REBOOTING THE WEB OF TRUST

DESIGNING THE FUTURE OF DECENTRALIZED SELF-SOVEREIGN IDENTITY

A WHITE PAPER FROM RWOT XI: THE HAGUE

Linking Credentials with Data Exchange Agreements through Secured Inclusive Interfaces

On the need to link verifiable credentials with the right to use data in a secure, inclusive user interaction

by Lal Chandran, Lotta Lundin, Fredrik Lindén, Philippe Page, Paul Knowles, Víctor Martínez Jurado, Andrew Slack

RWOT XI GOLD SPONSORS:

Abstract

In this collaborative work from RWOT11, we revisit the issue of patient data exchange in a setting requiring cross-border, multi-jurisdiction, and inclusive access to all participants. A fundamental problem in developing large-scale real-world solutions based on verifiable credentials is keeping the simplicity of usage for individuals in different contexts without sacrificing security.

We aim to highlight selected technical challenges and outline how the DEXA and OCA protocols contribute to scalable solutions.

We illustrate our essay with the well-known use case of the digitalised patient prescription, but cast in a multi-jurisdictional setting and considering the accessibility requirement of a visually impaired patient. This scenario provides a tangible setting to translate the technical challenges into legal and societal questions:

1. How Data Exchange Agreements address the fundamental legal data protection requirements (e.g. GDPR) in a scalable, auditable, and convenient manner for all parties involved in a data exchange transaction.

2. How task-oriented layered overlays offer a secure user-centric solution for language and accessibility requirements.

We start by stating the problem along three dimensions: i) verifiable credential presentation and wallet appropriation, ii) agreements for data exchanges in muti-jurisdictions, and iii) preservation of context. Then, the following sections outline the existing solutions and present the contributions of the DEXA and OCA protocols toward the solution.

The essay provides references and appendices for readers interested in going deeper.

1. Introduction

This essay links verifiable credentials with the right to use data in a secure and inclusive user interaction. We illustrate our approach through the well-known scenario provided by the digitalisation of the patient prescription.

1.1 Revisiting the issue of patient data exchange in a cross-border, multi-jurisdiction, and inclusive setting

In our scenario, Fredrik is a visually impaired Swedish resident undergoing treatment at a local healthcare provider. Following Fredrik's last visit, the healthcare provider delivered a digital prescription made available in the Swedish-governed healthcare data space. The health data space must meet the requirements of the countries' health professionals, including insurance, public health, and other third parties. The system is also accessible to patients, independent of their location, apart from allowing cross-border jurisdictional usage. For example, this will be necessary when Fredrik visits his daughter studying in Zurich, Switzerland (i.e. a non-EU jurisdiction).

While in Zurich, Fredrik uses his digital prescription in a Swiss pharmacy not connected to the Swedish healthcare system. Fredrik speaks only Swedish, and the pharmacist only German. Therefore we assume that both Fredrik and the pharmacist have an online connection and can exchange digital information.

Fredrik can provide verifiable information that the pharmacist must authenticate. In turn, the swiss pharmacist must also deliver authentic information that the Swedish healthcare system will require for its internal processes (e.g. to avoid prescription double-spend).

Our scenario requires that all transactions are auditable, and Fredrik is issued a receipt and warning in Swedish for the possible adverse effects of taking medicine.

This scenario exemplifies the need for human-centric, context-aware, device-independent automated agreement handling for data exchange between a Data Source (DS) and a Data Using Service (DUS).

1.2 Presentation - Agreements - Context

Verifiable credentials (VC) will become critical components for the digital transformation of real-world processes. However, in light of that positioning, VC will have to be integrated into digital processes that deliver at least the same level of security, usability, and safety as their paper-based counterparts in the physical world. The above scenario is a complex edge case for a system designer, but deviations from standard designs are the rule in real-world systems. Enabling this real-world diversity in a machine-readable format is the fundamental driver behind the growing emergence of decentralised systems.

To achieve this, the VC faces a few steep challenges to ensure broad adoption. In this paper, we illustrate three challenges:

- VC representation and wallet appropriation
- VC and multi-jurisdictional data exchange agreements
- VC and context preservation

1.3 The RWOT11 collaboration

The collaborative work done during the RWOT11 conference brought together authors from three organisations to address these challenges:

- [VM, AS] *Representations and Accessibility* requirements for VC;
- [LC, FL] *Data exchange agreements*. DEXA protocol for data exchange;
- [PP, PK] *Context preservation & governance*. Overlays Capture Architecture for data presentation.

At the start of his user journey, Fredrik has to interact with the information system. Section two, “Credential Representation”, deals with the challenges for systems designers. We present the current state-of-the-art credential rendering and demonstrate the need to decouple verifiable data from the presentation layer. For Fredrik and the Swiss pharmacists to have a trusted relationship, such decoupling is required. Each will rely on the level of assurance provided by their respective systems, not a common platform.

Similarly, section three, “Data Exchange Agreements (DEXA) protocol”, demonstrates the need to link verifiable data to context-dependent agreements. Fredrik receives a prescription within the Swedish ecosystem designed for the country and uses it in a different ecosystem. Starting from the legal requirement of data protection, we introduce how agreements link to a transaction through the open-source protocol DEXA.

The proposed data exchange agreements attached to the transaction integrate better into the context of the relationships between organisations and individuals, depending on their roles in different usage scenarios involving personal data. The agreements can be classified into four broad categories, as shown in the figure below. These are agreements between:

- An individual and an organisation (data agreement)
- Two organisations, a data source and a data-using service (data disclosure agreement)
- An organisation and its supplier (data processing agreement)
- Two individuals (delegation agreement)

In Section 4, “Context preservation — a decentralised semantic approach”, we deal with the dynamic context-aware requirement imposed by Fredrik. Different languages and accessibility requirements are examples of context-dependent use of verifiable information. These requirements differ from credential presentation in section two and data exchange agreements in section three. Collectively they point to decentralised semantics, a concept that breaks down the definition of digital objects into a layered structure. Finally, we introduce Overlays Capture Architecture (OCA) to enable Fredrik’s multi-lingual credential exchange independent of other presentation layers.

2. Credential representations

Any human-operated system's security and user experience depends on the contextual information conveyed through user interfaces, user responses, and the interpretation of user actions. Unlike physical credentials or closed-loop digital systems, issuers of VC rely on a variety of software or hardware wallets to interpret and convey comprehensible information to users. The wallets define the representation of data and user experience in critical moments of interaction, in which users have to make choices about sharing, accepting, and verifying that data.

