Selective disclosure of Digital Calibration Certificate in a quality infrastructure data space

Tomasz Sołtysiński, Jens Niederhausen and Sascha Eichstädt

Physikalisch-Technische Bundesanstalt, 10587 Berlin, Germany

Abstract

This short demonstrator report provides an overview of concept of selective disclosure of Digital Calibration Certificates (DCCs). DCCs contain several different information elements, structured in a way to be machine readable, to provide essential content on calibration process, technical requirements, metrological regulations and performance. In addition, specific sensitive information may be part of the information package to be shared with a DCC. Given the complexity of information, its unique and differential character comprising different aspects of metrological and industrial requirements, its trustworthy and reliable presentation constitutes a real challenge. In our work this challenge is addressed in a framework of verifiable presentations realized by applications of W3C decentralized identifiers (DID) and verifiable credentials (VC) in an international data spaces (IDS) approach. To realize a verifiable presentation of DCC content on demand, the dedicated tools of the Gaia-X environment have been adapted, like Identity & Trust Workpackage of XFSC Toolbox. The proposed approach is easily scalable, extendable, and accessible to any authorized body and industrial partner or company. Constructing verifiable presentation within a Semantic Web data space approach and its tools seems to pave a straightforward, trustworthy way towards machine-readable, interoperable selective disclosure of confident information. Proposed solution has potential to be quickly adaptable to any metrological infrastructure, especially considering a potential European Metrology Dataspace and the recently published Quality-X concept white paper.

Keywords

International Data Spaces, Digital Calibration Certificates (DCC), Decentralized Identifiers (DID), Verifiable Credentials (VC), Verifiable Presentation (VP), Gaia-X, Semantic Web, W3C

1. Introduction

Digital Calibration Certificates (DCC) contain several different information elements, structured in a way to be machine readable, to provide essential content on calibration process, technical requirements, metrological regulations and performance [1]. In addition, specific sensitive information may be part of the information package to be shared with a DCC [2, 3]. Given the complexity of information, its unique and differential character comprising different aspects of metrological and industrial requirements, its trustworthy and reliable presentation constitutes a real challenge [4]. Especially, if a state authority or a notified body claims an access to the content of a DCC, it should be presented quickly, limited to defined requirements on content;

The Second International Workshop on Semantics in Dataspaces, co-located with the Extended Semantic Web Conference, May 26 – 27, 2024, Hersonissos, Greece

tomasz.soltysinski@ptb.de (T. Sołtysiński)
0000-0003-3796-9598 (T. Sołtysiński)

in a restricted, secured and authorized way by means of automated protocols to be easily exchangeable and interoperable between involved parties [5, 6]. Moreover, a DCC framework should provide the data describing metrological information at all steps of calibration chain, i.e. to monitor metrological traceability [7]. DCC circulating in an ecosystem based on distributed ledger technology may fulfill such a requirement [8] and stays very well in line with our approach. In the scope of this study, we explore the research question on how to legally compliant and technically interoperable, selectively present an information carried by a digital certificate circulating in an ecosystem, which is based on a quality infrastructure. Selected use cases are anchored in metrology realm.

In this brief report we: introduce the concept of European Metrology Data Space along with digital certificates; overview general metrological legal landscape; introduce a framework for Quality-X, a digital quality infrastructure preserving trust; briefly characterize the Gaia-X framework; overview the W3C components: decentralized identifiers (DID) and verifiable credentials (VC); show how the derived methods have been adapted to disclosure a content of digital certificate; show the results, discuss them and draw the conclusions, regarding potential application areas.

2. Background and Related Work

2.1. European Metrology Ecosystem as a data space

Metrology activities all along the world bring together different institutions and partners, including public and state authorities, industrial partners and companies, auditors, scientific and research laboratories along with numerous development endeavors ending up with innovation creation [9]. According to a huge number of data created [10], exchanged, communicated and expected to serve in improvement of services to secure its quality is of highest demand [11, 12]. Especially applications based on artificial intelligence (AI) methods are very sensitive to the quality of data [13]. Combining the data, innovative methods and modern, automated semantic-driven exchange protocols adapted to industrial interfaces (Asset Administration Shell (AAS), OPC UA (Open Protocol for Communication Unified Architecture)) to provide better, smarter and real-time services constitutes an ecosystem which can be directly comprised within a data space [14, 15, 16].

Taking into account European regulations and values a European Metrology Data Space (figure 1) can be envisioned, serving as a realm for added value creation, synergistic harmonising particular activities of legal participants [17, 18, 19, 20]. The planes, shown on figure 1 comprise abstract layers, allowing to perform the actions, services and interoperable exchange the data (usage plane). Management plane contains elements responsible for issuing and managing of credentials allowing to exchange the metadata. Trust and identity plane recognizes self sovereign identity (SSI) along with VCs to assign and confirm the compliance. Such an approach allows to implement DCC within a modern, fully digital quality infrastructure meeting demands of industry 4.0 standards [21]. Current needs comprise incorporation of digital assets, like DCC (but also DCoC, Digital Conformity Certificate and DPP, Digital Product Passport) into frameworks based on innovative methods and modern, automated semantic-driven exchange protocols adapted to industrial interfaces (Asset Administration Shell (AAS), OPC UA (Open Protocol for Communication Unified Architecture)), allowing to combine the data in an interoperable manner. These principles have been already implemented in approaches like Catena-X and constitute a proposed framework for those under development, like Manufacturing-X.

