.

D. Cross-domain Perspectives on Trust and Privacy

Privacy-preserving data exchange has also become a major concern in other multi-party ecosystems. For example, recent studies have proposed blockchain-enabled approaches for secure medical data sharing, such as an Electronic Health Record (EHR) privacy framework combined with federated learning governance and a blockchain–AI model for privacy-preserving medical data transmission [17, 18]. These studies highlight the growing demand for mechanisms that ensure trust, privacy, and accountability in data-sharing environments.

E. Summary of Gaps and Proposed Method

While VC technology has been actively explored in various data-sharing use cases, existing systems still face fundamental limitations when applied to large-scale industrial PCF data sharing.

First, scalability remains a major challenge. Many existing frameworks, including TSX [12] and other standardized approaches, implicitly assume full certification of product data. However, in supply chains involving a huge number of companies and products, such assumption places a prohibitive operational burden on certification bodies and is widely recognized as impractical in real-world deployments. Even initiatives such as Catena-X acknowledge this limitation and adopt tiered verification policies to balance feasibility and assurance [3]. While such policy frameworks are beginning to be discussed, corresponding technical mechanisms to realize them have not yet been sufficiently established.

Second, post-disclosure security is insufficiently addressed. While conventional VC-based systems provide strong guarantees for authenticity and integrity at the time of issuance and presentation, they offer limited mechanisms to deter or respond to unauthorized use after legitimate disclosure [6]. In particular, existing approaches lack practical means to trace leaked data back to a specific recipient and to selectively revoke only the affected credentials once misuse is detected.

To address these shortcomings, we propose two complementary novel schemes. The Certified Provider (CP) scheme shifts the certification target from individual data records to the data-producing capability of providers, thereby significantly reducing certification and operational costs while preserving trust. In parallel, the Trace (TR) scheme introduces a linkage between Data with Watermark, verifiable credentials, and receiver identifiers via a Matching Table, enabling traceability and revocation in cases of unauthorized use.

By explicitly addressing both scalability and post-disclosure traceability, our approach fills critical gaps in prior VC-based data-sharing systems and enables practical deployment in large-scale industrial settings. To the best of our knowledge, no prior VC-based PCF data-sharing framework addresses these scalability and post-disclosure accountability.

III. Materials and Methods

This section describes the system models and processes of our proposed schemes for secure and operationally efficient PCF data sharing. The VC specifications required as preliminaries are provided in Appendix A. The system model of the TSX-based scheme [12], which is used for comparison in the evaluation section, is described in Appendix B.

A. Trace Scheme (TR Scheme)

This section describes our proposed Trace (TR) scheme, which enables tracking by sharing watermarked data with VCs. Its purpose is to deter the leakage of sensitive data and reduce the risk of leakage or misuse by enabling the provided data to be tracked.

A fundamental design choice of the TR scheme is to enable the identification of entities responsible for unauthorized use, thereby serving as a deterrent against data misuse. While conventional VC standards ensure authenticity during transmission, they remain vulnerable to the risk of unauthorized secondary use once the data is disclosed. This vulnerability stems from the inability to trace leaked data back to a specific recipient, making it impossible to enforce accountability. To address this, we introduce a mechanism that embeds a digital watermark into the shared data and links it to the corresponding VC. This linkage allows the system to bridge the gap between validity at presentation and accountability after disclosure.

1) Architecture of TR scheme

Fig. 1 depicts the ecosystem of the TR scheme, which consists of the following entities in addition to those in Appendix A.

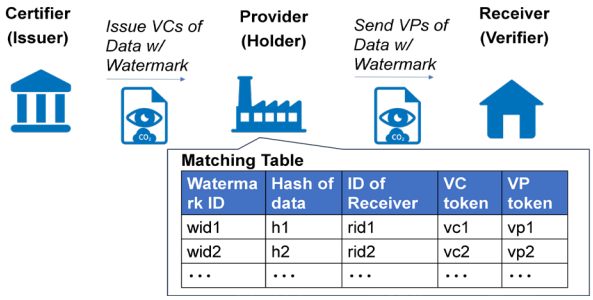

Fig. 1. Trace (TR) scheme ecosystem.

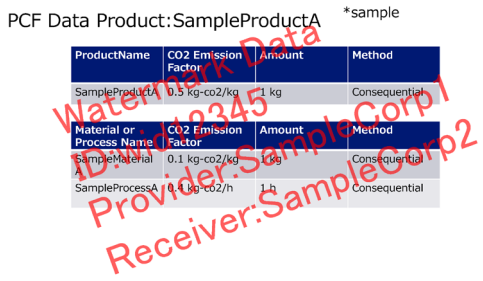

Fig. 2. Sample PCF Data with Watermark in PDF format.

1) Certifier

An entity that evaluates and certifies Data with Watermark (see Section III-A-1-d) and issues its VCs. Certifiers play the role of Issuers of the VCs of Data with Watermark in the VCs and Verifiable Presentations (VPs) specifications. In addition, the revocation process of the VCs is executed by Certifiers as Issuers of the VCs.

(e.g.) In the case of PCF data sharing, Certifiers evaluate PCF Data with Watermark of the upstream companies' products and certify that the PCF data are created appropriately. Certifiers issue VCs of the PCF Data with Watermark to the upstream companies.

2) Provider

An entity that embeds watermarks in Data with Watermark (see Section III-A-1-d), has a Certifier certify the data and issue VCs of the data, and presents the VCs as VPs to a Receiver. Providers play the role of Holders in the VCs and VPs specifications. In the VC revocation process, Providers identify potentially compromised data and request Certifiers to revoke the VCs of the data (see Section III-A-3).

(e.g.) In the case of PCF data sharing, Providers are upstream companies that have VCs of their products PCF data issued by Certifiers and present it as VPs to downstream companies.

3) Receiver

An entity that is presented, validates, and uses VCs of Data with Watermark. Receivers play the role of Verifiers in the VCs and VPs specifications.

(e.g.) In the case of PCF data sharing, Receivers are downstream companies who are presented VCs of PCF Data with Watermark of the upstream companies' products and use them for calculating and analyzing PCF data of their own products.

4) Data with watermark

Data with a digital watermark that is created by and provided from a Provider to a Receiver. The watermark contains a Watermark Identifier (Section III-A-1-e) and an identifier of the Receiver. The Provider stores these values in a Matching Table (Section III-A-1-f) to identify potentially compromised data and its Receiver.

(e.g.) In the case of PCF data sharing, Data with Watermark is PCF data with embedded watermarks of products provided by upstream companies to downstream companies. The data format can include a watermark, for example, in PDF format as shown in Fig. 2.

When the data is large or the data format cannot be handled by the VC as it is, the download URL and the hash value of the Data with Watermark SHOULD be contained as a claim of the VC for data integrity as shown in Listing 1.

```
{
  "credentialSubject": {
      "dataProvided": {
      "creationDate": 1717738276,
      "expDate": 1749274276,
      "pcfDataHash":  "{Hash  of  Data  with
Watermark}" ,
      "pcfDataURL": " https://****/****.pdf ",
      "productid": "pid0001",
      "productName": "SampleProductA",
      "providerName": "SampleCorp1",
      "watermarkid": "{WatermarkID}"
    },
    "id": "did:***:***"
},
  "issuer": {
    "id": "did:***:***"
  },
  "id": "urn:uuid:****",
  "type": ["pcfTR"],
  "credentialStatus": {
    "id": "https://****#1234",
    "type": "StatusList2021Entry",
    "statusPurpose": "revocation",
    "statusListIndex": 1234,
    "statusListCredential": "https://****"
```

```
  },

  "@context":
["https://www.w3.org/2018/credentials/v1"],

  "issuanceDate": "****",

  "proof": {

    "type": "JwtProof2020",

    "jwt": "****"

  }

}
```

Listing 1. A sample part of claims of VC of Data with Watermark in the TR scheme.

5) Watermark Identifier (ID)

A unique identifier for each data to be provided that a Provider embeds in the watermark of the Data with Watermark. In the case of identifying which Receiver is presented with which VP of Data with Watermark, the Provider SHOULD uniquely assign a Watermark ID and embed it in the Data with Watermark. The Provider stores the Watermark ID, the VC token, the VP token, the hash of Data with Watermark, and the identifier of the Receiver in the Matching Table so that they can be matched. When the Data with Watermark is compromised, it can be uniquely identified as a result of matching, and its VC can be revoked. The creation of Watermark IDs, creation of Data with Watermark, calculation of hashes, and the issuance of VCs MAY be done in batches.