Wallets also have to cater to existing user mental models regarding how credentials are represented and used. In many contexts there are pre-conceived ideas of what, for example, an id card, a passport, or a medical prescription 'looks like' and how it can be used. Relying on a wallet to replicate the appearance of an existing credential may initially seem appealing since such a skeuomorphic approach could ease public acceptance but there are drawbacks. Government and public body issuers have expressed concerns about confusion between digital and physical artefacts that may have differing legal status, liabilities, or associated level of assurance, as well as divergent acceptance and verification processes. It is therefore advised that VC should be distinct from any physical counterparts.

Additionally, physical credentials often contain accessibility features, or can be issued in alternative formats or languages, to support inclusivity requirements. Unfortunately, existing representation and interaction patterns in VC wallets tend towards visual-centric models that are not accessible. If VC and wallets are to support public sector applications they must meet accessibility requirements, such as European Standard for Digital Accessibility or US Section 508 [6], to make them usable for all in society.

While there are some common patterns that are applied to the representation of VC today, such as the prominent use of 'cards' as a way to display credentials, the implementation details remain at the sole discretion of wallet providers. This can lead to inconsistent data representations across software, platforms, and devices. As adoption and use of credentials expands, wallets are also needing to adapt to handle greater volumes and variety of data and more complex combinatorial applications of this data. It should therefore be anticipated that there will be an evolution, and potentially diversification, of wallet interaction models beyond the card-centric approach seen today. UX-informing material embedded or securely referenced within verifiable data can help issuers to ensure consistent, recognisable, and accessible representations of the data they sign within a diversity of wallet contexts.

Consistency in data representation does not need to mean uniformity in wallet experiences however. Wallets should provide cohesive, culturally and contextually relevant experiences that cater to individual preferences and needs. These experiences may vary significantly between individuals and regions and can relate to language, colours, symbology, motion, voices, and audio tones. A balance has to be found between consistent representation of issuer data and contextually relevant appropriations.

2.1 Current state of the art

Within the VC community, there exist a number of proposals for defining how a credential should be 'rendered', such as the Open Badges [12], DIF Wallet Rendering (draft) [9], and Credential Manifest [11] specifications, as well as another proposal from RWOT11 for Rendering Verifiable Credentials. All of these provide rendering 'hints' that are embedded, or linked, UI markup within the credential schema. While such approaches can give issuers control over the consistent representation of the credential, they promote document-centric representation of the data that reduces flexibility in its use and limits possibility for appropriation by wallets to meet consumer preferences or contextual needs. For example, pre-determined visual layouts for credentials, possibly from multiple issuers, may be challenging for wallets to cohesively display alongside each other. This could result in difficulty for users to understand data, and may induce additional cognitive burden.

Additionally, these approaches risk adding significant bulk to the credential size since additional render data is required despite the fact it may not be used in all cases; for example, a machine agent does not require a visual rendering. This can affect usability of the verifiable data, especially for those with limited network access that may want to interact with lighter versions of a credential. It would be preferable to keep credentials lean with the possibility for wallets to add contextually relevant semantics on demand.

The RWOT proposal addresses accessibility requirements by providing capability to embed alternative rendering formats or hints, such as audio or tactile instruction sets. However, this approach results in multiple duplicates of the same data being

provided for each rendering type and the need for format specific instructions to be included. This gives complete control to the issuer regarding the representation of the data across all representation types. Though a paired back approach, providing only the necessary metadata such as attribute labels and descriptions, would be sufficient for native or browser based assistive tooling to comprehend and interpret into relevant formats [6]; for example, audio, tactile, or haptic feedback. This would allow for a leaner credential and more flexibility in how a wallet could appropriate the data in contextually relevant ways while still ensuring the issuer was in control of defining the source data.

A pattern already seen in popular OS 'wallet apps' is for the wallet provider to define a set number of layout types depending on data object typology; for example, Apple Wallet has five "Pass" styles: Boarding pass, Coupon, Event ticket, Store card, and Generic. The data provider can then populate these layouts with attributes and attribute characteristics. This pattern provides a consistent in-wallet experience while allowing the data provider to define specific representation characteristics for data attributes in different media formats. This helps to create distinctive yet consistent representations, allowing for easier recognition and lower cognitive burdens for data consumers using the wallet. This approach also results in more constrained requirements in terms of data needed from the provider, leaving layout to the wallet.

2.2 Design for appropriation

This approach of decoupling verifiable data from the presentation layer would enable VC to move away from static, document-centric representations and embrace contextual flexibility and portability of user-held verifiable data. The Overlay Capture Architecture (OCA), described later in this paper, provides such a method to do this. Issuers are able to define and host a bundle of 'semantic overlays' that are referenced in the credential and that wallets can fetch as required. The overlays provide metadata that supports contextually relevant credential and attribute representations. For example, a language overlay can provide translated attribute descriptions, these could be used by assistive technologies to drive an audio representation. An asset overlay can provide the logo of the issuer and its display aspect ratio. The benefits of this decoupling of data and presentation are three-fold:

- It discourages skeuomorphic representations of data objects. For example, a passport that looks like a physical passport document. Verifiable data objects made to look like existing physical artefacts are a dangerous design pattern, with uninformed verifiers potentially reverting to visual information checks, trusting visual inspections rather than cryptographically verifying the data presented. It can also introduce confusion for users about how the data can be used and what the verification processes are.
- It allows verifiable presentations to draw on UX-informing material for specific attributes sourced from multiple credentials. This supports greater flexibility for individuals to re-use the data they hold.
- It supports greater inclusivity by providing attribute metadata that can be used to drive alternative representations of data using assistive technologies. Importantly, and uniquely, it does this in such a way that it does not encumber the VC itself with additional layout or formatting information that may not be necessary in all cases. Such additional data may itself exclude those who have limited network access.

2.3 Use case scenario

In the context of a cross-border health data exchange, credential representations need to be available in multiple languages and may need to meet regionally specific accessibility requirements. Within a population there will also be diverse access to technology, devices and networks. Individuals will have unique preferences and needs in how they consume their data, some perhaps with differing abilities requiring wallets that provide multimodal feedback. The preferences of the data subject may be very different from the requirements of the health professionals with whom they share their data.

The proposed approach of utilising semantic overlays to appropriate the representation of data in a way that is relevant to its contextual use supports this use case. We detail the flow later, in the conclusion of the paper.

3 Data Exchange Agreements (DEXA) protocol

3.1 Background: The data exchange landscape

New data regulations are emerging worldwide, mandating organisations to implement controls and safeguards when processing, consuming, and exposing personal data. Typically, a Data Protection Impact Assessment (DPIA) or similar process details the purpose of data usage, the lawful basis, etc.