Following specific recommendations for metrology (like SI - Standard International units, VIM - The International Vocabulary of Metrology , GUM - Guides to the expression of Uncertainty in Measurement, CODATA - Committee on Data for Science and Technology, ISO 17502) allows to conceptualize an ecosystem. This concept has been shown in 1. Proposed European Metrology Cloud, enabling interoperable exchange of data and protocols regarding metrology applications and specific use cases, like calibration of scales for weighting, used for instance in a market or warehouse, by certification of trolley or shopping carts, etc., can be integrated within an ecosystem where the mentioned standards and protocols are valid and respected. Using Gaia-X framework, effective and secure management can be implemented. Adaptation of this framework for another specific use case, comprising for instance calibration of scales for weighting in biomedical applications is straightforward and requires mostly adaptation of specific legal landscape, while following the general metrological rules.

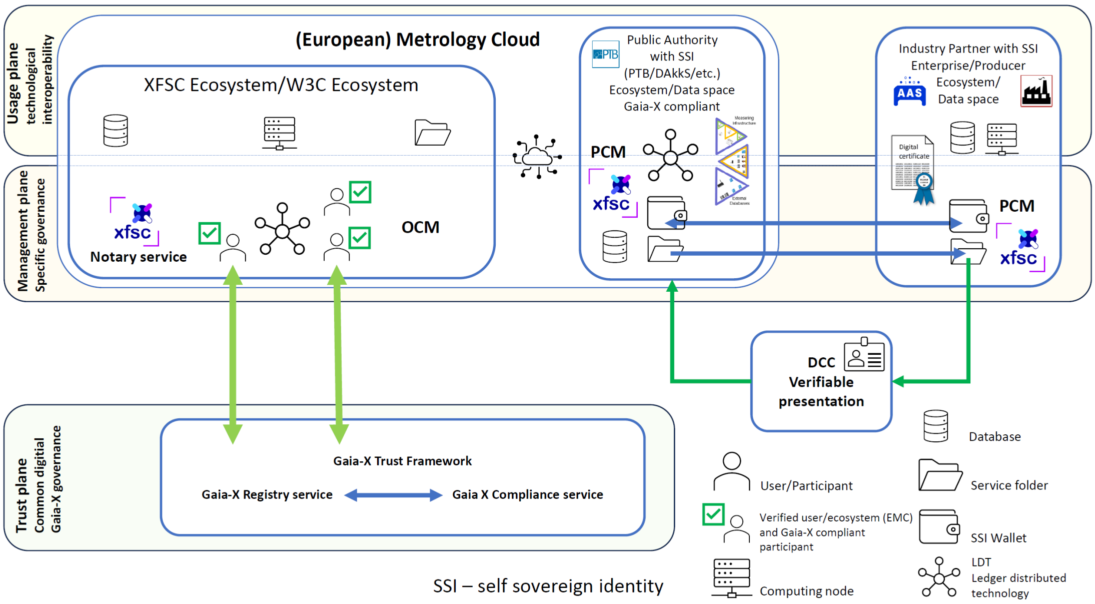

Figure 1: Metrology cloud as an ecosystem within a framework of International Data Space and Gaia-X Trust and Identity tools. Several building blocks and components allow to implement a concept of European Metrology Data Space connecting participants, their resources and mutually offered services. The lines and arrows show the general interactions between components within an ecosystem. Light green arrows show the issuing of verifiable credentials to the organisation; blue lines show the exchange of credentials between participants; dark green lines are showing DCC disclosure as a service offered in a catalogue. SSI is self-responsibly accomplished by the participants - the PTB and a company, in case of illustration.

2.2. Quality infrastructure as a modern and trustworthy digital Quality-X framework

The Quality infrastructure (QI) constitutes a well-established system that comprises all necessary organizations, both public and private, as well as the requisite policies, relevant legal and regulatory frameworks, and practices needed to support and enhance the quality, safety and environmental soundness of goods, services and processes [22]. It builds on metrology, standardization, conformity assessment, accreditation, and market surveillance [23].

Harmonized and interoperable national QI systems are essential for fostering cooperation, promoting mutual trust, and facilitating trade. The true potential of the QI is realized when its elements and actors are seamlessly integrated into a cohesive digital QI ecosystem (figure 1). Recent developments towards industrial international data spaces and specific needs in metrology realm enable such an ecosystem but require the integration of QI principles. As no specific platform has been yet created to tackle the challenge, Quality-X aims at setting the stage for the implementation of a QI ecosystem in international data spaces (IDS), GAIA-X and related German and European projects dedicated to secure data sharing. Quality-X, however, is not about the construction of a platform; it is the creation of an inclusive QI ecosystem with harmonized interfaces. Instead of imposing rigid data structures, it prioritizes interoperability.

