Requirements for a Trust Framework for Digital Verifiable Credentials for the Global Labor Market

Photo by Nastya Dulhiier

Photo by Nastya Dulhiier

Contents

Purpose of this document

There is an incredible community of individuals and organizations around the world working to reduce friction, empower individuals and accelerate labor markets by transitioning from the current paper/PDF based world of credentials, education and employment records to a digital, verifiable world.

And yet, progress toward mass-adoption is slow. We propose that one of the main reasons for slow progress is that the current effort is extremely fragmented. There are approximately 250-300 different projects or ecosystems worldwide, each with their own approach to technology, governance and trust.

The purpose of this document is to advance collaboration between the many projects around the world, accelerate consolidation efforts and drive towards interoperability which will enhance utility for all stakeholders.

The goal is to generate a common understanding of what “good looks like”: what future are we working towards.

The assumption is that a more aligned effort by the community will drive more adoption, and “a rising tide lifts all boats”.

If we can agree on all, or on a majority of the elements of a shared future, that would be ideal. But even where we cannot agree, understanding what we agree on and where we have differences that either need to be resolved or accommodated has immense value.

This document began its journey at the inaugural Global Digital Collaboration Conference in Geneva, July 2025. An initial draft of the requirements was created and discussed in preparation for, and at a lively panel during the event. The intent is to expose it to a growing number of professionals in the field, as an open working document, and continue to improve it through the contribution of the community.

Stefan Liström: This document attempts to approach requirements from a broader perspective than currently already existing individual technical implementations from wallet providers, issuers, relying parties or trust infrastructure suppliers. As such if you are a stakeholder already implementing trust within your part of this eco-system it is beneficial to take a step back and try to look at the bigger picture while reading this document.

Personas we are trying to solve for

At the Global Digital Collaboration Conference, we presented three personas for whom we are trying to solve the challenges of verifiable digital credentials.

Vanessa Lin

Registered Nurse

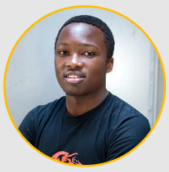
Born, educated and began career in the Philippines (first license and first nursing job, multiple certifications and trainings).

Then moved to Dubai to be a nurse (additional license and job history, new certifications).

Then moved to Netherlands to get an advanced degree in a specialized nursing area.

Then moved to the US. Needs to get a license and a job.

Challenges of global mobility in a highly regulated industry.



Iszak Mulama

Cyber-security specialist

Recent graduate in mechanical engineering from university in Kenya.

From age 14 has been hacker and gamer and has amazing software development and cyber-security skills and knowledge.

Has led a team to win a hackathon at the local university.

Wants to apply to a remote job at a global software company or gig opportunities via a global gig platform.

Challenges of skill recognition from informal learning. Challenges of global employers and global gig platforms

Bot1627

IT Specialist

Resume meets all requirements for each job description.

Identity documents, education diplomas and professional certification documents all look perfect.

Run by North Korean company.

Challenges of AI & increased fraud

These three personas are by no means exhaustive. They are representative of different populations and challenges that exist today in the labor market.

Sharon Lue: I think that a good world is where humans are acknowledged for the abilities that they have and we have a system that allows that to occur efficiently and effectively.

Joan Beets: If we think about the amount of people who don't have that privilege, who don't choose to move, but are forced to move, what success for me would look like is that for those individuals, there are far less barriers to entry into the labor market. Because the labor market is a market with far too many barriers for entry. What I would like to see is that that gets lowered and that everyone has an equal chance. Mobility is going to happen whether we like it or not, at least because of climate change, and so I'd like us to have a far more even playing field.

Tanya Troshyna: Our vision is where each of us has the chance to get our background verified quickly, reliably. We are in control of the data. We decide. It's fundamental as a human being to have my own data , and I can allow a certain amount of data, at the time I want, to who I want, just in the amount that is required to get the job done. And as an employer we need an ecosystem where they can verify the individual very quickly, with no loss of time, credibility or life.

Stephanie Winet: Employers need to be able to verify credentials instantly and digitally, resulting in faster hiring and onboarding cycles. These credentials need to be recognized and portable across borders.

Wesley Teter: Aligned with the UN Sustainability Development Goals to "Achieve equitable access to life-long learning opportunities" and to "decent work opportunities".