In the DEXA framework, the conversion of DPIA results to a machine-readable format constitutes the basis for any agreement between the stakeholders in the data exchange ecosystem, as illustrated in figure 3.1 below.

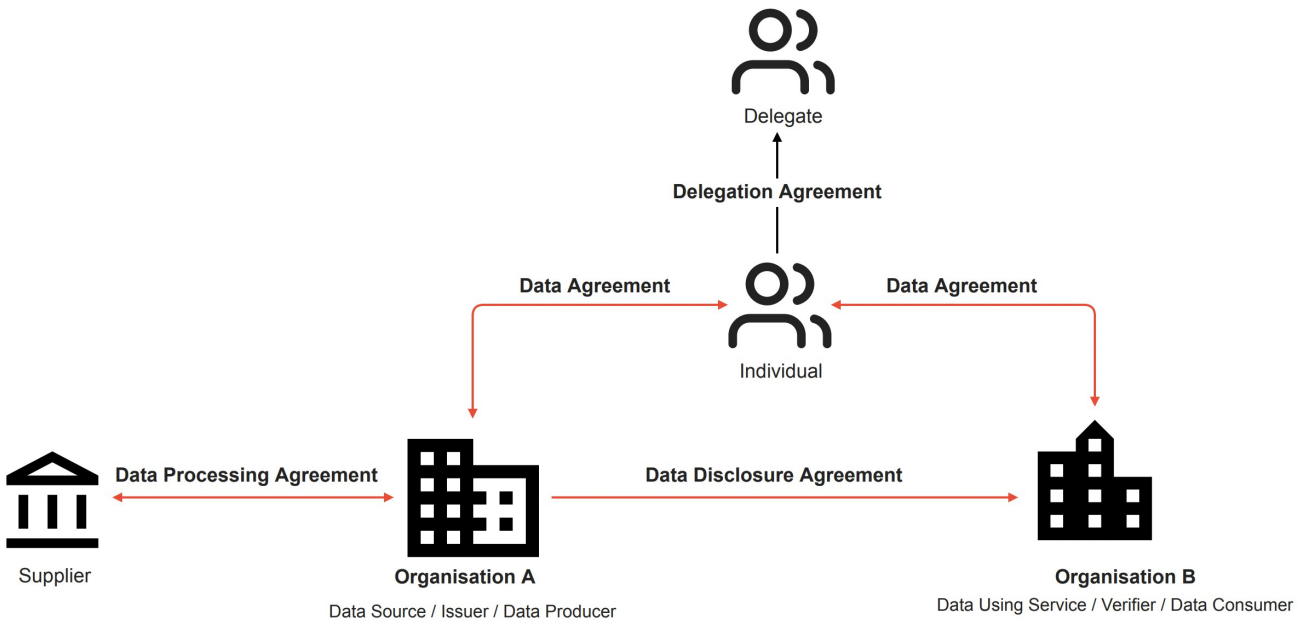

FIGURE 3.1: DATA EXCHANGE AGREEMENT LANDSPACE [4]

The Data Exchange Agreement (DEXA) [4] protocol suite enables automated agreement handling for data exchange between a Data Source (DS) and a Data Using Service (DUS). DEXA provides a human-centric and auditable approach to data transactions through cryptographically-signed data agreements between individuals and organisation(s) involved in data exchange. For organisations, it helps to be transparent and legitimate in their data usage while leveraging data in a scalable manner as part of a data ecosystem. Furthermore, the DEXA protocol brings in the requisite trust and governance to establish a ubiquitous data exchange space while empowering individuals to control their data.

3.2 Data Agreements

A *Data Agreement* (DA) is a construct between an organisation and an individual regarding the use and processing of personal data [2]. It records the conditions for an organisation to process personal data following the relevant data protection regulations, which could be data laws or norms such as the MyData principles. It can have any legal basis outlined by the applicable data protection regulation. The agreement can be with a data source (issuer) or a data-using service (verifier) or used for personal data exchange with third parties.

A data agreement gives a simple overview of the data usage for humans and machines alike that is enforced between the parties involved. A W3C-specified decentralised identifier (DID) implements the data agreement within DEXA [3]. Shown below is an example of a Data Agreement as part of a credential presentation:

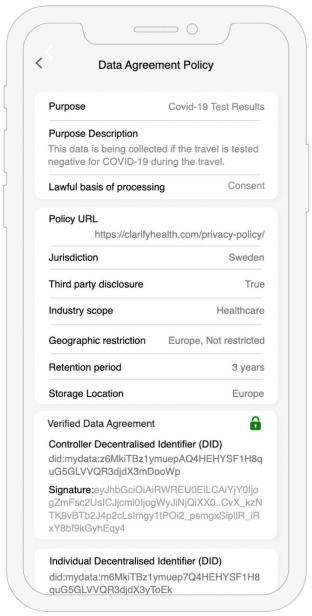

FIGURE 3.2: EXAMPLE DATA AGREEMENT FROM IGRANT.IO DATA WALLET [4]

Appendix C provides the DA ontology and reference [20] provides the demonstration of an implementation using iGrant.io Data Wallets.

3.3 Data Disclosure Agreements

A *Data Disclosure Agreement* (DDA), also referred to as Data Sharing Agreement, enables automated agreement handling for data exchange between a Data Source (DS) and Data Using Service (DUS). It helps organisations to continue leveraging their data assets while being transparent and legitimate in their data usage. Automated agreement handling is a requisite when establishing a scalable regulatory-compliant data space. It also provides individuals control over how their data is used and exchanged.

Appendix C provides the DDA ontology.

3.4 Data Processing Agreements

A *Data Processing Agreement* (DPA) is a construct between an organisation and its suppliers, as illustrated in figure 3.1. Here, there is a vertical relationship between Organisation A as a data controller and its supplier as a data processor or sub-processor. For a higher level of accountability between these organisations, and mandatory for the GDPR, a data processing agreement is set up, which lays out what routines are required to be in place; for example, a data processor's obligations in case of a data breach or how the rights of the individual, such as access rights, are supported, among other policies and routines. An auditor should also be able to inspect the organisation and use the data processing agreement as reference material during the inspection. As depicted in figure 3.1, the data processing agreement is connected to the individual at the top of the hierarchy via the data controller organisation.

3.5 Delegation Agreements

A delegation agreement describes scenarios in which a delegate acts on behalf of an individual in signing off a data exchange. There are several scenarios where delegation is necessary. For example, in the case of:

- guardianship when an individual is incapable of signing off due to infirmity, incapacity or illness; or
- an individual receives temporary rights to sign off on behalf of another individual: for example, purchasing medicine at a pharmacy or collecting a parcel from a post office.