The Quality-X framework [24] should seamlessly integrate various components, actors, and assets to create a unified, efficient, and transparent environment. Therefore, Quality-X concept builds upon the existing fundamental elements of IDS:

- **Functional agreements** in a digital QI must contain specifications of services such as calibration, conformity assessment, or accreditation. Each service should have a well-defined definition of processes and roles associated with it, often outlined in regulations or defined by standards. Consequently, functional agreements need to reference their regulatory basis in a traceable manner.
- **Technical agreements** in a digital QI contain definitions of interfaces, data formats, and semantics to ensure interoperability between different organizations within the QI, as well as for the interoperability of QI statements and services with other infrastructures. Frequently, international standards and regulatory documents specify corresponding requirements for these technical agreements.
- **Operational agreements** for digital QI processes must ensure that their origin and outcome are documented in an unambiguous and trustworthy way. Typically, access to data and information relies on well-defined roles, such as market surveillance officers or accreditation auditors, and these roles should be clearly defined in operational agreements.
- **Legal agreements** on data exchange for digital QI processes in data spaces can often be derived from existing legal agreements based on roles and responsibilities in the QI. Transitioning from traditional QI legal agreements to digital QI processes in data spaces presents challenges. The digital landscape amplifies concerns around data privacy, interoperability, jurisdictional variances, and intellectual property rights. Additionally, the redefinition of roles, enforceability of digital contracts, and complexities in liabilities and dispute resolution require attention.
- **Commercial assumptions** in a digital QI are of relevance for all QI services provided by private organizations. For instance, product testing, conformity assessment and

calibration services are often provided by companies. The corresponding assumptions for their integration in a data space must take into account the need for authentication and accreditation of such service providers. A calibration service in regulated areas, for example, can only be provided by a company that has a corresponding accreditation.

- **Liaisons agreements** are an important factor for digital QI processes because services and certificates are typically part of international agreements, treaties and regulations in trade and commerce.

The trustworthy integration of digital QI-related assets, e.g., digital certificates, smart standards, or system of units, with third-party validation has not yet been communicated.

2.3. Gaia-X

Gaia-X is a framework to construct a Gaia-X compliant ecosystem through enabling trust, identity and governance. A set of modules provides building blocks to govern the resources and processes, to grant access and set up the rules through attributes and criteria verified by conformity assessment bodies to be executed within compliance service trust actions. By associating the credentials to the specific requirements (rules, roles, access to resources, etc.) a system of labels (comprising 3 different sets of criteria) has been designed to assign specific participation modus for each user or organisation. A distributed tool called Digital Clearing House (Gaia-X DCH; GXDCH) serves to verify the rules providing a verification node to obtain Gaia-X compliance to be part of the Gaia-X ecosystem. Multiple nodes are being operated by service providers acting as federators. The GXDCH services are under Gaia-X AISBL [25] governance, and anyone can operate it, if compliance to the GXDCH operation rules is proved. The GXDCH is composed of the Gaia-X registry, Gaia-X compliance, Gaia-X notarisation service which are compulsory and can be optionally extended by a portal or catalogue, containing, for instance, offered services. Specific management of the trust and identities is accomplished through two other Gaia-X XFSC Toolbox items; Organisational Credential Manager (OCM) and Personal Credential Manager (PCM).

2.4. W3C components: decentralized identifiers and verifiable credentials

Digital identifiers serve to identify different subjects like persons, objects, organizations, resources or abstract things [26]. Applying cryptographic algorithms, a subject can prove the ownership of information. There is no need for a centralized registry or party in the ecosystem to avoid the single point of failure. To identify a resource, a universal resource identifier (URI) is used, in a similar way when requesting resources via a URL from the world wide web. The required resources to prove the ownership are stored in an associated DID document. These may contain the public keys or a service endpoint to get more information about the subject. The DID method defines in which way to resolve a DID document by getting information from a verifiable data registry. Since the DID core specification is written to support multiple verifiable data registries, the DID method is the required connector between the data registry and the wanted DID document. The W3C specification allows the implementation of multiple methods to deal with DIDs. The only requirement is a unique identifier; the rest is optional or can be expanded by new attributes. By constructing a new method, the basic operations to create, read, update and delete a DID need to be defined. A DID can be designed to be immutable, so no update or delete operation is required and therefore not implemented.

VC is a digital equivalent of paper-based identity documents [27]. Typical VC consist of metadata issuer (issuance date, expiration date, type, description); claims (statement about a subject, for instance: “a company is certified and has obtained valid DCC”) and proof (a digital signature by the issuer) realized in a form of a cryptographic key. The credentials are used for multiple applications like certificates of identity such as personal identity cards; legal entity identification (GLEIF, Global Legal Entity Identifier Foundation); certificates such as ISO 27001 certificates, BSI (The British Standards Institution) security certificates, ITIL (Information Technology Infrastructure Library) or TOGAF (The Open Group Architecture Framework) certificates; attestations, Gaia-X compliance level, authenticity confirmation, vaccination confirmation; competences such as a license to practice medicine, data scientist qualification; contracts, used to specify negotiated cloud service or data usage policies; powers such as official authority (EU, Gaia-X AISBL) or residence permits; qualifications, for example, proof of trained personnel to administer cloud services; membership cards, e.g. Gaia-X membership, club cards, proof of membership of an association or society; loyalty cards such as bonus cards or frequent flyer programs.