6) Matching table

A data table managed by a Provider to identify potentially compromised data. The Provider stores the Watermark ID, the VC token, the VP token, the hash of Data with Watermark, and the identifier of the Receiver in the Matching Table so that they can be matched as shown in Table I. The Provider uniquely identifies potentially compromised data by checking whether the Watermark ID of the data or the hash of the data exists in the Matching Table.

TABLE I. SAMPLE MATCHING TABLE

Watermark ID	Hash of data	ID of Receiver	VC token	VP token
wid1	h1	rid1	vc1	vp1
wid2	h2	rid2	vc2	vp2
…	…	…	…	…

2) Process of TR scheme

This section describes the process of VC issuance and presentation of our proposed TR scheme. The overall process is shown in Fig. 3.

The process is described in detail below.

- (TR 1) Insert record into Matching Table:

The Provider creates the Data with Watermark. The Provider uniquely assigns the Watermark ID and embeds it in the Data with Watermark. The Provider calculates the hash of the Data with Watermark. The Provider stores the Watermark ID and the hash of the Data with Watermark in the Matching Table. The creation of Watermark Identifiers, creation of Data with Watermark, and calculation of hashes MAY be done in batches.

- (TR 2) Issue VC:

The Certifier issues the VC of Data with Watermark to the Provider. The download URL and the hash value of the Data with Watermark SHOULD be contained as claims of the VC for data integrity. VCs MAY be issued in batches.

The Provider receives the VC of Data with Watermark and determines whether the values in the claims of the VC match the values in the Matching Table. In particular, the values of the Watermark ID and the hash of the Data with Watermark are checked. The Provider stores the VC token of the Data with Watermark in the Matching Table.

- (TR 3) Send VP:

The Provider sends the VP of Data with Watermark to the Receiver. The Provider stores the VP token of the Data with Watermark and the Identifier of the Receiver in the Matching Table.

- (TR 4) Validate VP:

The Receiver validates the VP of Data with Watermark first in accordance with the VC and VP specifications. The Receiver MUST check whether the value of the hash of the Data with Watermark in the VC claim matches the hash calculated from the Data with Watermark by the Receiver itself. This enables the Receiver to validate the integrity of the Data with Watermark provided.

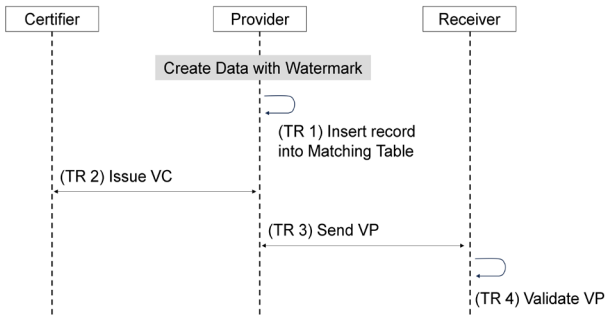

Fig. 3. Trace scheme VC issuance and presentation flow.

3) Process of identification and revocation in the TR scheme

This section describes the process of identifying potentially compromising data and revoking its VC in the TR scheme.

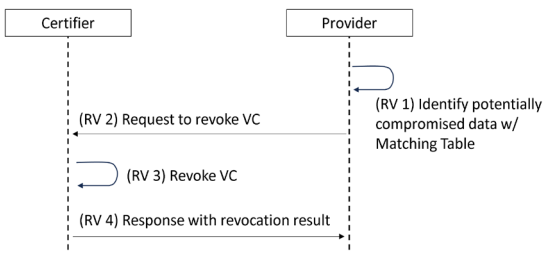

Fig. 4. TR scheme identification and revocation flow.

The proposed scheme is based on the Bitstring Status List [19], the standard specification of VC revocation. Fig. 4 depicts the process.

- (RV 1) Identify potentially compromised data:

The Provider discovers the data itself or the Watermark ID of the potentially compromised data. The Provider identifies whether the data is compromised by checking whether the Watermark ID of the data or the hash of the data exists in the Matching Table. If the data is identified to be uncompromised and its VC (VC of Data with Watermark) does not require revocation, the process is complete here.

- (RV 2) Request to revoke VC:

The Provider requests the Certifier to revoke the VC of identified compromised data (VC of Data with Watermark by Certified Provider) by sharing the uniquely identifiable information such as the Watermark ID or the hash or the VC token of the identified compromised data.

- (RV 3) Revoke VC:

The Certifier revokes the VC of the identified compromised data (VC of Data with Watermark by Certified Provider).

- (RV 4) Response with revocation result:

The Certifier responds with the result of the revocation of the VC of the identified compromised data (VC of Data with Watermark by Certified Provider).

B. Certified Provider Scheme (CP Scheme)

This section describes our proposed Certified Provider (CP) scheme, which enables data provision by Certified Providers to be verified.

For example, in the case of PCF data sharing, there are large numbers of products, so it is difficult for Certifiers to evaluate and certify the large amount of PCF data itself and issue VCs (see Section IV-C). Therefore, in this scheme, Certifiers certify that upstream companies are capable of properly evaluating and creating PCF data.

A fundamental design choice of the CP scheme is to shift the certification target from individual data records to the data-producing capability of the data provider. While per data certification offers granular assurance, it imposes prohibitive operational latencies and costs within large-scale industrial supply chains. By binding a Data VC to a Capability VC, we achieve a scalable balance between trust and efficiency. Our approach introduces a cryptographic binding mechanism that ensures the integrity and explicit association between the data and the data producing capability.

1) Architecture of CP scheme

Fig. 5 depicts the ecosystem of the CP scheme, which consists of the following entities in addition to those in Appendix A.

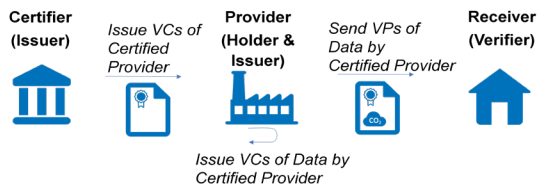

Fig. 5. Certified Provider (CP) scheme ecosystem.

1) Certifier

An entity that evaluates and certifies that Providers are qualified to create data to be provided to Receivers and issues the VCs of Certified Provider to the Providers. Certifiers play the role of Issuers of the VCs of Certified Provider in the VCs and VPs specifications.

(e.g.) In the case of PCF data sharing, the Certifiers issue the VCs of Certified Provider. This means that Certifiers evaluate and certify that the upstream companies are qualified to create the PCF data appropriately and provide it to the downstream companies.

2) Provider

An entity that is certified to create the Data to be Provided, issues the VC of Data by Certified Provider to themselves, and presents the VC of the Data by Certified Provider to the Receiver as a VP. Providers are issued VCs of Certified Provider by Certifiers. Providers play the role of Holders of the VCs of Certified Provider and Issuers of the VCs of Data by Certified Provider in the VCs and VPs specifications.

(e.g.) In the case of PCF data sharing, Providers are upstream companies who are issued VCs of Certified Provider (see Section III-B-1-e) from Certifiers, who issue VCs of Data by Certified Provider (see Section III-B-1-f) to themselves and who present the VCs of Data by Certified Provider to downstream companies.

3) Receiver

An entity that is presented, validates, and uses VCs of Data by Certified Providers. Receivers play the role of Verifiers of VPs of Data by Certified Provider in the VCs and VPs specifications.

(e.g.) In the case of PCF data sharing, Receivers are downstream companies who are presented the VCs of Data by Certified Provider (see Section III-B-1-f) from upstream companies.

4) Data to be provided

Data that is created by and provided from a Provider to a Receiver.

(e.g.) In the case of PCF data sharing, Data to be Provided is PCF data of upstream companies' products provided by upstream companies to downstream companies.

5) VC of certified provider

A VC that certifies the Provider's ability to create Data to be Provided and issue VCs of Data by Certified Provider (see Section III-B-1-f). A VC of Certified Provider is issued to the Providers from the Certifiers. A VC of Certified Provider includes a Provider ID (see Section III-B-1-h) in claims.

(e.g.) In the case of PCF data sharing, a VC of Certified Providers is the VC that certifies the ability to create PCF data and issue VCs of PCF data. The VC of Certified Provider is issued to the upstream companies from the Certifiers. Listing 2 depicts the sample claims of the VC.

```
"credentialSubject": {

    "cpData": {

       "certificateDate": 1711897200,

       "certificateExpDate": 1743433200,

       "certificateOf":      "certificates      of
calculating pcf",

       "certifierName": "SampleCertifier2",

       "providerName": "SampleCorp1",

       "providerid": "{ProviderID}"

     },

   "id": "did:***:***"

 }
```

Listing 2. A sample part of claims of VC of certified provider in the CP scheme.