3.6 The rationale for a multi-jurisdictions approach

Today, the governance of data exchanges is dependent on centralised platforms, limiting the impact of an end-user self-sovereign approach, as the transaction's regulatory compliance remains under the platform's control. Despite having the decentralised capacity to authenticate itself, the end-user remains trapped in a "cookie" style agreement over the overall relationship instead of receiving proof of compliance specific to a transaction.

To illustrate the limitation of the platform governance approach, we revisit a classic use case of a patient receiving a medical prescription and using it to receive the medication. The thorny problem lurking behind this use case differs from the authentication of the prescription holder. Instead, it introduces a *double-spend* problem. How the system ensures the medication is only sometimes requested.

The "*platform approach*" might be tempting within a single jurisdiction. Still, when real-world constraints are applied, it quickly becomes apparent that the mesh of agreements to be satisfied by a given transaction requires either re-centralisation of the whole process or simplification that strongly limits the applicability (and thus adoption) of the system. At a time when the concept of European-wide health data space is gaining traction, the problem needs urgent scrutiny to prevent wrong core architectures from being developed.

4. Context preservation — a Decentralised Semantic approach

See reference [7,8]

4.1 Semantics to the rescue

"Context preservation" is a common requirement lurking behind the challenges presented in sections 2 (VC presentation) and 3 (VC links to agreements).

In each challenge, the system must be aware of the context in which the user operates. Specifically, the issuer controlling the credentials related to the prescription has no control over its presentation on a patient's device. Moreover, the chosen scenario shows a use case where the issuer does not control the jurisdiction where the user will carry out its transactions. The challenge is to securely provide a deterministic digital item in contexts not known in advance.

A complete framework addressing these topics is the Dynamic Data Economy (DDE) [13] architecture based on the four domains of data management (Inputs, Semantics, Governance, Economy)

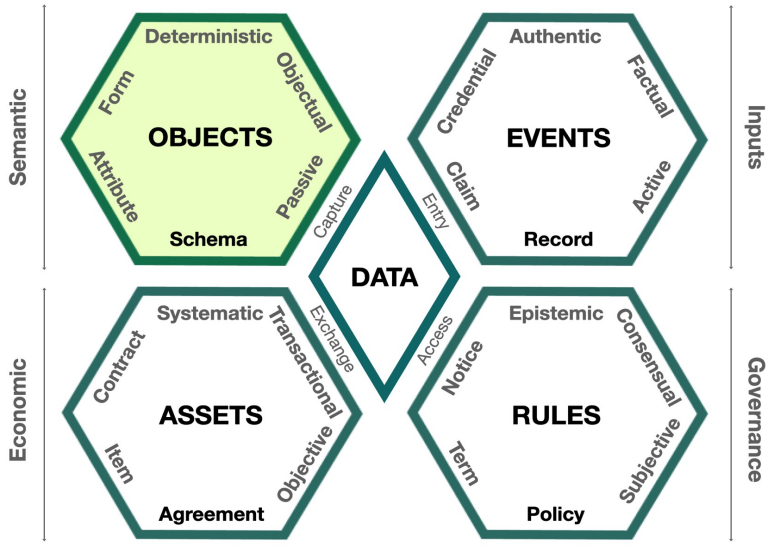

FIGURE 4.1: DYNAMIC DATA ECONOMY FOUR DOMAINS [13]

This paper shows how the semantic domain, layer 1 of the DDE technology stack, contributes to solutions through the Overlays Capture Architecture (OCA), a specific reference implementation of decentralised semantics [7] developed at the Human Colossus Foundation [13].

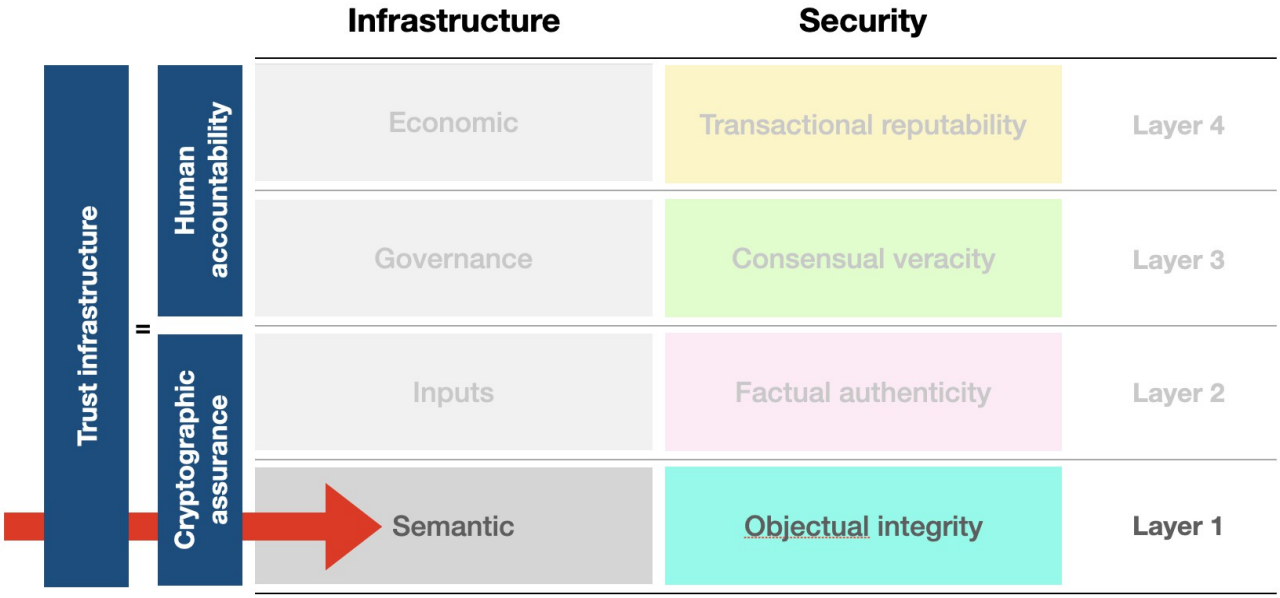

FIGURE 4.2: DYNAMIC DATA ECONOMY TECH. STACK [14]

The Overlays Capture Architecture (OCA) is an explicit representation of task-specific objects ("Overlays") that have deterministic relationships with other objects. These "Overlays" define individual semantic tasks, which, when combined, provide additional context to the object. An OCA bundle consists of a "Capture Base" and "Overlays". The sum of its parts represents a contextually-rich schema.