3. Methods

In our work the challenge of a trustworthy integration of digital QI-related assets, with third-party validation, is addressed in a framework of verifiable presentations realized by applications of W3C DID and VC [28] in an international data spaces (IDS) approach [29, 30]. We construct a Gaia-X compliant data space, securing trust through assigning the credentials and identity by means of DIDs and SSI. To realize a verifiable presentation of DCC content on demand, the Identity & Trust Work Package from XFSC Toolbox within the Gaia-X environment [25] has been adapted. Such an open-source-based approach, utilizing the tools of Cross Federation Services developed by Gaia-X [31] and the Eclipse Foundation [32] demonstrates a secured, restricted and interoperable, automated framework to present only required information of interest to a state authority or any government office.

To realize the data space the following W3C Spec standardized components have been adopted: DID, DID documents, VC, VP, and non W3C elements, like Gaia-X GXFS/XFSC Toolbox OCM, and PCM.

Sovereign self-description with SSI has been accomplished through self-generated decentralized identifiers assigned within a user domain according to a chosen method and associated with a specific DID document along with gathered credentials. A DID-Doc can be resolved in the global Web and the credentials can be read out, verified, and presented. All obtained or assigned credentials are stored in the user’s wallet (PCM). SSI is done locally, DID has been associated with a local testbed domain implemented on Amazon AWS EC2 environment. To perform the tests, a framework was used, as implemented by the GXFS Tech Workshop #5 [33].

4. Results

The results are shown on figures 2 to 4 along with thorough discussion in this section.

To accomplish a selective disclosure a verifiable presentation is done. According to demand and needs only selective information extracted from a DCC is provided, as permitted by owned credentials. As the specific authorities require access to limited information of specified kind, only selective, restricted, limited (if required, anonymised or pseudonymised) content is published to the authority. In this way, an individual, unique verifiable presentation is created (figure 2). For instance, if a one dedicated authority (in our case, Physikalisch-Technische Bundesanstalt, the PTB) requires access to a digital certificate (like DCC) it can be accomplished through posting a relevant service in a data space catalogue, which is accessible from the side of addressed company (they share the corresponding credential). At the same time the company enables access to its catalogue from the side of the authority, offering a specific authority-tailored selective disclosure. In this way, a digital certificate can be read out, while keeping secret information. The same scenario can be realized by another authority (the DAkkS), interested in other specific content of the same digital certificate possessed by the company.

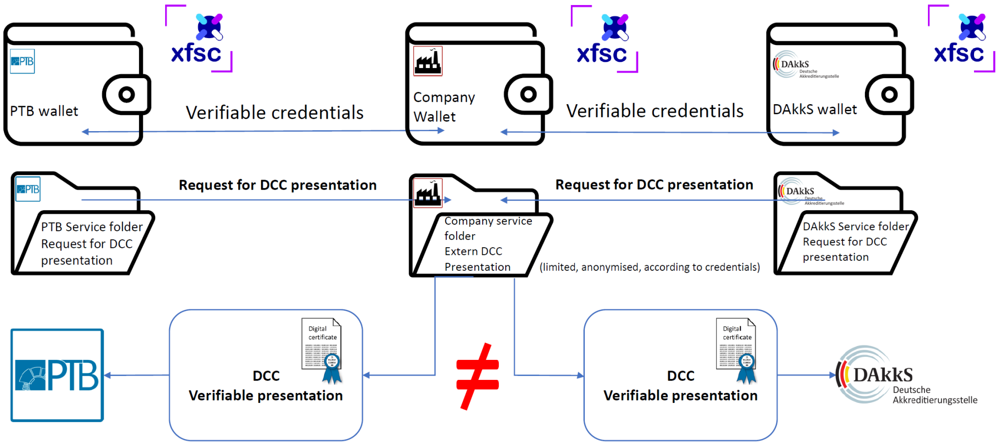
xfsc
PTB wallet
Verifiable credentials
Company Wallet
xfsc
Verifiable credentials
DAkkS wallet
xfsc
Request for DCC presentation
Request for DCC presentation
PTB Service folder Request for DCC presentation
Company service folder Extern DCC Presentation
(limited, anonymised, according to credentials)
DAkkS Service folder Request for DCC presentation
PTB
Digital certificate
DCC Verifiable presentation
≠
Digital certificate
DCC Verifiable presentation
DAkkS Deutsche Akkreditierungsstelle

Figure 2: Storing a set of tailored verifiable credentials in a wallet, assigned to each participant, specific services may be offered, being exposed in dedicated service catalogues. By verifying the credentials, a verifiable presentation on demand can be accomplished, adapted to the needs of a public authority. Verifiable presentation to PTB is not equal to the one disclosed to DAkkS, as explained in the text of the manuscript.