6) VC of data by certified provider

A VC of Data to be Provided issued by and to a Provider itself and presented by the Provider to a Receiver. The Provider is certified to be able to create the Data to be Provided and to issue the VC of Data by Certified Provider. The Provider is issued the VC of Certified Provider from the Certifier. The VC of Data by Certified Provider includes the VC token of Certified Provider in claims. The VC of Data by Certified Provider is signed by the private key referenced by the Provider ID (see Section III-B-1-h) as shown in Listing 3. The Receiver validates the signature of the presented VC of Data by Certified Provider with the public key referenced by the Provider ID. Thereby, the Receiver confirms that the VC of Data by Certified Provider is issued by the Provider certified by the VC of Certified Provider.

```
{

  "kid": "{ProviderID}",

  "alg": "ES256K",

  "typ": "JWT"

}
```

Listing 3. A sample part of claims of JWT header of VC of data by certified provider in the CP scheme.

(e.g.) In the case of PCF data sharing, VCs of Data by Certified Provider are the VCs of PCF data issued by and to an upstream company itself and presented by the upstream company to a downstream company. Listing 4 depicts the sample claims of the VC.

```
  "credentialSubject": {

   "dataProvided": {

      "cpvc": "{VC token of Certified Provider}",

      "creationDate": 1717738276,

      "expDate": 1749274276,

      "productName": "SampleProductA",

      "productid": "pid0001",

      "providerName": "SampleCorp1",

      "pcfDataHash":   "{Hash   of   Data   to   be
Provided}",

      "pcfDataURL": " https://****/****.pdf "

    },

    "id": "did:***:***"

  }
```

Listing 4. A sample part of claims of VC of data by the certified provider in the CP scheme.

7) Certified provider binding

Ability of the Provider to prove a VC of Data is legitimately issued by Certified Provider by proving control over the private key of the issuance of VC of Data by Certified Provider. This key is also associated with the subject of the VC of Certified Provider. The Provider ID (see Section III-B-1-h) can be used as a claim to indicate the subject.

8) Provider ID

A claim that is included in claims of a VC of Certified Provider and a reference to a signing key of a VC of Data by Certified Provider as shown in Listings 2 and 3. A Receiver validates the signature of the presented VC of Data by Certified Provider with the public key referenced by the Provider ID and confirms that the VC of Data by Certified Provider is issued by the Provider certified by the VC of Certified Provider.

(e.g.) DID [20], X.509 certificates [21] can be used.

2) Process of CP scheme

This section describes the process of our proposed CP scheme. The overall process is shown in Fig. 6.

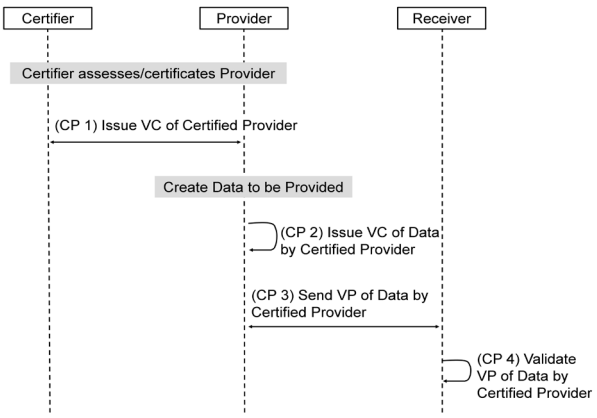

Fig. 6. CP scheme VC issuance and presentation flow.

The process is described in detail below.

- (CP 1) Issue VC of Certified Provider:

The Certifier assesses and certificates the Provider's ability to create Data to be Provided. The Certifier issues the VC of Certified Provider to the Provider. (The VC contains the Provider ID claim as shown in Listing 2.)

- (CP 2) Issue VC of Data by Certified Provider:

The Provider creates the Data to be Provided. The Provider issues the VC of Data by Certified Provider to the Provider itself. The VC of Data is signed with the private key referenced by the Provider ID. (e.g. In the case of JWT [22], the kid claim [23] corresponds to the Provider ID as shown in Listings 2 and 3.)

- (CP 3) Send VP of Data by Certified Provider:

The Provider sends the VP of Data by Certified Provider to the Receiver.

- (CP 4) Validate VP of Data by Certified Provider:

The Receiver validates the VP of Data by Certified Provider first in accordance with the VC and VP specifications. The Receiver also validates the VC of Certified Provider that is included in the VC of Data by Certified Provider. In addition, the Receiver validates the signature of the VC of Data by Certified Provider with the public key referenced by the Provider ID, which is included in the VC of Certified Provider. Thereby, the Receiver confirms that the VC of Data by Certified Provider is issued by the Provider certified by the VC of Certified Provider.

C. Hybrid Scheme (HY Scheme)

This section describes our Hybrid (HY) scheme, which combines the proposed TR and CP schemes.

1) Architecture of HY scheme

The two previously proposed schemes can be used independently but can also be combined. This helps secure and scalable data sharing by enabling the provision of data by certified Providers to be verified and data to be traced.

Fig. 7 depicts the ecosystem of the HY scheme, which consists of the following entities in addition to those in Appendix A.

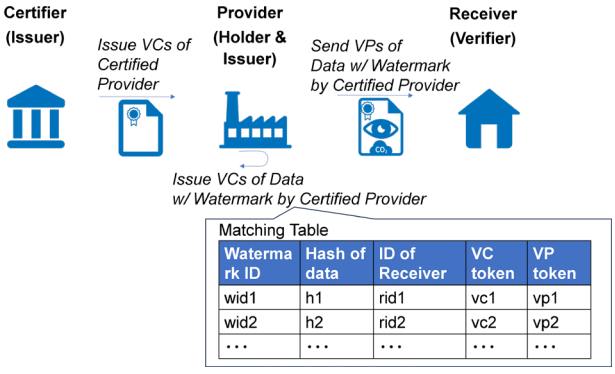

Fig. 7. Hybrid (HY) scheme ecosystem.

1) Certifier

See the description of Certifier in Section III-B-1.

The Data to be Provided in the CP scheme corresponds to the Data with Watermark in the HY scheme.

2) Provider

See the description of Provider in Section III-B-1.

The Data to be Provided in the CP scheme corresponds to the Data with Watermark in the HY scheme. In addition, the revocation process of the VCs of Data with Watermark by Certified Provider is executed by Providers as Issuers of the VCs.

3) Receiver

See the description of Receiver in Section III-B-1. The Data to be Provided in the CP scheme corresponds to the Data with Watermark in the HY scheme.

4) Data with watermark

See the description of Data with Watermark in Section III-A-1.

5) Watermark Identifier (ID)

See the description of Watermark Identifier (Watermark ID) in Section III-A-1.

6) VC of Certified Provider

See the description of VC of Certified Provider in Section III-B-1. The Data to be Provided in the CP scheme corresponds to the Data with Watermark in the HY scheme.

7) VC of data with watermark by certified provider

See the description of VC of Data by Certified Provider in Section III-B-1. The Data to be Provided in the CP scheme corresponds to the Data with Watermark in the HY scheme. The download URL and the hash value of the Data with Watermark SHOULD be contained as claims of the VC of Data with Watermark by Certified Provider for data integrity. Listing 5 depicts the sample claims of the VC.

```
{
  "credentialSubject": {
    "dataProvided": {
      "cpvc": "{VC token of Certified Provider}",
      "creationDate": 1717738276,
      "expDate": 1749274276,
      "pcfDataHash": "{Hash of Data with Watermark}",
      "pcfDataURL": " https://****/****.pdf ",
      "productid": "pid0001",
      "productName": "SampleProductA",
      "providerName": "SampleCorp1",
      "watermarkid": "{WatermarkID}",
    },
    "id": "did:***:***"
  },
```

```
  "issuer": {
    "id": "did:***:***"
  },
  "id": "urn:uuid:****",
  "type": ["pcfHY"],
  "credentialStatus": {
    "id": "https://****#1234",
    "type": "StatusList2021Entry",
    "statusPurpose": "revocation",
    "statusListIndex": 1234,
    "statusListCredential": "https://****"
  },
  "@context":
["https://www.w3.org/2018/credentials/v1"],
  "issuanceDate": "****",
  "proof": {
    "type": "JwtProof2020",
    "jwt": "****"
  }
}
```


Listing 5. A sample part of claims of VC of data with watermark by the certified provider in the HY scheme.