The segregation of overlays by task enables interoperability in the construction process of any digital object without compromising the integrity of the semantic structure, the encapsulated objects, or the relationship between those objects.

4.2 Health domain regulations

Internationalisation for presentations and documents in different languages is an apparent first application of OCA in multi-jurisdiction settings. However, this is the tip of the iceberg. Health care is a highly regulated domain. Any process must fulfil conformity requirements in the European Health Data Spaces [Ref], which drives the need for regulatory compliance and data provenance. For example, the testing requirements reference several standards bodies.

OCA is ontology-agnostic, offering a harmonisation solution between data models and data representation formats. OCA provides a roadmap to resolve privacy-compliant data sharing between servers and networks across sectoral or jurisdictional boundaries. Therefore, the layered architecture of OCA offers a bridging mechanism between different data standards used by various actors. For example, bridging a FHIR-profile to an OCA-resource for data capture facilitates interoperability with CDISC-profiles. The interplay between overlays and the unicity of composite bundles is an exciting field of research for processes dealing with a complex mesh of data exchange agreements.

4.3 OCA for inclusive representations of credentials

The specification of OCA rests on the concept of overlays. Therefore, here we add definitions of relevant overlays for the use case at hand:

Overlay Name	Description in prescription use case
Capture Base	A stable base object that defines a single dataset in its purest form, providing a structural base to harmonise data.
Meta Overlay	An overlay that defines any language-specific information about a schema.
Character Encoding Overlay	An overlay that defines the process of assigning numbers to graphical characters, especially the written characters of human language, allowing them to be stored, transmitted, and transformed using digital computers.
Format Overlay	An overlay that defines an input and display format for data fields.
Information Overlay	An overlay that defines attribute field descriptions and usage notes to assist the data entry process or to add context to presented data.
Label Overlay	An overlay that defines attribute and category labels.

The OCA specification v1.0 can be found on in reference [17] together with additional documentation and code examples. In addition, for sake of completeness, we provide a short version of the OCA specification at the time of the RWOT11 conference as an appendix.

5. Conclusions

"*Naked VCs do not scale; they must be dressed!*" could be the punch-line conclusion of this work. However, we point to something more profound. In part of the text, we use the terminology of "verifiable information" instead of "verifiable credential". This distinction underlines that, often, it is the purpose and the authenticity of information that drives user interaction. The trust relationship between the two parties of a transaction can emerge from a digital system only if the presentation of the information in the users' context and the liability of each interacting party is secured and expressed in a simple form. Fredrik and the Swiss pharmacist each rely upon their own digital systems that must provide an assurance level matching the potential risk of a transaction.

The challenges we presented, credential presentation, data exchange agreements, accessibility, and international requirements all point in the same direction. For verifiable credentials to be used in a broad ecosystem will require a strong link (in the cryptographic sense) to other data objects.

We provided a view of the current state-of-the-art and a constructive approach to address these challenges using the existing DEXA and OCA protocols.

Our approach is a Self-Sovereign not because of an SSI technology but because the user (e.g. Fredrik, Pharmacist) is the holder and driver of the contextual use of verifiable information. Specifically, this means:

1. the user is the carrier of trust across ecosystems (see EU Horizon 2020 projects eSSIF-Lab DKMS-4-SSI [17] , eSSIF-Lab Dynamic Data Sharing Engine [16], DAPSI Digital Immunization Passport [15]);
2. the organisations partake in cross-border data exchange in a scalable, regulatory-compliant, and auditable manner.

Those stakeholders will find data interactions through user-centric data agreements exciting. However, the most compelling factor is the interoperability requirements defined by HIE and EHDS concerning jurisdictional and sectoral regulations. Rather than a secondary process to meet inclusivity compliance requirements, this steers consideration of up-front accessibility requirements as key to enabling interoperability at scale.

The challenges addressed in this paper have a primary interest for any organisation currently involved in the digital transformation of citizen-centric processes, particularly for the healthcare sector with large-scale initiatives like the EU Health Data Space or the US-HIE (Health Information Exchange). It shows that the concept of Self-Sovereign Identity, as

developed until now, must and can consider the societal landscape. The risks of not doing so emerged in numerous discussions at this RWOT11 conference and others attended by some of the authors (i.e. the Cancer Drug Development Forum workshop on patient right of equity to access treatments [18] or DPO Associates' Master Class "Cloud or Not-Cloud"[19]).

6. Acknowledgements

We thank the participants and organisers of RWOT11 for providing the space for insights full discussions.

7. References

[1] European Union e-Health network, e-prescriptions and eIDAS integrated vision: https://health.ec.europa.eu/latest-updates/eprescription-eidas-integrated-vision-2022-08-01_en (Last accessed: 08-Oct-2022)

[2] Automated Data Agreement specification, available at: https://github.com/decentralised-dataexchange/automated-data-agreements/blob/main/docs/data-agreement-specification.md (Last accessed: 08-Oct-2022)

[3] DID Data Agreement WG: https://github.com/decentralized-identity/data-agreement (Last accessed: 08-Oct-2022)

[4] iGrant.io whitepaper: Data Exchange Agreements - Removing the barriers to consent-based, auditable and immutable data transactions: https://igrant.io/papers/iGrant.io_DataExchangeAgreements_v2.0.pdf (Last accessed: 18-Nov-2022)

[5] Reference relevant technical standards e.g. WCAG for HTML and javascript content (Last accessed: 12-Oct-2022)

[6] European digital accessibility standard for public sector organisations (EN 301 549), US Section 508 requirements for Federal Agencies

[7] Overlays Capture Architectures (OCA) specifications, https://oca.colossi.network/v1.1.0-rc.html (Last accessed: 11-Nov-2022)

[8] "OCA transformation layer", The Official OCA website, last accessed November 1st

[9] DIF Wallet Rendering Specification (draft): https://identity.foundation/wallet-rendering/

[10] An AnonCreds OCA Architecture, https://docs.google.com/presentation/d/1Ps7OPrcQBSem6ygSLSYoYq3HfpNevNYYy5e2ziGjsqU/edit#slide=id.p (Last accessed: 11-Nov-2022)

[11] DIF Credential Manifest Specification 0.0.1 https://identity.foundation/credential-manifest/

[12] Open Badges Specification https://1edtech.github.io/openbadges-specification/ob_v3p0.html

[13] "Dynamic Data Economy Principles", Human Colossus website, last accessed on November 1st 2022

[14] "Humancolossus Trust Infrastructure Stack V1.0", The Human Colossus Foundation website

