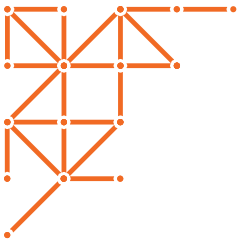
Indicio

Trust, Verifiable Credentials, and Interoperability

Trevor Butterworth & Sam Curren



What does it mean to have a digital identity? The internet and the web evolved with effective ways to identify computers and websites but less so the people using them.

Introduction

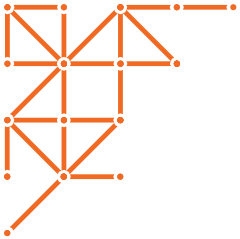
Life online would be impossible without interoperability. Without TCP/IP (Transmission Control Protocol/Internet Protocol), a shared set of standards and rules allowing computers to communicate with each other, there would be no internet. Without HTML—Hypertext Markup Language—there would be no World Wide Web. And, as you read this—almost certainly in HTML on the WWW through TCP/IP—a new set of protocols are being built and adopted which aim to create interoperability around new technologies for digital Identity, data sharing, verification, and trust.

What does it mean to have a digital identity? The internet and the web evolved with effective ways to identify computers and websites but less so the people using them. Arguably, email addresses became the first way to establish human identity. They are the key building block for creating and accessing user accounts, often as login credentials, in tandem with passwords.

Whether as an email address leased from an email provider, or as a user account brokered by an email account, these digital identities are not owned by us. They can be revoked. Because they are easy to create, they often require additional personal information to be verifiable.

All this real-world and virtual data is stored by the "identity leasing agencies"—the myriad companies and services we use online through email and user accounts. This includes the metadata we generate by being online, which is aggregated, packaged, and sold on to other parties for undisclosed purposes, but which frequently include marketing and advertising. We must give prior consent to our data being used in this way in order to lease our digital identities.

While all of this is presented as either mostly benign or mildly annoying, and unavoidable—a trade-off for the plenitude of goods and efficiencies online—the system is



designed to fail. Emails are easy to find or guess. Passwords, if easy to remember, are easy to hack. People are easily "phished"into giving up personally-identifying information that can be used to replicate their identity online.

Identity fraud is endemic to this system. Data breaches are frequent and expensive, a combination of the cost of lost data, the cost of being fined for losing the data, the cost of meeting increasingly stringent data privacy mandates, the cost of implementing better security, and the reputational cost of lost trust from losing all your customer data.

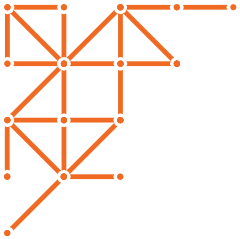
In this system of centralized databases, each identity can be a single point of failure for the entire system. Federated identity, once thought of as a solution, replicates the underlying problem with higher stakes: if something goes wrong, you lose access to everything tied to your digital identity.

New, decentralized identity technologies mean that we can completely overhaul this system. We can establish digital uniqueness independent of any third party. We can generate the kind of verification that enables trust without storing personal information on third-party databases.

Verifiable credentials provide the authentication needed to establish trust in each other and in the data we need to share. They mitigate the compliance burden; they make digital life simpler. Imagine being able to log into any site or service by scanning a QR code. Imagine a world where you can forget your passwords…forever. With the bureaucracy of verification removed and the barrier to trust lifted, the transformation of the digital economy through trusted digital ecosystems can begin.

But only if verifiable credentials are interoperable.

With the bureaucracy of verification removed and the barrier to trust lifted, the transformation of the digital economy through trusted digital ecosystems can begin.



Nobody, in theory, dislikes interoperability.

The good news is that interoperability is the mantra of those bearing verifiable digital credentials. Everyone understands that interoperability is the way to organically scale this massively beneficial technology. Everyone building decentralized solutions knows that their customers see interoperability as fundamental to these solutions' value proposition. Verifiable digital credentials must be seen by their users as being valuable—and they will be valuable if they can be used for lots of different and important purposes.

The bad news is that claiming to be interoperable is far easier than making actual systems interoperate. This gap between rhetoric and reality needs to be closed—and urgently. This requires clarification of the problem, action from the community, and the encouragement of informed consumers.

The goal of this paper is to help all three.

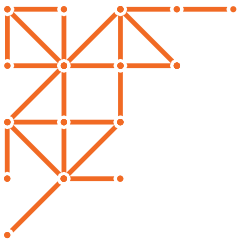
Our first task is to describe the current state of interoperability in a way that is fair to all participants.

The second is to map a path to interoperability through clarifying alignments between components and standards and by positing a systematic way of qualifying and checking for alignment.