8) Certified provider binding

Certified Provider Binding is also included in the HY scheme. See the description of Certified Provider Binding in Section III-B-1. The VC of Data by Certified Provider in the CP scheme corresponds to the VC Data with Watermark by Certified Provider in the HY scheme.

9) Provider ID

See the description of Provider ID in Section III-B-1. The Data to be Provided in the CP scheme corresponds to the Data with Watermark in the HY scheme.

2) Process of HY scheme

This section describes the process of the HY scheme. The overall process is shown in Fig. 8.

The process is described in detail below.

- (HY 1) Issue VC of Certified Provider:

See the description of the step (CP 1) in Section III-B-2.

- (HY 2) Insert record into Matching Table:

See the description of the step (TR 1) in Section III-A-2.

- (HY 3) Issue VC of Data with Watermark by Certified Provider:

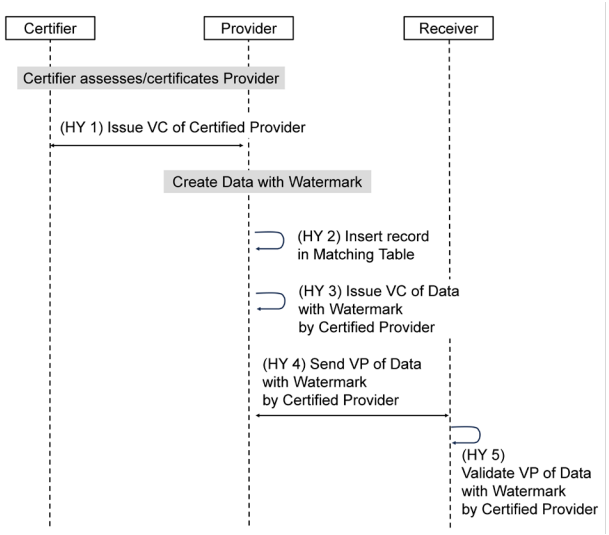

Fig. 8. HY scheme VC issuance and presentation flow.

See the description of the step (CP 2) in Section III-B-2. The Data to be Provided in the CP scheme corresponds to the Data with Watermark in the HY scheme.

The download URL and the hash value of the Data with Watermark SHOULD be contained as claims of the VC of Data with Watermark by Certified Provider for data integrity. The Provider stores the VC token in the Matching Table.

- (HY 4) Send VP of Data with Watermark by Certified Provider:

See the description of the step (TR 4) in Section III-A-2. The VP of Data with Watermark in the TR scheme corresponds to the VP of Data with Watermark by Certified Provider in the HY scheme.

- (HY 5) Validate VP of Data with Watermark by Certified Provider:

The Receiver validates the VP of Data with Watermark by Certified Provider and the VC of Certified Provider first in accordance with the VC and VP specifications. The Receiver MUST validate whether the value of the hash of the Data with Watermark in the VC claim matches the hash calculated from the Data with Watermark by the Receiver itself. This enables the Receiver to validate the integrity of the Data with Watermark provided. The Receiver also validates the VC of Certified Provider that is included in the VC of Data with Watermark by Certified Provider. In addition, the Receiver validates the signature of the VC of Data with Watermark by Certified Provider with the public key referenced by the Provider ID included in the VC of Certified Provider. Thereby, the Receiver confirms that the VC of Data with Watermark by Certified Provider is issued by the Provider certified by the VC of Certified Provider.

3) Process of identification and revocation in the HY scheme

The VC of Data with Watermark in the TR scheme corresponds to the VC of Data with Watermark by Certified Provider in the HY scheme. See the description

in Section III-A-3. In the process of the identification and revocation in the HY scheme, the Provider plays both roles of the Issuer and Holder of the VC of Data with Watermark by Certified Provider in the TR scheme.

IV. Results and Discussion

In this section, we first describe the implementation of the proposed schemes to assess their feasibility. Next, we describe the results of the performance evaluation to determine whether the proposed system can be implemented in a practical processing time. We also describe the results of operational time evaluation to assess whether the proposed schemes can share PCF data for a huge number of products, which is important for sharing PCF data in actual operation. Finally, security of the proposed schemes is also analyzed.

A. Implementation

To assess the feasibility of the proposed schemes, we implemented a prototype system using them.

Our model can be implemented and run on VC platforms currently provided by existing Identity-as-a-Service (IDaaS) services. As a VC implementation platform, we used Auth0 lab [24], an IDaaS that provides standard functions of VC Issuer, Wallet, and Verifier. Issuer is implemented as a web service, while Wallet and Verfier are implemented as Single-Page Applications (SPAs). The system processes of the proposed schemes were implemented as follows. Wallet was implemented in javascript on a computer with Windows 10 Enterprise 22H2 with 8 GB RAM and Intel(R) Core (TM) i5-7Y57 CPU @ 1.20GHz. Verifier was implemented in nodejs on a computer with WSL2 Linux server running with Ubuntu 22.04.4 LTS with 8 GB RAM and Intel(R) Core (TM) i5-7Y57 CPU @ 1.20 GHz. We used jose [25] for signature verification and pdf-watermark [26] for watermark creation. As an IDaaS implementation platform that can realize the proposed schemes, any IDaaS that provides standard VC functions is acceptable, and although not mentioned in this paper, Microsoft Entra ID [27] was also found to realize the proposed schemes.

B. Performance Evaluation

To determine whether the process of the system based on the proposed schemes is feasible in practical time, we analyze the process time of PCF data sharing for the implemented system.

In addition, it is crucial to evaluate the practicality of sharing PCF data, including the operation time of PCF data for a huge number of products. The evaluation of operation time is described in the next section.

For the performance evaluation, we measured the processes of the HY scheme as a representative of the proposed schemes, since TR and CP share common processing components.

For comparison, we also measured the processes of the TSX-based scheme [12], which follows a conventional VC/VP-based PCF data-sharing approach. The detailed description of the TSX-based scheme is described in Appendix B. We performed 10 measurements and calculated their means and corrected sample standard deviations. These measurements were obtained in a controlled experimental environment with limited network bandwidth and a small number of simulated participants. While absolute processing times may vary in real-world deployments with more participants or different network conditions, the relative performance trends between the schemes are expected to remain consistent.

Table II shows the process time of our proposed HY scheme and of the TSX-based scheme for comparison. Compared to the TSX-based scheme, the proposed HY scheme increases the total process time of the system due to the additional process of issuing the VC of the certified provider. Looking at VC issuance, a large portion of the process time is spent in (HY 1) and (HY 3), where JWT transmission processing takes place. The proposed scheme issues a VC of the certified provider and a VC of data by the certified provider, which increases the processing time. However, the increase is not synergistic, but additive, indicating that it can be performed in practical time. Looking at VP sending, a large portion of the process time is spent in (HY 4), where JWT transmission processing takes place. In both the proposed HY and TSX-based schemes, a VP is sent only once, and they do not significantly differ in terms of processing time. In conclusion, the process time of the proposed scheme is as expected from the processes, and the process completes in practical time.

While the measurements confirm practical feasibility under the evaluated conditions, the prototype-based evaluation focuses on relative processing costs rather than absolute throughput. The comparison with the TSX-based scheme highlights structural design differences. In large-scale deployments, operations such as issuance, verification, and revocation checking are expected to scale linearly with the number of credentials. Although absolute performance may vary in distributed or optimized implementations, the observed relative differences reflect architectural characteristics rather than prototype-specific artifacts. Overall, the proposed schemes demonstrate practical performance with scalability primarily determined by their design.

TABLE II. Process Time

Scheme	Process	Time (ms)
HY scheme	Total processes	8468.4 ± 156.2
	(Breakdown)	-
	(HY 1)	2932.9 ± 124.5
	(HY 2)	134.2 ± 3.2
	(HY 3)	2943.8 ± 162.3
	(HY 4)	2361.7 ± 157.7
	(HY 5)	93.2 ± 8.2
TSX-based scheme [12]	Total processes	4903.0 ± 268.3
	(Breakdown)	-
	Issue VC OID4VCI (VC2)–(VC 6)	2627.0 ± 189.6
	Send VP OID4VP (VP1)–(VP 3)	2276.0 ± 352.4

Regarding the matching table, the number of unique watermarks and corresponding entries increases in

proportion to the number of issued credentials and data-sharing events. Since the associated metadata are of limited size, the resulting storage growth is expected to be linear. Lookup operations for watermark identification can be efficiently supported using standard indexed data structures, achieving constant- or logarithmic-time retrieval in practical deployments. Therefore, conventional database technologies and key-value stores are expected to sufficiently manage watermark-related metadata at scale.

C. Operation Cost Analysis

In this section, we analyze and evaluate the operational cost required to operate PCF data sharing for each scheme.