[15] EU Horizon 2020 -New Generation Internet DAPSI "Digital Immunization Passport" grant agreement 871498 https://dapsi.ngi.eu/hall-of-fame/dip/

[16] EU Horizon 2020 -New Generation Internet sSSIF-Lab Business Oriented Call#1 "Dynamic Data Sharing Hub" grant agreement 871932 https://essif-lab.eu/dynamic-data-sharing-hub-with-consent-flow-by-the-human-colossus-foundat ion/

[17] EU Horizon 2020 -New Generation Internet sSSIF-Lab Infrastructure Oriented Call#3 "DKMS-4-SSI" grant agreement 871932 https://essif-lab.eu/decentralized-key-management-infrastructure-for-ssi-by-the-human-colossus -foundation/

[18] HCF: "A distributed governance approach" in CDDF workshop *Leveraging the potential of precision medicine: Ensuring equity of access to precision diagnostics and treatments for patients*, Amsterdam, Netherlands November 15th 2022

[19] HCF: "Cloud or *not* Cloud", DPO Associate's Master Class, Lausanne, Switzerland November 24th 2022

[20] Data wallet with data agreements for consent-based auditable and immutable data transactions, https://www.youtube.com/watch?v=lx8F5D9qPQI (Last accessed: 11-Dec-2022)

Appendix A: Use case — Using a medical prescription in a different country

A typical cross-border data exchange scenario is well laid out in the European Union e-Health network, e-prescriptions, and eIDAS integrated vision [1] and is as reiterated below:

1. A Patient receives a prescription from an authorised Prescriber in Country A. The Wallet of the Patient [or their authorised Representative] receives a prescription notification.

   The Wallet connects to the ePrescription service in Country A, which displays ePrescriptions (as per pre-requisites).

2. The Patient [or their Representative] from Country A visits a pharmacy in Country B to get the medicine(s) prescribed in Country A.

3. (optional) The Patient [or their Representative] identifies themself to the Pharmacist at the Pharmacy.

   The case of representation (by an authorised third party, e.g., a Next of Kin) needs to be covered.

   The wallet provides user identification (also: representation).

4. The health professional (Pharmacist) informs the Patient [or their Representative] about their data protection rights and asks for the Patient's consent (where applicable).

   Option A Prescription list. The Patient [or their Representative] presents a QR code containing the following:

   - Member State code
   - Set of the prescription holder's identifiers.
   - Set of the wallet holder's identifiers (if different from the prescription holder).
   - Timestamp and digital signature.

   The Wallet generates a QR code containing identifiers and instructions to fetch the prescription list.

   The Wallet could show a prescription list to the Patient.

   Option B Specific prescription. The Patient [or their Representative] presents a QR code containing the following:

   - Member State code
   - Set of prescription holder's identifiers
   - Set of the wallet holder identifiers (if different from the prescription holder)
   - Prescription ID, dispensation PIN or other similar details
   - ATC code of the prescription, IDMP attributes (such as EDQM dose form), prescribed amount or other critical data
   - Timestamp and digital signature

   The Wallet generates a QR code containing identifiers and instructions on how to fetch a specific prescription, including limited prescription details (for offline use in exceptional circumstances).

5. The dispensation provider (Pharmacy) scans the QR code, verifies the digital signature and generates a request to send to country A based on the information provided.

6. **Option A** Default option [Typical steps following the MyHealth@EU workflow leading to possible dispensation]

   Option B Exceptional situations (internet disruption or other similar use cases)

   In case of disruption or other exceptional circumstance that prevents communication via MyHealth@EU, the Dispenser evaluates the possibility of dispensing medicine based on the information included in the QR code (If supported by both Country A and Country B).

   The pharmacy system will store the data if the Dispenser can perform dispensation. Upon restoring connectivity, follow the steps for the Default option, 6A.

7. The pharmacist system reads the electronic Product Information (ePI) and correlates it to the Patient's IPS (https://international-patient-summary.net/). The Pharmacy has two competitive brands available in-store rather than the prescribed Brand Medicine. However, the system can provide notifications based on the ePI information, Electronic Product Information (http://build.fhir.org/ig/HL7/vulcan-eproduct-info/toc.html). The Pharmacist receives visual notification, and due to chosen accessibility features on their phone, the Patient receives verbal notification that one of the two drugs contains a chemical substance that the Patient is allergic/sensitive to, so they need to agree on which medicine to dispense.

8. The Dispenser provides the drug to the Patient.

   In the case of 6B, the Dispenser manually invalidates the prescription in the Wallet app.

9. The Wallet receives an updated prescription status from Country A with the invalidated or updated (in the case of a partial dispense) dispensed prescription.

   A push notification provides an updated prescription status in the Wallet.

10. Termination of the workflow. No more access to the Patient's data from Country A is possible.

Appendix B: Overview of OCA Overlays

For completeness, we present additional information on OCA valid at the time of RWOT11 event participation.

The OCA specification is maintained at the Human Colossus Foundation and can be accessed here [17]. Readers can find more information about OCA on the official OCA website.

The following OCA features support the inclusive representation of credentials:

Capture Base

A list of attributes in the schema for credential type. The attribute adheres to types defined in the OCA specification. The list of Flagged Attributes that contain identifying information. The flagged attribute list marks elements to protect against unwarranted disclosure at the application level. Without holder intervention, the flagged attribute list can guide wallets on which sensitive information not to render immediately.

Meta Overlay

Defines localised meta-information about the credential in a given language.

Character Encoding Overlay

Defines the encoding used for each attribute for correct display at the application level.

Format Overlay

Defines the localised display format of the data in a given language or preference setting. For example, date-time formatting in a calendar application.

Label Overlay

Defines the label for each attribute in a given language. Assistive Technologies (AT) can use this label to describe data consistently.

Information Overlay

Defines attribute field descriptions and usage notes. Assistive Technologies (AT) can use this information to assist the data entry process or to add context to presented data.

We also propose additions to the OCA architecture to support improved usability and accessibility of data represented at the application layer.