A legal participant is being registered in a Gaia-X notary service through issuing relevant credential. Issuing subsequent credentials, the conformity with Gaia-X legal terms and conditions is accomplished. Combining the credentials together with a DID document, a compliance within federated data space is secured. Final credentials are then stored in the wallet of a legal participant, which can be further presented on demand, or used to execute offered services exposed in a federated catalogue (figure 3). Each component in the ecosystem is identified through a specific DID, relevant DID-Doc and a final set of credentials confirming the compliance and credibility of the participant (the PTB as authority, in the case) is further presented out. This set of credentials may be associated to specific service to be found in a relevant catalogue, recognizable by other parties (like a company with DCC).

The credentials are managed using two tools running in a system and communicating through APIs: OCM and PCM [34]. The OCM runs in a federated ecosystem and establishes trust between the different participants within the Gaia-X ecosystem by offering credentials to company. PCM acts as a user representative, securely holding the acquired distributed identity credentials and identity attributes, providing the technical means to selectively disclose the attributes for authentication and service consumption. The PCM, as a Gaia-X component, is used by a natural person – typically in the form of a personal wallet for a user. The PCM enables users to interact with the SSI-based ecosystem through VC'S and DID's in a privacy-preserving way. The PCM form factors are smartphone-based applications and browser-based applications/add-ons for stationary PCs and notebooks. In our case, the holder of PCM wallet is a representant of authority, granted with the access to the DCC content.

Constructed scenario demonstrates the concept to realize selective disclosure of confident data contained in a DCC, to be automatically, interoperable read out. Such a protocol can be used, for instance, to extract and publish the information on metrological traceability of particular measurements, their uncertainties performed over a chain of calibrations. In this way a path originating from digital SI units can be followed and all the measurement chain is reliably known and monitored, as shown in details on (figure 4). The scenario has been implemented and tested internally and none web interface is accessible yet from outside.

As already mentioned in introduction, an exchange of metadata, data, and certificates regarding calibration of scales for weighting is a very attractive application domain. A need to communicate between stakeholders (legal or accrediting authority, company, warehouse, calibration laboratory) spread in different Member States of EU can be successfully fulfilled, if proposed protocols would operate within the European Metrology Cloud and its ecosystem, following the rules of international data spaces.

5. Discussion and conclusion

The proposed approach is easily scalable, extendable, and accessible to any authorized body and industrial partner or company, as all the required effort is to self-describe themselves with DID and DID-Doc and to gather required credentials. By accepting terms and conditions of the Gaia-X ecosystem, any legal participant can join the ecosystem and use the offered services exposed in a federated catalogue [35]. Ongoing research is performed to validate and evaluate this approach in the frameworks of local infrastructure and already developed and implemented preliminary demonstrators for communication layer and European Metrology Cloud proposed by the PTB.

Due to the current state-of-the-art frameworks and technological solutions based on public

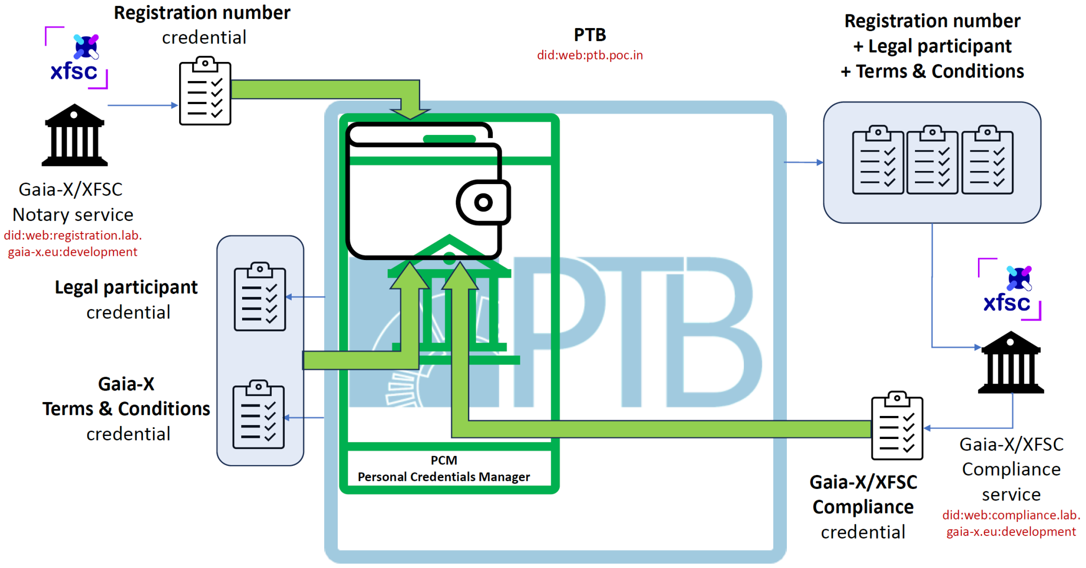

Figure 3: A legal participant is required to be identified and registered in a Gaia-X framework. Self-description is performed by creating DIDs, issuing the credentials and storing them in DID documents. The credentials need to be verified (through resolving DIDs and relevant DIDs documents) by relevant services (notary, compliance ones). If succeeded, the final credential set is being kept in a wallet and serve to perform verifiable presentation allowing to join a federation and enabling publishing one's service offerings to a catalogue. Light green lines are showing how the particular credentials are stored in a wallet, other lines let to follow the flow of credentials in the process of compliance assignment.

and private RSA-keys, the use of DIDs and VCs establishes a secure framework. Regarding the specification under development and ongoing efforts towards standardization potential security vulnerabilities and privacy implications are yet to be analysed as such issues are beyond the scope of this paper and hardly addressed in the up-to-date literature. To the point, the system mitigates risks associated with decentralized identifiers in the same way, as when the RSA-cryptography is used. Securing DIDs and DID documents relies on the users and is their specific responsibility. Current state of technology and well established strength of RSA methods ensure data privacy and credibility of ecosystem's data traffic.