The more companies that share PCF data, the more effective the analysis and policies will be. In the future, it is desirable that many companies, ideally all companies, participate. To achieve this, optimal data sharing schemes need to be considered in terms of the operation cost. In terms of the operation cost, certifiers who are at the top of the supply chain are expected to be the bottleneck due to the huge number of products and companies participating in the project. We estimated and compared the operation time cost of each scheme for the operation of certification and creation of PCF data and operation of certification of the PCF data creation ability.

In the TSX-based and proposed TR schemes, certifiers certify PCF data. In the proposed CP and HY schemes, certifiers certify upstream-product companies' PCF data creation ability. We estimate the time cost required for each actor, i.e., certifiers and upstream-product companies, to certify PCF data, create PCF data, and certify the PCF data creation ability under each scheme.

Assuming that the number of product companies is N and that every company has M products, T_d, T_{cd}, and T_{cc} are the time costs required to create PCF data, certify PCF data, and certify the PCF data creation ability, respectively. For these variables, the values in Table III were used in the evaluation.

TABLE III. VARIABLES AND VALUES FOR OPERATION TIME COST EVALUATION

Variables	Description	Values
T_d	Time cost required to create PCF data	75–180 person-days
T_{cd}	Time cost required to certify PCF data	10–30 person-days
T_{cc}	Time cost required to certify the PCF data creation ability	10–30 person-days
N	Number of product companies	3,384
M	Number of products	32

For estimating specific values for each variable for PCF data certification, PCF data creation, and PCF data creation ability, we use estimates of the number of working days for External Life Cycle Assessment (LCA) [28]. LCA is a standard method for evaluating environmental impacts, such as GHG emissions, and is used to calculate PCF data. For the time required for certifying PCF data by certifiers and certifying the PCF data creation ability, the value of the peer review time in External LCA is used. For the time cost required for PCF data creation for an upstream-product company, the value of the total estimate time cost for External LCA is used. We note that these LCA related values may vary across industry sectors and product categories.

For calculations with specific values for the number of companies and products, we use the figures from EU ecolabel 2025 [29]. EU ecolabel is a voluntary environmental label for products, recognized throughout Europe and awarded to those that meet specific criteria related to reducing environmental impact. This means that the evaluation is based on a sense of scale in terms of the number of companies and products in environmentally-conscious companies. PCF data sharing could initially be a system in which environmentally-conscious companies would benefit from participating, and this evaluation would be useful in analyzing the operation cost of such a system. In addition, although the number of companies and products would be enormous if PCF data sharing were mandated, we do not conduct such a study because the EU ecolabel figures are sufficient to demonstrate the effectiveness of the proposed schemes. Table IV shows the equations for the operational time cost of certifying PCF data, creating PCF data, and certifying the PCF data creation ability for each actor in each scheme, and the results of substituting specific values from Table III. Of the operations, the most time-costly bottleneck was the certification operations for certifiers. For the TSX-based and TR schemes, the total operation time cost is 1,082,880–3,248,640 person-days for certifiers and is 2,400–5,760 person-days for each upstream-product company.

TABLE IV. THE OPERATION TIME COST EVALUATION

Scheme	Item	Certifier	Upstream Company
TSX-based scheme [12], TR scheme	Operation	Certification of PCF data	Creation of PCF data
	Equation of operation time cost	$N \times M \times T_{cd}$	$M \times T_d$
	Numerical result	1,082,880–3,248,640 (person-days)	2,400–5,760 (person-days)
CP scheme, HY scheme	Operation	Certification of the PCF data creation ability	Creation of PCF data
	Equation of operation time cost	$N \times T_{cc}$	$M \times T_d$
	Numerical result	33,840–101,520(person-days)	2,400–5,760 (person-days)

For the CP and HY schemes, the total operation time cost is 33,840–101,520 person-days for certifiers and 2,400–5,760 person-days for each upstream-product company. In other words, assuming PCF data sharing with the number of companies and products involved in EU ecolabel, the CP and HY schemes are 32 times more efficient than the TSX-based and TR schemes for certifiers. Expressing it with variables, those are M times more efficient. If PCF data sharing becomes mandatory, this efficiency will become even more important, as the number of companies and products will be enormous.

V. Security Analysis

This section describes the security threats and countermeasures of our proposed model.

A. Threat Model

1) Threat actors

We consider the following potential adversaries:

Providers, who may attempt to issue falsified PCF data, exceed their certified capabilities or cause verifiable credentials to become invalid or improperly managed.

Receivers, who may misuse legitimately obtained PCF data, deny unauthorized use, or cause verifiable credentials to become invalid or improperly managed.

Certifiers, who may cause verifiable credentials to become invalid or improperly managed.

External Attackers, who could access public endpoints and attempt attacks such as spoofing, tampering, or service disruption.

2) Security goals

The primary security goal is to ensure the Confidentiality, Integrity, and Availability (CIA) of the data, system components, and data flows involved in PCF data sharing.

3) Scope of analysis

The scope of this security analysis encompasses the three VC-based PCF data sharing architectures introduced in this paper (TR, CP, and HY schemes), as illustrated in Figs. 1, 6, and 8.

The protected assets include the PCF data itself, associated verifiable credentials (VC of Data and VC of Certified Provider), verification processes, and the overall trustworthiness of the data sharing system.

The scope of the threat analysis covers the core data flows defined in the system model, including:

(i) issuance of VCs,

(ii) presentation of VPs, and

(iii) identification and revocation of issued VCs.

Attacks outside these flows (e.g., physical compromise of infrastructure) are considered out of scope.

B. Security Resistance

To systematically identify and analyze security threats, we adopt the STRIDE threat modeling framework [30] and conduct a comprehensive threat analysis. This paper focuses on scheme-specific threats that are particularly relevant to PCF data sharing. The summary of the results is shown in Table V.

TABLE V. The Security Analysis Results

Stride Category	Potential Threat in PCF Data Sharing	Countermeasures
Spoofing	Impersonation of a legitimate provider	Implementation compliant with VC standards specifications, CP and HY scheme
Tampering	Tampering with VCs, VPs or PCF data across the supply chain.	-Implementation compliant with VC standards specifications, TR, CP and HY Scheme -Audit and accountability
	Tampering with embedded watermarks	-Implementation compliant with VC standards specifications, TR and HY Scheme -Strong and Robust Watermarking Techniques
Repudiation	Denial of unauthorized use	-Implementation compliant with VC standards specifications, TR and HY Scheme -Audit and accountability
	Denial of validity of VCs or VPs	-Implementation compliant with VC standards specifications, TR, CP and HY Scheme -Audit and accountability -Credential Lifecycle Management
Information Disclosure	Unintended disclosure of VCs or VPs or PCF data	-Implementation compliant with VC standards specifications, TR and HY Scheme
	Unintended disclosure of supply chain relationships through data linkability	-Implementation compliant with VC standards specifications, TR and HY Scheme -Identifier Management
Denial of Service	Denial-of-Service (DoS) attacks against system endpoints	-Implementation compliant with VC standards specifications, CP and HY Scheme -DoS/ Distributed Denial-of-Service (DDoS) Protection
Elevation of Privilege	Issuing VCs of Data exceeding certified capabilities	-Implementation compliant with VC standards specifications, CP and HY Scheme -VC of Certified Provider Lifecycle Management

1) Impersonation of a legitimate provider

External Attackers, malicious receivers or providers may impersonate a legitimate (different) provider during VC issuance, VP presentation, or VC revocation processes. As a scenario example, an attacker may attempt to perform a replay attack by reusing a VP token obtained from a certified provider during a previous VP presentation.

All the proposed schemes are built on the established VC standard specifications [6–8], and implementations are required to conform to these specifications. For example, robust authentication and authorization controls prevent impersonation attacks. The use of nonces further prevents replay attacks by requiring verifiers to confirm that the nonce included in each VP matches the nonce originally issued for the corresponding authorization request. In addition, by verifying the Certified Provider Binding, a receiver can cryptographically confirm that the VC of Data presented by a provider was issued by a legitimate provider whose data creation capability has been certified and for which a corresponding VC Certified Provider has been issued.

2) Tampering with VCs, VPs or PCF data across the supply chain

There is a threat that an external attacker or malicious provider may tamper with VCs, VPs, or PCF values to alter them in a way that favors their own interests. As a representative scenario, a malicious provider may deliberately manipulate PCF values to report figures lower than the actual emissions to remain within the prescribed carbon emission limits.