Asset Overlay

Defines assets for describing attributes visually, such as logos and icons. For example, visually describing data with icons within the health domain can support health professionals in parsing data, reducing cognitive burden.

```
{
  "capture_base": "EPMaG1h2hVxKCZ5_3KoNNwgAyd4Eq8zrxK3xgaaRsz2M",
  "type": "spec/overlays/assets/1.0",
  "issuedBy": "../IssuerLogo.svg",
  "dateOfBirth": "../vectorIcons/calendar.svg"
}
```

Presentation Overlay

Defines the representation of the data object at the application layer, supporting accessibility concerns and providing issuer-defined aesthetic attributes. We propose changing the existing ‘Layout Overlay’ to express representation definitions as key-value pairs that any application layer codebase may interpret.

```
{
  "capture_base": "EPMaG1h2hVxKCZ5_3KoNNwgAyd4Eq8zrxK3xgaaRsz2M",
  "type": "spec/overlays/credential_representation/1.0",
    "primary_colour": "rgba(0,0,0,1)",
    "secondary_colour": "rgba(255,255,255,1)",
    "background-image": "../backgroundImage.svg",
    "minimum-contrast-ratio": "4.5:1",
    "voice": "en-US-JennyNeural", //SSML voice support
    "maximum-line-length": "70", //characters for readability
    "hyphenation": "none", //supports readability
    "primary_attribute": "fullName", //defines ordering of attributes, could
alternatively be an ordered array
    "secondary_attribute": "dateofBirth",
}
```

Data-Representation Overlay

Defines the representation of individual attributes at the application layer so that data providers can define attribute-specific representation behaviours. For example, verifiable presentations may use these definitions to draw on attributes from multiple credentials.

```
{
  "capture_base": "EPMaG1h2hVxKCZ5_3KoNNwgAyd4Eq8zrxK3xgaaRsz2M",
  "type": "spec/overlays/data_representations/1.0",
  "photoImage": {
        "aspect_ratio": "3:4",
        "color_space": "RGB"
        },
    "dateofBirth": {
        "color": "rgba(255,0,0,1)"
        }
    "documentType": {
        "backgroundImage": "./animatedGenerativePattern.svg"
    }
}
```

Appendix C: Data Exchange Agreement Ontologies

Data Agreement ontology

The latest data agreement ontology is provided below [2].

Attribute Name	Description
@context	The context of this document. E.g. the link, the JSON-LD
id	Identifier to the data agreement instance addressed to a specific individual (Data Subject)
version	Version number of the data agreement
template_id	Identifier to the template of the data agreement
template_version	Version number of the data agreement template
language	The language used. If not present, default language is English
data_controller_name	The name of the data controller processing the data
data_controller_url	The controller URL
data_controller_legal_id	The legal ID to the data controller. E.g. Swedish org. number
data_policy	Encapsulation of the data policies used for the use of personal data.
- policy_URL	URL to the privacy policy document of the data controller organisation
- jurisdiction	The jurisdiction associated with the organisation processing personal data that the privacy regulation is followed. This can be a country, economic union, law, location or region. [value based on W3C Location and Jurisdiction]
- industry_sector	The sector to which the data controller belongs to
- data_retention_period	The amount of time that an organization holds onto any personal data, in days (per purpose)
- geographic_restriction	Restriction on the country or economic union for processing personal data [value based on W3C Location and Jurisdiction]
- storage_location	The geographic location where the personal data is stored
- third_party_disclosure	A boolean value to indicate that the DA is used for third party data disclosures. This indicates that some data disclosures will happen and is used to release personal data to DUS based on an agreement
purpose	The purpose for which a data controller (DSor DUS) uses personal data. This is the purpose for which the data agreement is being formulated. [values based on W3C DPV Purposes]
purpose_description	A description of the purpose for which the personal data is used
lawful_basis	The lawful basis for processing personal information. This can be based on consent, legal obligation, contract, vital interest, public task or legitimate_interest. [values based on W3C DPV legal basis]
method_of_use	Type of processing of personal data [value based on W3C DPV Processing]
personal_data []	Encapsulation of the attributes used for the usage purpose defined
- attribute_id	Identity of the attribute that is being processed
- attribute_name	Name of the attributes that is being processed
- attribute_sensitive	[OPTIONAL] Definition of the sensitivity of the data as per PII (Personal Identifiable Information)

- attribute_category	An explicit list of personal data categories to be processed for the specified purpose. The categories shall be defined using language meaningful to the users and consistent with the purposes of processing. [values based on W3C DPV-DP]
- restrictions []	[OPTIONAL] Restriction on where the data is being consumed
– schema_ID	[OPTIONAL] Restriction on data from this personal data schema issued by a legal entity
– credential_def_ID	[OPTIONAL] Restriction on data from this credential schema from an organisation
dpia	Encapsulation of the organisation performing the Data Protection Impact Assessment (DPIA)
- dpia_date	The data when the latest DPIA was carried out
- dpia_summary_url	The URL to the DPIA summary information
code_of_conduct	The data controller may follow a code of conduct which sets the proper application of privacy regulation, taking into account specific features within a sector. The code of conduct shall reference the name of the code of conduct and provide a public accessible reference.
event []	Encapsulation of the data agreement lifecyle event data. For e.g. Data Agreement Offer, Accept, Reject, Terminate etc.
- id	Event identifier
- time-stamp	Event timestamp (ISO 8601 UTC)
- did	The DID associated with the entity executing the event. E.g. An organisation (Data Controller) or an Individual (Data Subject)
- state	The current state of the event during a data agreement lifecycle. E.g. Offer, Accept, Reject and Terminate
proof []	Encapsulation of the event signatures that allows anyone (e.g. an auditor) to verify the authenticity and source of the data agreement. It uses linked data proofs as per W3C and contains a set of attributes that represent a Linked Data digital proof and the parameters required to verify it
- id	Proof identifier
- type	Signature schema type (For e.g. ed25519, es256 e.t.c.)
- created	Creation time of the proof (ISO 8601 UTC)
- verificationMethod	Should match the data_using_service DID
- proofPurpose	Purpose of the proof
- proofValue	Proof value
data_subject_did	The DID of the data subject signing the agreement
revocation_list	Link to the storage location of the revocation list for the agreement
data_expiry	Expiry for the agreement (in epoch time)