We hope this paper encourages debate, and we welcome community efforts to build on and expand the ideas contained herein.

Key Points

1. **There are seven aspects of interoperability for verifiable credentials.**
2. **All seven aspects of interoperability must be compatible for two solutions to be functionally compatible.**
3. **Vendors must clearly articulate all aspects of interoperability for their solution.**
4. **Customers can assess interoperability by evaluating how vendor solutions perform on these aspects.**
5. **Interoperability profiles will serve an important role in providing a fixed target for development and testing.**
6. **Interoperability testing will make true interoperability evaluations much simpler as these testing tools are developed and improved.**



The scope of interoperability will likely change over time. Convergence in one area can effectively eliminate its potential for incompatibility, while new technology may introduce new areas of incompatibility.

Seven aspects of interoperability

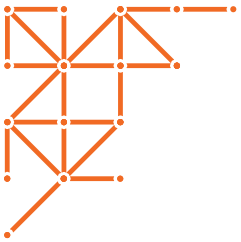
All systems are the result of design and technical choices. In designing for interoperability, the following technical aspects of a decentralized identity system must align.

Note that some elements in this list (DID methods, some credential formats, etc.) require dependent infrastructure such as a ledger or web-hosted assets. Each element of dependent infrastructure in an interaction must be accessible and acceptable to each party.

The scope of interoperability will likely change over time: Convergence in one area can effectively eliminate its potential for incompatibility, while new technology may introduce new areas of incompatibility. Consider this list as a snapshot in time, subject to adjustment as circumstances require.

1. DID methods

The fully interoperable stack must be able to resolve the DIDs used by all involved parties. With the number of DID methods available, this is no small feat. The Universal Resolver can solve some of this problem, but only with careful management to avoid relying on the trust of an externally managed system. To trust the results of any given Universal Resolver resolution, one must trust that the code operates properly. To trust the results of a Universal Resolver run by another party, you must trust the other party to have both sufficient security to prevent outside manipulation and to not manipulate the results themselves. This trust is possible but it is not automatic.



2. Content encryption key types

Information between parties is usually encrypted; therefore, each party must use compatible encryption keys and a compatible encryption scheme to allow decryption by the other party. Encryption at this level is used to encrypt protocol messaging and credential communication back and forth between parties.

3. Communication protocols

The methods of communication used between issuers, holders, and verifiers must be common between the parties in any given interaction. Different protocols can be used in each exchange as appropriate, but the combination of protocols must form a continuous chain of communication extending to all parties. Examples of these protocols are CHAPI, OpenID Connect, and DIDComm.

4. Credential format and signature types

The credential format used must be acceptable to all parties. Credential formats include JSON-LD (as depicted in the W3C verifiable credential data model specification), and JSON-based formats including JWT and AnonCreds. Credentials must also use signature types acceptable to all parties. Signature types include CL-signatures, BBS+, and Linked Data Signatures. Credential revocation methods must also be understood and testable by all parties.

5. Credential access / storage (wallet)

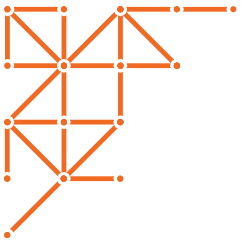
This may or may not be an issue, depending on how credentials are transferred from one party to another. If transferred directly to and from storage and not via another protocol, the data access needs to be compatible.

6. Credential protocols and coordination formats

The parties involved in exchanging credentials must communicate with each other about the credential. This includes communicating about the type and content of the credential before it is transferred. Even with identical credential formats, these protocols must be compatible to enable a transaction. Examples of these protocols and formats are the Aries Issue Credential and Present Proof protocols, The W3C Verifiable Presentation Request Specification, and the DIF Credential Manifest and Presentation Exchange formats.

7. Compatible governance / trust

With digital credentials, the issue of trust is critical but often ignored. Which issuer is the verifier willing to trust? This answer is solved through governance, machine-readable governance, and trust registries.



Converging on full-stack interoperability is not impossible: If we name the problems, we can develop the solutions.

The Vendor challenge: Labeling and mislabeling interoperability

Unfortunately, interoperability problems are everywhere and no-one is labeling in a way to guide enterprises and organizations seeking implementations.

It is not sufficient to claim interoperability with a single aspect—such as W3C credential format—and leave it at that. This kind of claim will lead to customer confusion and frustration. Whether misleading claims are intentional, due to sunk investments, or simply inadvertent, misleading claims about interoperability end up hurting the entire marketplace for decentralized identity.