Incorporating semantic web framework the DCCs (or DCoC, DPPs) can be further automatised to provide reach protocols allowing not only to read out the metadata, data, specific information but also to operate on the content through attached machine-executable services [36].

As well a DCoC or DPP can be equipped with digital rights, implemented as transferable VCs, a VP can be realized to provide selective disclosure also regarding potential GDPR- or user- or local-policy-conform selective reading out of a DCoC/DPP, keeping sensible information protected. Thus, any interoperable machine-readable automation of the process within a data space should be straightforward. A DCC is not so restrictive and leave much more freedom in constructing a disclosure.

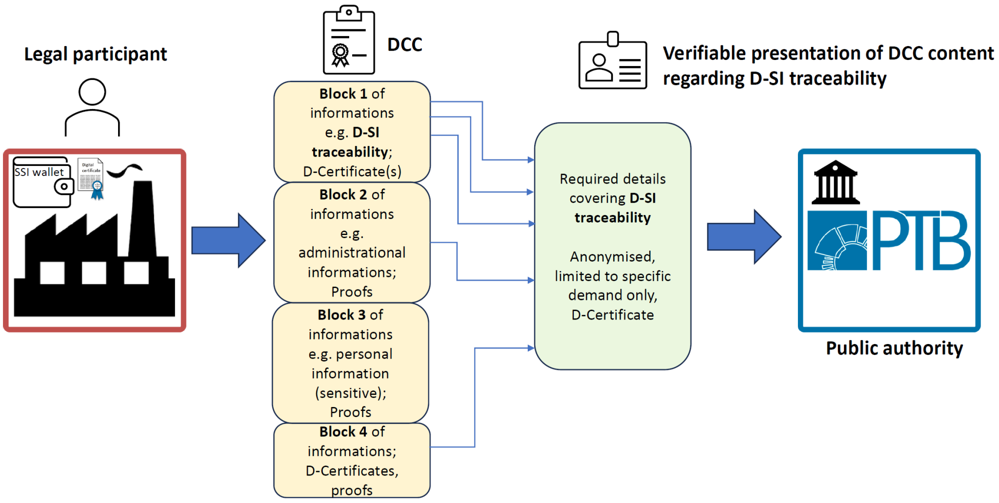
Legal participant
SSI wallet
DCC
Block 1 of informations e.g. D-SI traceability; D-Certificate(s)
Block 2 of informations e.g. administrational informations; Proofs
Block 3 of informations e.g. personal information (sensitive); Proofs
Block 4 of informations; D-Certificates, proofs
Verifiable presentation of DCC content regarding D-SI traceability
Required details covering D-SI traceability
Anonymised, limited to specific demand only, D-Certificate
PTB
Public authority

Figure 4: Performing a service of selective disclosure, made available in a federated catalogue and according to assigned credentials, the verifiable presentation is accomplished revealing only the required metadata. The verifiable presentation is proven by resolving associated DIDs, DIDs documents, assigned credentials allowing to disclose the specific content of DCC (chosen fields of DCC blocks) by a company to an authority (like PTB). In this way, a selective disclosure is performed in the framework of minimal viable Gaia-X product (MVP).

Through application of DIDs, VCs, self-description and secured communication, we developed a scenario demonstrating a concept for selective disclosure of digital certificates along with a discussion of a use case in a metrology network. Such an approach is easily adaptable to any metrological infrastructure, especially considering a potential European Metrology Dataspace and the recently published Quality-X concept white paper [24]. Although some software tools have been proposed to store the data in DCC [37], there are no satisfactory solutions for managing and sharing DCCs. Completed efforts, like DCC2GO project [38], undertaken by the PTB and cooperating partners, cover several activities considering this challenge. Proposed DCC starter kit contains step-by-step guidance for the creation, practical implementation and secure delivery of temperature and pressure DCCs [39]. That project comprises knowledge and experience on IT tools for the creation and usage of DCCs, addresses the question on how cryptographic tools, in particular digital signatures can be securely used with DCCs to protect and validate their content. The results of DCC2GO also show how to consider the large number of issued calibration certificate types and their wide range of applications. Our work preliminary contributes to such endeavors using novel conceptual approach adopting Gaia-X and IDS frameworks. Moreover, such an approach allows to include blockchain technology (e.g. EBSI) to secure traceability, what constitutes one of possible future research directions. The presented use case constitutes a minimum viable product (MVP) in the framework of the Gaia-X ecosystem and is directly extendable by any IDS component, including Eclipse connectors [40].