Data Disclosure Agreement ontology

Attribute Name	Mandatory	Description
@context	TRUE	The context of this document. E.g. the link, the JSON-LD
id	TRUE	Identifier to the data disclosure agreement instance addressed to a specific DUS
version	TRUE	Version number of the data disclosure agreement
template_id	TRUE	Identifier to the DDA offer
template_version	TRUE	Version number of the DDA offer
language	TRUE	Language used. If not present, default language is English
data_controller	TRUE	Encapsulation of the data controller data
- did	TRUE	The DID of the data source preparing the agreement
- name	TRUE	The name of the data source exposing the data
- legal_id	TRUE	The legal ID to the data source. E.g. Swedish Organisation Number
- url	TRUE	The data source organisation URL
- industry_sector	TRUE	Industry sector that the DS belongs to
agreement_period	TRUE	Duration of the agreement after which the data disclosure agreement expires
data_sharing_restrictions	TRUE	Used by the DS to configure any data sharing restrictions towards the DUS. This could reuse the data agreement policy parameters as is.
- policy_URL	TRUE	URL to the privacy policy document of the DS
- jurisdiction	TRUE	The jurisdiction associated with the data source exposing the personal data whose privacy regulation is followed. These can be country, economic union, law, location or region. [value based on W3C Location and Jurisdiction]
- industry_sector	FALSE	The sector to which the data source restricts the use of data by any data using services. If no restriction, leave blank
- data_retention_period	TRUE	The amount of time that the data source holds onto any personal data, in days.
- geographic_restriction	FALSE	Restriction on the country or economic union for processing personal data. [value based on W3C Location and Jurisdiction] for the data source
- storage_location	FALSE	The geographic location where the personal data is stored by the data source
purpose	TRUE	The purpose for which the data source shares personal data as described in the data agreement [values based on W3C DPV Purposes]
purpose_description	TRUE	Additional description of the purpose for which the data source shares personal data
lawful_basis	TRUE	The lawful basis for sharing personal data. These can be consent, legal obligation, contract, vital interest, public task, or legitimate_interest. [values based on W3C DPV legal basis]
personal_data []	TRUE	Encapsulation of the attributes shared by the data source
- attribute_id	TRUE	Identity of the attribute that is being shared
- attribute_name	TRUE	Name of the attributes that is being shared
- attribute_sensitive	FALSE	The sensitivity of the data as per PII

- attribute_category	FALSE	An explicit list of personal data categories to be shared. The categories shall be defined using language meaningful to the users and consistent with the purposes of the processing. [values based on W3C DPV-DP]
code_of_conduct	FALSE	The code of conduct is followed by the data source. This provides the proper application of privacy regulation taking into account specific features within a sector. The code of conduct shall reference the name of the code of conduct and provide a publicly accessible reference.
data_using_service	TRUE	The data using services that have signed up for consuming data. This get populated after the data disclosure agreement is proposed by the data using service
- did	TRUE	The DID of the data using service signing the agreement
- name	TRUE	Name of the DUS signing the agreement
- legal_id	TRUE	The legal ID of the data using service
- url	TRUE	The data using service organisation URL
- industry_sector	TRUE	Industry sector that the DUS belongs to
- usage_purposes	TRUE	The purpose for which the data is being used by the DUS
- jurisdiction	TRUE	The jurisdiction associated with the data using service consuming personal data whose privacy regulation is followed. These can be country, economic union, law, location or region. [value based on W3C Location and Jurisdiction]
- withdrawal	FALSE	Reference to how data subject may withdraw
- privacy rights	FALSE	Reference to information on how to exercise privacy rights (ex. erasure, objection, withdrawal, copy)
- signature_contact	FALSE	The responsible entity or person in the organisation signing the data disclosure agreement
event []	TRUE	Encapsulation of the data disclosure agreement lifecycle event data. For e.g. data disclosure agreement Offer, Accept, Reject, Terminate etc.
- id	TRUE	Event identifier
- time-stamp	TRUE	Event timestamp (ISO 8601 UTC)
- did	TRUE	Should match the data_using_service DID
- state	TRUE	The various available states are: offer/accept/reject/terminate/fetch-data
proof []	TRUE	
- id	TRUE	Proof identifier
- type	TRUE	Signature schema type (For e.g. ed25519, es256 e.t.c.)
- created	TRUE	Proof creation time (ISO 8601 UTC)
- verificationMethod	TRUE	Should match the data_using_service did
- proofPurpose	TRUE	Contract agreement (Type inferred from JSON-LD spec)
- proofValue	TRUE	Proof value

Additional Credits

Lead Author: Dr. Philippe Page [PP] (Human Colossus Foundation, Switzerland)

Authors: Mr. Lal Chandran [LC] (iGrant.io, Sweden), Ms. Lotta Lundin [LL] (iGrant.io, Sweden), Mr. Fredrik Lindén [FL] (MyData, Sweden), Dr. Philippe Page [PP] (Human Colossus Foundation, Switzerland), Mr. Paul Knowles [PK] (Human Colossus Foundation, Switzerland), Mr. Víctor Martínez Jurado [VM] (SICPA, Switzerland), Mr. Andrew Slack [AS] (SICPA, Switzerland)

Contributors: Mr. Jan Linquist (Linaltec, Sweden), Mr. Max Carlson (Govstack Initiative), Mr. George Padayatti (iGrant.io, Sweden,) Dr. David Goodman (iGrant.io, Sweden)

Sample APA Citation

Chandran, L., Lundin, L., Lindén, F. Page, P., Knowles, P., Jurado, M., and Slack, A. (2022). Linking Credentials with Data Exchange Agreements through Secured Inclusive Interfaces. Rebooting the Web of Trust XI. Retrieved from https://github.com/WebOfTrustInfo/rwot11-the-hague/blob/master/final-documents/data-exchange-agreements-with-oca.pdf.

About Rebooting the Web of Trust

This paper was produced as part of the Rebooting the Web of Trust XI design workshop. On September 26th to 30th, 2022, over 60 tech visionaries came together in The Hague, The Netherlands to talk about the future of decentralized trust on the internet with the goal of writing at least 5 white papers and specs. This is one of them.

• **RWOT Board of Directors:** Christopher Allen, Joe Andrieu, Erica Connell.

• **RWOT11 Coordination Team:** Will Abramson, Christopher Allen, Joe Andrieu, Shannon Appelcline, Erica Connell, Eric Schuh, Carsten Stöcker.

• **Workshop Credits:** Will Abramson (Producer), Christopher Allen (Founder), Shannon Appelcline (Editor-in-Chief), Erica Connell (Host), Amy Guy (Ombudsperson), Willemijn Lambert (Graphic Recorder), Eric Schuh (Ombudsperson), Carsten Stöcker (Co-Producer, Demo Organizer), Dorothy Zablah (Facilitator).

• **Gold Sponsors:** The City of the Hague, Digital Contract Design, Dutch Blockchain Coalition, The Hague University of Applied Sciences, eSSIF-Lab.

• **Contributing Sponsors:** Blockchain Commons, Legendary Requirements, Spherity.

Thanks to all our attendees and other contributors!

What's Next?

The design workshop and this paper are just starting points for Rebooting the Web of Trust. If you have any comments, thoughts, or expansions on this paper, please post them to our GitHub issues page:

https://github.com/WebOfTrustInfo/rwot11/issues

The twelfth Rebooting the Web of Trust design workshop is scheduled for late 2022. If you'd like to be involved or would like to help sponsor the event, email: Leadership@WebOfTrust.info