All proposed schemes, which are built on established VC standard specifications [6–8], employ digital signatures and holder binding to ensure that each presented VC is issued to its legitimate holder and has not been altered. Verifiers can therefore validate the authenticity and integrity of the credentials. In the TR and HY schemes, receivers must verify whether the value of the hash of the Data with Watermark in the VC claim matches the hash calculated from the Data with Watermark by the Receiver itself. If not, the binding between the verifiable credential and the actual shared data cannot be guaranteed. In such a case, the receiver loses the ability to detect tampering or substitution of the shared data or referenced URL by a malicious provider or a third party. As a result, the integrity of the shared data is no longer assured, and the receiver may incorrectly accept modified or unrelated content as being covered by a valid verifiable credential. In addition, the CP and HY schemes incorporate a Certified Provider Binding mechanism, which enables receivers to verify that Data VCs are issued by legitimate providers that have themselves been issued a Certified Provider VC. This mechanism ensures the authenticity of the issuing provider, even though the data itself is not directly certified by the certifier in the CP and HY schemes. Because certification is applied to provider capabilities rather than individual data items, additional measures are required to ensure auditability and accountability. In the CP and HY schemes, misbehavior is primarily detected ex post through periodic audits, event-driven spot checks, or disputes raised by downstream stakeholders. The deterrent effect against such threats can be strengthened by randomly sampling audit targets, prioritizing audits for PCF data with high reported emissions, and imposing stricter penalties when misconduct is identified through audits. Once misbehavior is detected, its impact can be effectively contained by invalidating the Certified Provider VC. This enables receivers and verifiers to recognize that Data VCs issued by the affected provider are no longer trustworthy, thereby preventing further reliance on compromised or fraudulent data.

3) Tampering with embedded watermarks

Malicious receivers or external attackers may attempt to tamper with watermarks embedded in shared data by providers to compromise traceability, for example through watermark removal, collusion attacks, or data reformatting.

As a fundamental assumption, providers are required to implement the TR or HY schemes as specified so that traceability is properly enforced. Furthermore, to increase robustness against watermark tampering, techniques such as redundant embedding, spread-spectrum watermarking, nonlinear or adaptive embedding, and collusion-resistant codes can be applied. In practice, watermark robustness is not absolute and depends on the embedding algorithm, parameter settings, and the type and intensity of data transformations applied after distribution. While robust techniques can tolerate moderate modifications, aggressive processing, severe reformatting, or large-scale collusion among malicious receivers may degrade detection performance. Therefore, the watermark-based traceability depends on implementation quality and operational conditions, rather than as a mechanism that guarantees perfect detection under all adversarial scenarios. Accordingly, for industrial sectors with stringent robustness requirements, governance frameworks should mandate the adoption of advanced watermarking techniques and well-defined implementation and evaluation standards to ensure reliable traceability.

4) Denial of unauthorized use

A malicious receiver may attempt to deny unauthorized use of VCs. For example, PCF data that has been illicitly leaked by a malicious receiver may be discovered on an underground marketplace, however, the receiver may deny being the source of the leakage.

Providers must implement the TR or HY schemes in accordance with their specifications to ensure effective traceability, with particular attention to faithfully implementing the Matching Table mechanism. In the event of a security incident, repudiation should be prevented by demonstrating through audits that the system and its functions have been properly operated as intended. To this end, it is necessary to preserve the Matching Table, as well as relevant VCs, VPs, and their associated operational logs, to support accountability and forensic verification. Particularly, the Matching Table plays a critical role in linking Data with Watermark to the corresponding verifiable credentials and associated identifiers (e.g., Watermark IDs). In real deployments, it is assumed to be managed by a trusted operational entity and protected using standard security and operational controls. Access to the Matching Table is restricted to authorized system components through strict access control mechanisms, and the table is stored in a secure environment with encryption at rest. All accesses and updates are recorded in audit logs to support accountability and post hoc inspection in the event of misuse or security incidents. Furthermore, continuous monitoring and periodic audits can be applied to detect unauthorized access or anomalous behavior. While specific implementations may vary depending on organizational policies and deployment environments, these measures enable secure management of the Matching Table in practical operational settings.

5) Denial of validity of VCs or VPs

The validity of VCs or VPs may be repudiated. As a representative scenario, although tampering with PCF data by a malicious provider is later discovered, a legitimate receiver may be unable to prove the impact because the corresponding VP (or VC) has not been retained, allowing the malicious provider to deny responsibility.

To ensure the validity of VCs and VPs, implementations must strictly follow the VC standard specifications [6–8] as well as the TR, CP or HY schemes. When a security incident occurs, repudiation should be prevented by demonstrating through audits that the system has been operated correctly and in accordance

with the prescribed procedures. To enable such audits, it is necessary to retain the matching tables, preserved VCs and VPs, as well as relevant operational logs.

PCF data is often subject to regulatory or industry-driven retention requirements. For example, according to the WBCSD data exchange protocol [1], PCF data may be considered valid for up to three years after the reference period ends when no explicit validity period is specified. We refer to this three-year duration solely as a reference value reflecting existing industry practice, rather than as a fixed requirement. In this context, retaining PCF data together with related verifiable credentials and operational logs for an appropriately long period supports non-repudiation, ex-post audits, and dispute resolution.

Key management for long-term operations follows established practices within the VCs and DID ecosystems [6, 20]. Each provider and certifier manage their own cryptographic keys and publishes the corresponding public keys through DID documents or equivalent verifiable data registries. To maintain security during long-term operations, a DID controller updates verification methods (such as public keys) as necessary. If a key is compromised or its operational role ends, it must be invalidated. The controller achieves this by either removing the relevant verification method from the DID document or performing deactivation according to the procedures defined by the specific DID method. During verification, a verifier obtains information regarding the public keys by resolving the provider's DID, which allows them to stay informed of key updates and revocations. To confirm whether a key was valid at the specific point in time a signature was made, the verifier utilizes values included in the DID document metadata, such as versionId, versionTime, updated, and nextUpdate. These mechanisms enable continuous and scalable key lifecycle management.

Bitstring Status Lists must be properly managed. Verifiers obtain revocation status by resolving the credentialStatus reference at verification time or by refreshing cached Bitstring Status Lists when their ttl expires, in accordance with the VC Status List specification. In addition, point-in-time status verification can be performed when required, such as during audits or retrospective checks. If revocation information becomes stale, revoked or corrected PCF credentials may be temporarily treated as valid, potentially propagating outdated PCF values downstream and affecting overall system reliability. However, strict real-time revocation checks are not always practical in large-scale industrial deployments. Therefore, acceptable refresh intervals should be determined based on domain-specific operational cycles, such as product updates, regulatory requirements, or periodic reporting, balancing timeliness and scalability.

6) Unintended disclosure of VCs or VPs or PCF data

Although proposed technologies such as Selective Disclosure JSON Web Token (SD-JWT) [31] can control the scope of data disclosure, there are cases where confidential data must still be shared. In such situations, a malicious Receivers could exploit data shared in VPs without the Provider's consent—for example, by selling it to a competitor. This scenario is known as an unauthorized use attack [6].

Our TR and HY scheme helps mitigate this risk. When data suspected of unauthorized use is detected, its watermark identifier or hash value can be used to identify the data. Additionally, by optionally storing each data item's watermark identifier in one-to-one correspondence with the associated VP and receiver identifiers, we can determine which VP's data was exploited and to which receiver it was sent. These measures can deter unauthorized use. Furthermore, the VC associated with the compromised data can be revoked, further mitigating the risk. Providers must implement the TR or HY schemes in accordance with their specifications to ensure effective traceability, with particular attention to faithfully implementing the Matching Table mechanism.

7) Unintended disclosure of supply chain relationships through data linkability

Malicious receivers or external attackers may perform identifier linkage (entity resolution) to infer information that was not intended to be disclosed. As a scenario example, external attackers may obtain multiple Data VCs (e.g., through unauthorized use) and perform linkage based on shared watermark identifiers or receiver identifiers, potentially revealing transaction relationships that were not originally known to the attackers.

Including receiver identifiers improves traceability of data disclosure, but it may raise concerns about the potential exposure of business relationships. In practice, a receiver identifier alone does not directly reveal the identity of downstream companies or contractual relationships. However, when multiple Data with Watermark are disclosed, there exists a potential risk of linkage or inference, particularly for rare products or limited distribution scenarios. Depending on operational priorities, different design choices are possible. In ecosystems where business relationships are already public or where deterrence against unauthorized use is emphasized, receiver identifiers or even receiver names may be intentionally exposed. Conversely, when protecting sensitive business relationships is required, common mitigation techniques against identifier linkability can be applied, such as issuing distinct receiver identifiers on a per-product or per-service basis and updates those identifiers while maintaining internal mappings. These approaches allow systems to balance traceability and confidentiality according to application requirements.