Acknowledgments

We would like to thank the Gaia-X Association along with Gaia-X Federation Services, now converted to Cross Federated Services (XFSC), The Eclipse Foundation and International Data Space Association (IDSA) for developing open source solutions, letting to implement a basic federated data space.

References

[1] S. Hackel, S. Schönhals, T. Krah, L. Doering, Maschinenlesbares und maschineninterpretierbares digitales Kalibrierzertifikat (DCC) und sein Einsatz in der Praxis, tm - Technisches Messen 91 (2024) 51–62. URL: https://doi.org/10.1515/teme-2022-0117. doi:doi:10.1515/teme-2022-0117.

[2] J. Schaerer, T. Braun, A distributed Calibration Certificate Infrastructure, 2022, pp. 1–4. doi:10.1109/BRAINS55737.2022.9909437.

[3] J. Nummiluikki, S. Saxholm, A. Kärkkäinen, S. Koskinen, Developing and testing Digital Calibration Certificate in an industrial application, 2022, pp. 1–4. doi:10.21014/tc6-2022.026.

[4] T. Engel, GEMIMEG-II - how metrology can go digital…, Measurement Science and Technology 34 (2023). doi:10.1088/1361-6501/ace468.

[5] E. Morse, S. Heysiattalab, A. Barnard Feeney, T. Hedberg, Interoperability: Linking design and tolerancing with metrology, Procedia CIRP 43 (2016) 13–16. doi:10.1016/j.procir.2016.04.106.

[6] C. Brown, T. Elo, K. Hovhannisyan, D. Hutzschenreuter, P. Kuosmanen, O. Maennel, T. Mustapää, P. Nikander, T. Wiedenhoefer, Infrastructure for Digital Calibration Certificates, 2020, pp. 485–489. doi:10.1109/MetroInd4.0IoT48571.2020.9138220.

[7] P. Neyezhmakov, S. Zub, S. Pivnenko, Preliminary E-infrastructure for Digital Calibration Certificate, Measurement: Sensors 18 (2021) 100332. URL: https://www.sciencedirect.com/science/article/pii/S2665917421002956. doi:https://doi.org/10.1016/j.measen.2021.100332.

[8] T. Takatsuji, H. Watanabe, Y. Yamashita, Blockchain technology to visualize the metrological traceability, Precision Engineering 58 (2019) 1–6. URL: https://www.sciencedirect.com/science/article/pii/S0141635919303071. doi:https://doi.org/10.1016/j.precisioneng.2019.04.016.

[9] S. Eichstädt, M. Gruber, A. P. Vedurmudi, Integrating metrological principles into the Internet of Things: a digital maturity model for sensor network metrology, tm - Technisches Messen 91 (2024) 17–31. URL: https://doi.org/10.1515/teme-2023-0103. doi:doi:10.1515/teme-2023-0103.

[10] E. Ramalli, B. Pernici, Challenges of a Data Ecosystem for scientific data, Data Knowledge Engineering 148 (2023) 102236. URL: https://www.sciencedirect.com/science/article/pii/S0169023X23000964. doi:https://doi.org/10.1016/j.datak.2023.102236.

[11] A. M. Schleimer, N. Jahnke, B. Otto, Architecture design options for Federated Data Spaces, 2023. doi:10.24251/HICSS.2023.447.

[12] S. Windmann, A. Maier, O. Niggemann, C. Frey, A. Bernardi, Y. Gu, H. Pfrommer, T. Steckel, M. Krüger, R. Kraus, Big Data analysis of manufacturing processes, Journal of Physics: Conference Series 659 (2015) 012055. URL: https://dx.doi.org/10.1088/1742-6596/659/1/012055. doi:10.1088/1742-6596/659/1/012055.

[13] S. Knake-Langhorst, C. Linder, J. Mazzega, GAIA-X 4 KI: Daten- und Dienste-Ökosystem für KI-orientierte Forschung & Entwicklung, 2021.

[14] S. Auer, Semantic integration and interoperability, in: B. Otto, M. ten Hompel, S. Wrobel (Eds.), Designing Data Spaces : The Ecosystem Approach to Competitive Advantage, Springer International Publishing, 2022, pp. 195–210. URL: https://doi.org/10.1007/978-3-030-93975-5_12. doi:10.1007/978-3-030-93975-5_12.

[15] M. Neubauer, L. Steinle, C. Reiff, S. Ajdinović, L. Klingel, A. Lechler, A. Verl, Architecture for Manufacturing-X: Bringing Asset Administration Shell, Eclipse Dataspace Connector and OPC UA together, Manufacturing Letters 37 (2023) 1–6. URL: https://www.sciencedirect.com/science/article/pii/S221384632300024X. doi:https://doi.org/10.1016/j.mfglet.2023.05.002.

[16] A. Vedurmudi, M. Gruber, S. Eichstädt, Semantic description of Quality of Data in sensor networks, Sensors 21 (2021). doi:10.3390/s21196462.