Simply put, we need accurate labeling. This means that all claims about a solution being interoperable must be qualified by explaining what, exactly, it will interoperate with. In doing this, we are simply being fair with our customers; but we are also reminding ourselves to build to the goal we claim to believe in.

There are many community-driven ways this can be achieved. Groups such as the Decentralized Identity Foundation, Hyperledger Aries, and the Trust over IP Foundation can establish specific interoperability profiles. These will not only serve as a focus for development, they will serve as specific labels for identifying interoperable products and projects.

Converging on full-stack interoperability is not impossible: If we name the problems, we can develop the solutions. But as with everything worthwhile, it's going to require effort, and it's going to take community leadership to drive this effort.

Proposed Label

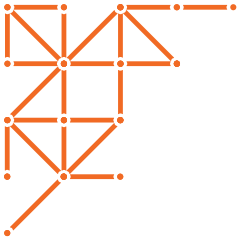
We propose a label in the following format. For products for which an item does not apply, it may be left blank or removed from the label. This label can be located within the product, on an associated website, shared with others during interoperability efforts, and any combination of these methods.

Enumerating the aspects of interoperability in the following manner makes it easier for customers to compare products. They can verify interoperability by identifying common choices—and they can articulate their needs in a way that helps technology providers. There is, perhaps, no better incentive to close the gaps between products by identifying them to consumers.

In the following draft label, we see Interoperability profiles as providing the fastest way to identify common capabilities, while individually enumerated support delineates the specifics necessary for a more detailed comparison.

Product Name	
DID Methods	
Content encryption key types	
Communication protocols	
Credential format and signature types	
Credential access / storage (wallet)	
Credential protocols and coordination formats	
Compatible governance / trust	
Interoperability Profiles	

Customers can articulate their needs in a way that helps technology providers. There is, perhaps, no better incentive to close the gaps between products by identifying them to consumers.

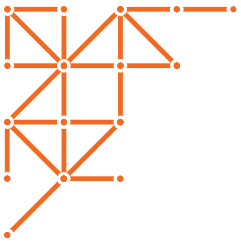


Examples

Consider the two fictitious products below. They overlap in some areas and have no overlap in others.

Example Product A	
DID Methods	did:peer, did:sov
Content encryption key types	ed25519
Communication protocols	DIDComm
Credential format and signature types	AnonCreds, JSON-LD BBS+
Credential access / storage (wallet)	
Credential protocols and coordination formats	Issue Credential v2.1, Present Proof v2, Credential Manifest
Compatible governance / trust	Social Identifiers
Interoperability Profiles	
WACI-Pex AIP 1.0 AIP 2.0	

Example Product B	
DID Methods	did:peer, did:ion, did:btc
Content encryption key types	ed25519, secp256k1
Communication protocols	VC-HTTP-API
Credential format and signature types	JSON-LD BBS+
Credential access / storage (wallet)	Universal Wallet API
Credential protocols and coordination formats	Credential Manifest
Compatible governance / trust	
Interoperability Profiles	
Sample Interop Profile 1.2	



Conclusion and recommendations for community action

Accurate labeling is, we believe, an important, achievable first step toward interoperability; but, it is not a complete solution. We must use interoperability profiles to fix development goals and then develop the necessary interoperability testing to provide the evidence consumers need.

As more attention is paid to protocols, credentials, and the rest of the stack, adjustments to labeling will, of course, be needed to accommodate innovation, new technology options, and community convergence. But the fact that labeling will continue to be needed means we should get started on it right away.

Indicio

About the Authors

Trevor Butterworth VP Governance

Trevor Butterworth is co-founder and VP of Governance of Indicio. He is also the chair of the Steering Committee for the Cardea Project at Linux Foundation Public Health, an open source project for sharing verifiable digital health credentials in a privacy preserving way. He is also a member of the Steering Committee for the Covid Credentials Initiative, also at Linux Foundation Public Health, and he is on the Stewards Governance Committee of the Velocity Network.

Trevor was educated at Trinity College Dublin, Georgetown University, and Columbia University's Graduate School of Journalism. He was a visiting fellow at Cornell, and is currently a visiting adjunct assistant professor in the Trinity Biomedical Sciences Institute at Trinity College Dublin.

Sam Curren Chief Architect/Deputy CTO

Sam Curren is Indicio's Senior Systems Architect and works on both open source and customer projects. He has been involved in the Identity Community for over 12 years, working and researching on personal data, distributed systems, supply chain digital birth certificates, and Decentralized Identifiers (DIDs). He is a co-chair of both the Hyperledger Aries project and the DIF DIDComm Working Group, and is also a member of the Decentralized Identity Foundation Steering Committee. Sam has a Masters Degree in Computer Science from Brigham Young University.