8) Denial of Service (DoS) and Distributed Denial-of-Service (DDoS) attacks against system endpoints

External attackers may launch DoS and DDoS attacks against the system's publicly exposed endpoints.

Typical countermeasures against Denial of Service (DoS) and Distributed Denial-of-Service (DDoS) attacks include network filtering, rate limiting, traffic filtering, and the use of firewalls or managed DDoS mitigation services. In addition, scalability measures such as load

balancing and horizontal scaling help maintain service availability under high traffic conditions. Furthermore, in the CP and HY schemes, endpoints involved in issuing VCs of Data do not need to be publicly exposed, which reduces the overall attack surface.

9) Issuing VCs of data exceeding certified capabilities

A provider may intentionally or unintentionally issue VCs of Data beyond its certified data creation capabilities. For example, a provider may fail to update its VC of Certified Provider after a significant revision of the PCF calculation standard. As a result, the provider continues to issue VCs of Data using an outdated methodology. Such behavior undermines the reliability of PCF data across the supply chain.

To mitigate this threat, receivers validate the Certified Provider Binding to ensure that each Data VC is cryptographically linked to a valid Certified Provider VC and that the data issuance falls within the provider's certified capabilities. During verification, the contents of the Certified Provider VC—such as the certified scope, validity period, and applicable standards—are carefully checked. In addition to technical verification, operational policies must be established within each industrial supply chain to govern the lifecycle management of VCs of Certified Provider. Clear communication of updates to certification criteria and renewal procedures helps ensure that providers maintain up-to-date capabilities and prevent the continued issuance of VCs of Data based on outdated or unauthorized methodologies.

VI. Conclusion

In this work, we presented the design, implementation, and evaluation of a novel system for sharing data on the basis of Verifiable Credentials (VCs). The system incorporates two key schemes to ensure secure and feasible data sharing among entities. The first scheme employs digital watermarking to identify and revoke shared data, deterring leakage of sensitive information and mitigating the impact of any misuse. The second scheme verifies that data are created by providers certified by a trusted authority, enabling wide participation and trust in data sharing. We implemented the proposed system in the context of Product Carbon Footprint (PCF) data sharing and evaluated its performance, cost, and security. Quantitatively, the CP and HY schemes achieved up to a 32-fold improvement in operational efficiency for certifiers compared with conventional full-data certification models by shifting the focus from per-dataset verification to provider capability, based on the figures from EU ecolabel 2025. Performance measurements confirmed that the system operates within a practical timeframe, with a total processing time of approximately 8.5 seconds. Furthermore, security analysis demonstrated that the TR scheme enables effective deterrence of unauthorized data use by supporting traceability and revocation of compromised data. These results indicate that the proposed model successfully addresses the combined challenges of scalability, operational feasibility, and security in large-scale industrial data exchange.

While the proposed schemes are expected to play particularly important roles in the emerging industrial use case of PCF data sharing, they can further contribute to verifiable data sharing in a wider spectrum of applications. For example, the TR scheme can be applied to the sharing of sensitive industrial and personal data where traceability of data disclosure is required to deter misuse. In addition, the CP and HY schemes are well suited to digital product passport ecosystems, where certifying data-producing manufacturers or suppliers, rather than individual product records, enables scalable credential issuance. These examples illustrate the broader applicability of the proposed schemes beyond PCF data sharing. In future work, we will explore additional potential use cases for these schemes beyond PCF data sharing.

Appendix A. OpenID for Verifiable Credential Issuance (OID4VCI) and OpenID for Verifiable Presentations (OID4VP) Specifications

A. Architecture of OID4VCI and OID4VP Specifications

We describe the entities of OpenID for Verifiable Credential (OID4VCI) [7] and OpenID for Verifiable Presentations (OID4VP) [8] specifications, which are the basis for our proposed method.

VCs are technologies which aim to transmit credentials in the digital world more securely and conveniently. Fig. A1 depicts the VCs ecosystem [6]. VCs systems consist of the following entities.

Fig. A1. Verifiable Credentials ecosystem [6].

1) *Issuer:* An entity that issues VCs.
2) *Holder:* An entity that receives VCs and has control over them to present them to the Verifiers as VPs.
3) *Verifier:* An entity that requests, receives, and validates VPs.
4) *Wallet:* An entity used by the Holder to request, receive, store, present, and manage VCs and key material.
5) *Credential:* A set of one or more claims about a subject made by a Credential Issuer.
6) *VC:* An Issuer-signed Credential whose integrity can be cryptographically verified.
7) *Presentation:* Data that is presented to a specific verifier, derived from one or more VCs that can be from the same or different Credential Issuers.
8) *VP:* Data that is presented to a specific Verifier, derived from a Credential, with a cryptographic proof of Holder Binding.
9) *Holder Binding:* Ability of the Holder to prove legitimate possession of a Verifiable Credential.

10) *Cryptographic Holder Binding:* Ability of the Holder to prove legitimate possession of a VC by proving control over the same private key during the issuance and presentation. Mechanism might depend on the Credential Format. For example, in jwt_vc_json Credential Format, a VC with Cryptographic Holder Binding contains a public key or a reference to a public key that corresponds to the private key controlled by the Holder.

B. *Process of OID4VCI and OID4VP Specifications*

We describe the process of OID4VCI [7] and OID4VP [8].

The process of OID4VCI Authorization code flow wallet-initiated variation is as follows. The process is shown in Fig. A2.

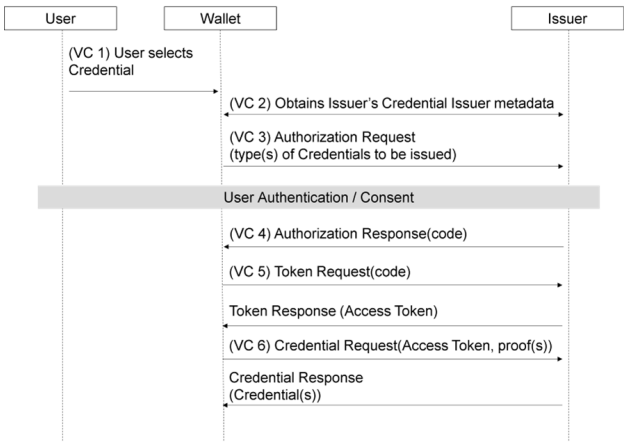

Fig. A2. OID4VCI authorization code flow wallet-initiated variation [7].

- (VC 1) The End-User requests a Credential via the Wallet from the Credential Issuer.
- (VC 2) The Wallet obtains Credential-Issuer Metadata from the Issuer.
- (VC 3) The Wallet sends an Authorization Request to the Authorization Endpoint. The Authorization Endpoint processes the Authorization Request, which typically includes authenticating the End-User and gathering End-User consent.
- (VC 4) The Authorization Endpoint returns the Authorization Response with the Authorization Code upon successfully processing the Authorization Request.
- (VC 5) The Wallet sends a Token Request to the Token Endpoint with the Authorization Code obtained in Step (VC 4). The Token Endpoint returns an Access Token in the Token Response upon successfully validating the Authorization Code.
- (VC 6) The Wallet sends a Credential Request to the Credential Issuer's Credential Endpoint with the Access Token and (optionally) the proof of possession of the private key of a key pair to which the Credential Issuer should bind the issued Credential to. Upon successfully validating Access Token and proof, the Credential Issuer returns a Credential in the Credential Response.

Fig. A3 is a sequence diagram of the Cross Device Flow of Verifiable Presentations. The process of this is as follows.

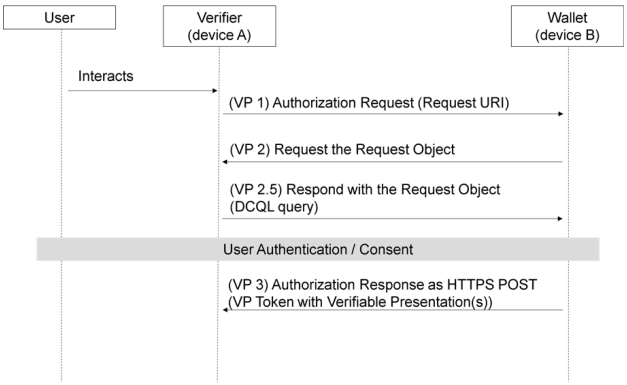

Fig. A3. OID4VP Cross device flow [8].