[17] E. Farrell, M. Minghini, A. Kotsev, J. Soler-Garrido, B. Tapsall, M. Micheli, M. Posada, S. Signorelli, A. Tartaro, J. Bernal, M. Vespe, M. Di Leo, B. Carballa-Smichowski, R. Smith, S. Schade, K. Pogorzelska, L. Gabrielli, D. De Marchi, European data spaces – Scientific insights into data sharing and utilisation at scale, Publications Office of the European Union, 2023. doi:doi/10.2760/400188.

[18] A. Gieß, F. Möller, T. Schoormann, B. Otto, Design options for Data Spaces, 2023.

[19] S. Scerri, T. Tuikka, I. Vallejo, E. Curry, Common European Data Spaces: Challenges and Opportunities, 2022, pp. 337–357. doi:10.1007/978-3-030-98636-0_16.

[20] I. Jussen, F. Möller, J. Schweihoff, A. Gieß, G. Giussani, B. Otto, Issues in inter-organizational data sharing: Findings from practice and research challenges, Data Knowledge Engineering 150 (2024) 102280.

[21] S. Hackel, S. Schönhals, L. Doering, T. Engel, R. Baumfalk, The Digital Calibration Certificate (DCC) for an End-to-End Digital Quality Infrastructure for Industry 4.0, Sci 5 (2023). URL: https://www.mdpi.com/2413-4155/5/1/11. doi:10.3390/sci5010011.

[22] S. Eichstädt, D. Hutzschenreuter, J. Niederhausen, J. Neumann, The Quality Infrastructure in The Digital Age: Beyond machine-readable documents, 2022, pp. 1–4. doi:10.21014/tc6-2022.042.

[23] Qi-Digital Initiative, 2023. URL: https://www.qi-digital.de/, accessed: 2024-03-12.

[24] Quality-X White Paper, 2023. URL: https://www.qi-digital.de/fileadmin/user_upload/website/publikationen/1022_Brosch%C3%BCre_Quality-X_v4.pdf, accessed: 24-04-17.

[25] Gaia-X Association, 2024. URL: https://gaia-x.eu/, accessed: 2024-03-12.

[26] Analysing the SSI World, Whitepaper, August 2023. Whitepaper.

[27] B. Meier, N. Pohlmann, Gaia-X secure and trustworthy ecosystems with Self Sovereign Identity, 2022. Whitepaper.

[28] C. Brunner, U. Gallersdörfer, F. Knirsch, D. Engel, F. Matthes, DID and VC: Untangling

Decentralized Identifiers and Verifiable Credentials for the Web of Trust, 2021. doi:10.1145/3446983.3446992.

[29] S. Bader, J. Pullmann, C. Mader, S. Tramp, C. Quix, A. Müller, H. Akyürek, M. Böckmann, B. Imbusch, J. Theissen-Lipp, S. Geisler, C. Lange, The International Data Spaces Information Model – An Ontology for Sovereign Exchange of Digital Content, 2020, pp. 176–192. doi:10.1007/978-3-030-62466-8_12.

[30] International Data Spaces Association, 2024. URL: https://internationaldataspaces.org/, accessed: 2024-03-12.

[31] Gaia-X Cross Federation Services, 2024. URL: https://www.gxfs.eu/, accessed: 2024-03-12.

[32] Eclipse Foundation XFSC, 2024. URL: https://projects.eclipse.org/projects/technology.xfsc, accessed: 2024-03-12.

[33] GXFS Tech Workshop #5, 2023. URL: https://gitlab.eclipse.org/eclipse/xfsc/workshop/xfsc-tech-workshop-5/documentation-for-xfsc-tech-workshop-5, exercise 1.

[34] Gaia-X Federation Services, Gaia-X Ecosystem Kickstarter, December 2021.

[35] A. M. Schleimer, E. Duparc, Designing digital infrastructures for industrial data ecosystems - a literature review, 2023.

[36] G. Öktem, S. Hackel, F. Härtig, J. Loewe, B. Gloger, J. Jagieniak, Digital SchemaX and the future of the Digital Calibration Certificate, 2022, pp. 1–4. doi:10.21014/tc6-2022.028.

[37] D. Baslev-Harder, A. Bošnjaković, H. D. Brown, C., L. Lillepea, A. Karkkainen, K. A., P. Østergaard, Example for the creation of a Digital Calibration Certificate (DCC) in XML and PDF/A-3 for people who start working with DCCs., Zenodo. https://doi.org/10.5281/zenodo.8199718, 2023.

[38] DCC2GO, 2023. URL: https://www.ptb.de/dcc2go/project, accessed: 2024-03-12.

[39] D. Baslev-Harder, A. Bošnjaković, C. Brown, D. Hutzschenreuter, A. Karkkainen, K. Anke, L. Lillepea, P. Østergaard, J. Vahi, Freely available and validated, Digital Calibration Certificates (DCC) starter kit for DCC implementation; containing step-by-step guidance for the creation, practical implementation and secure delivery of temperature and pressure DCCs, 2023. URL: https://doi.org/10.5281/zenodo.8199700. doi:10.5281/zenodo.8199700.

[40] W. Melo Junior, Blockchains and legal metrology: applications and possibilities (2021). doi:10.13140/RG.2.2.16861.95208.