- (VP 1) The Verifier sends to the Wallet an Authorization Request that contains a Request URI from where to obtain the Request Object containing Authorization Request parameters.
- (VP 2) The Wallet sends a request to the Request URI to retrieve the Request Object.
- (VP 2.5) The response returns the Request Object containing Authorization Request parameters. It contains a Digital Credentials Query Language (DCQL) query that describes the requirements of the Credential(s) that the Verifier is requesting to be presented. The Wallet processes the Request Object and determines what Credentials are available matching the Verifier's request. The Wallet also authenticates the End-User and gathers their consent to present the requested Credentials.
- (VP 3) The Wallet prepares the VPs of the VCs that the End-User has consented to. It then sends to the Verifier an Authorization Response where the VPs are contained.

APPENDIX B. TSX-BASED SCHEME

A. *Architecture and Process of TSX-Based Scheme*

We describe a VC-based PCF data-sharing scheme that strictly follows the VC and VP specifications and is consistent with the TSX approach proposed by Shams *et al.* [12]. In this paper, we refer to this scheme as the TSX-based scheme. The scheme is intentionally defined without additional optimization or delegation mechanisms to serve as a standard-compliant baseline for performance evaluation. Fig. A4 shows the ecosystem of the TSX-based scheme. The TSX-based scheme systems consist of the following entities in addition to those in Appendix A.

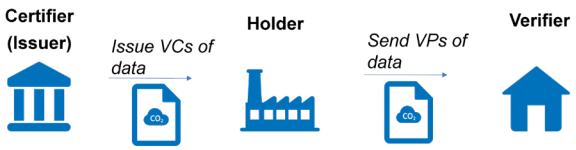

Fig. A4. TSX-based scheme ecosystem [12].

1) Certifier

An entity that evaluates and certifies data and issues its VCs. Certifiers play the role of Issuers in the VC and VP specifications.

(e.g.) In the case of PCF data sharing, Certifiers evaluate PCF data of the upstream companies' products and certify that PCF data are created in appropriate manners. Certifiers issue VCs of PCF data to the upstream companies.

2) Holder

This entity is a Holder in the VC and VP specifications.

(e.g.) In the case of PCF data sharing, Holders are upstream companies that have VCs of its products PCF data issued by Certifiers and present those as VPs to downstream companies.

3) Verifier

This entity is a Verifier in the VC and VP specifications.

(e.g.) In the case of PCF data sharing, Verifiers are downstream companies that receive VPs of PCF data from upstream companies and use those to calculate their own PCF data.

The process of the scheme basically follows the standard VC and VP specifications. Certifiers issue VCs of PCF data to upstream companies. The upstream companies are issued VCs as Holders and present the VCs to downstream companies as VPs.

CONFLICT OF INTEREST

The author declares no conflict of interest.

ACKNOWLEDGMENT

The support of colleagues, Ken Okamoto, Takashi Ikeda, Yuji Maeda is acknowledged.

REFERENCES

[1] WBCSD. (2025). Technical Specifications for PCF Data Exchange (Version 3.0.3). [Online]. Available: https://wbcsd.github.io/tr/data-exchange-protocol/latest/

[2] Green x Digital Consortium. (2024). Technical Specifications for Data Exchange Version 2.0. [Online]. Available: https://www.gxdc.jp/pdf/technical_spec_2.0en.pdf

[3] Catena-X. (2024). Catena-X and TFS PCF Verification Framework. [Online]. Available: https://catenax-ev.github.io/assets/files/CX-NFR-PCF_TFS-verification_v.1.0-9c745192bc2871adda513e4b7a22bab2.pdf

[4] WBCSD. Defining a practical and robust PCF validation approach. [Online]. Available: https://wbcsd.github.io/tr/websitedocs/PACT_whitepaper_validation.pdf

[5] C. Allen. (2016). The Path to Self-Sovereign Identity. [Online]. Available: https://www.lifewithalacrity.com/article/the-path-to-self-sovereign-identity/

[6] M. Sporny, D. Longley, D. Chadwick, and I. Herman. (2025). Verifiable Credentials Data Model v2.0. [Online]. Available: https://www.w3.org/TR/vc-data-model-2.0/

[7] T. Lodderstedt, K. Yasuda, T. Looker, and P. Bastian. (2025). OpenID for Verifiable Credential Issuance 1.0. [Online]. Available: https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html

[8] O. Terbu, T. Lodderstedt, K. Yasuda, D. Fett, and J. Heenan. OpenID for Verifiable Presentations 1.0. OpenID for Verifiable Presentations 1.0. [Online]. Available: https://openid.net/specs/openid-4-verifiable-presentations-1_0.html

[9] C. Mazzocca, A. Acar, S. Uluagac, R. Montanari, P. Bellavista, and M. Conti, "A survey on decentralized identifiers and verifiable credentials," arXiv preprint, arXiv240202455, 2024.

[10] A. Satybaldy, M. S. Ferdous, and M. Nowostawski, "A taxonomy of challenges for self-sovereign identity systems," *IEEE Access*, 2024.

[11] Gaia-X. (2024). Identity, Credential and Access Management Document. [Online]. Available: https://docs.gaia-x.eu/technical-committee/identity-credential-access-management/24.07/

[12] S. B. Shams *et al.*, "Trustworthy supply chain exchange for product carbon footprint," presented at the 2023 IEEE International Conference on Artificial Intelligence, Blockchain, and Internet of Things (AIBThings), IEEE, 2023.

[13] I. I. García, F. D. Muñoz-Escoí, J. A. Aroca, and F. J. F.-B. Peñuela, "Digital product passport management with decentralised identifiers and verifiable credentials," arXiv preprint, arXiv:2410.15758, 2024.

[14] R. Mandaroux, C. Dong, and G. Li, "A European emissions trading system powered by distributed ledger technology: An evaluation framework," *Sustainability*, vol. 13, no. 4, 2106, 2021.

[15] S. Rasool, A. Saleem, M. I. ul Haq, and R. H. Jacobsen, "Towards zero trust security for prosumer-driven verifiable green energy certificates," presented at the 2024 7th International Conference on Energy Conservation and Efficiency (ICECE), IEEE, 2024.

[16] M. Kim, K. Park, and Y. Park, "A reliable and privacy-preserving vehicular energy trading scheme using decentralized identifiers," *Mathematics*, vol. 12, no. 10, 1450, Jan. 2024.

[17] J. A. Alzubi, O. A. Alzubi, A. Singh, and M. Ramachandran, "Cloud-IIoT-based electronic health record privacy-preserving by CNN and blockchain-enabled federated learning," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 1, pp. 1080–1087, Jan. 2023.

[18] O. A. Alzubi, J. A. Alzubi, K. Shankar, and D. Gupta, "Blockchain and artificial intelligence enabled privacy-preserving medical data transmission in Internet of Things," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 12, e4360, 2021.

[19] D. Longley, M. Sporny, and O. Steele. (2025). Bitstring Status List v1.0. [Online]. Available: https://www.w3.org/TR/vc-bitstring-status-list/

[20] Decentralized Identifiers (DIDs) v1.0. [Online]. Available: https://www.w3.org/TR/did-1.0/

[21] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, and W. Polk, "Internet X.509 public key infrastructure certificate and Certificate Revocation List (CRL) profile," RFC Editor, RFC5280, May 2008.

[22] JSON Web Token (JWT). (May 2015). [Online]. Available: https://www.rfc-editor.org/rfc/rfc7519

[23] JSON Web Key (JWK). (May 2015). [Online]. Available: https://www.rfc-editor.org/rfc/rfc7517

[24] Auth0 Lab. [Online]. Available: https://lab.auth0.com/

[25] jose. [Online]. Available: https://github.com/panva/jose/tree/main

[26] pdf-watermark. [Online]. Available: https://github.com/admondtamang/pdf-watermark/tree/main

[27] Microsoft Entra ID. [Online]. Available: https://learn.microsoft.com/en-us/entra/verified-id/

[28] PRé. (Jan. 2016). Introduction to LCA with SimaPro. [Online]. Available: https://pre-sustainability.com/files/2014/05/SimaPro8IntroductionToLCA.pdf

[29] European Commission. (2024). EU Ecolabel facts and figures. Sep. [Online]. Available: https://environment.ec.europa.eu/topics/circular-economy/eu-ecolabel/businesses/ecolabel-facts-and-figures_en

[30] L. Kohnfelder and G. Praerit, "The threats to our products," *Microsoft Interface*, 1999.

[31] D. Fett, K. Yasuda, and B. Campbell. (2025). Selective disclosure for JWTs (SD-JWT). [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-oauth-selective-disclosure-jwt/