Scope of this document

> "A trust framework is a set of rules, policies, and standards that govern the operation of identity systems and establish trust among participants."
>
> **National Institute of Standards and Technology -** *NIST SP 800-63-3, Digital Identity Guidelines*

> "A trust framework is an agreed-upon set of policies, business rules, and legal agreements that establish trust between identity providers and relying parties."
>
> **Kantara Initiative -** *Kantara Initiative Trust Framework Operations Program*

This document aims to cover the requirements for a trust framework for the exchange of digital verifiable credentials for the global labor market.

The focus is on the requirements of the "envelop" (credential wrapper and signatures) and the "mail system" (methods of offering, issuing, disclosing and verifying credentials as well as identification of participants) to ensure trust across all participants in the ecosystem.

Out of scope

In addition to the trust framework, we recognize that there are more elements that need to be discussed and resolved to drive mass adoption of verifiable digital credentials in the global labor market. At this point, for the purpose of focus, we leave these out of this current document.

These include, but are not limited to:

Technical solutions - The document focuses on requirements and not on how these requirements are delivered technically.

Semantics - the content semantic interpretation of the credentials – the skill taxonomies and competencies models, the processes for evaluation and comparison/acceptance of qualification frameworks.

User Experience (UX) and User Interface (UI) of software applications for the different users (Issuers, individuals & relying parties). In an open ecosystem different suppliers of application will innovate and differentiate themselves on top of a common utility which is the trust framework. UX/UI is a critical layer to ensure inclusivity, accessibility and usability for all.

Sustainable business model and monetization – There is much discussion about the sustainable financing of a public-good trust framework and whether it should be funded by government, by non-profit organizations, or by the organizations utilizing and benefiting from the trust, speed and reduced cost of digital verification.

Adoption - The discussion about the important challenge of adoption is key, but not part of this document. A complete trust framework is a basic requirement, but surely not sufficient to address the many barriers to adoption. Accelerating Adoption is a multi-sided network problem, and the majority of use-cases suffer from a "cold-start-problem". The Chicken, egg and Rooster problem.

This is an ecosystem development challenge, where value is created for the majority of stakeholders only when there is sufficient "density". Although adoption is not in scope, we do believe that solving for trust in a collaborative and effective way will enable pooling/aligning the efforts of many contributors into this space, which will accelerate adoption and enable "all boats to raise on an incoming tide".

Requirements for Who?

The trust framework must address the needs of multiple stakeholders. The main groups of stakeholders which we should ensure we address include the individuals, Issuing Organizations, Relying Parties and Solution Providers to all these network participants.

Individuals

Individuals are the earners of credentials through formal education, informal learning, work and many other methods. Often referred to as the Learner, Employee, Holder (of credentials).

The individuals primarily aim to be able to simply, quickly, cheaply be able to showcase the knowledge, skills, experiences, licenses or other information in pursuit of employment, income and personal growth.

Issuing Organizations

Organizations making an attestation about an individual and making this attestation available to the individual in the form of a digital credential (issuing).

Issuing organizations are a wide variety of types of organizations with different roles and relationships with the individuals. This includes, but is not limited to employers, education institutions, licensing bodies, training providers, assessment vendors, certification bodies and more.

The issuing organizations primarily would like to provide their learners/workers/customers with documentation of their successful completion of a course, program, degree, challenge, certification, license etc. They often would like to ensure that individuals can efficiently use the credentials for the purpose of advancing their careers. These organizations often would like to protect their brands and/or the public by ensuring that there is trust in the credentials that they issue.

Relying Parties

Organizations receiving a credential or set of credentials (a presentation) from an individual and verifying these.

Issuing organizations are a wide variety of types of organizations with different roles and relationships with the individuals. This includes, but is not limited to employers, education institutions, licensing bodies, training providers, assessment vendors, certification bodies and more.

The relying parties would like to be able to receive a disclosure of credentials from an individual and verify these at an appropriate level of assurance (depending on the use case), within a minimum time and at a minimum cost.

Solution Providers

Software vendors who provide solutions for all the participants in the credential ecosystem.

Solution providers to issuing organizations – Student Information Systems (SIS), Learning Management Systems (LMS), HR Management Systems (HRMS) and Credentialing Platforms that enable issuing organizations.

Wallet providers to the individuals.

Solution providers to relying parties – Recruiting Marketing Systems, Candidate Relationship Management, Applicant Tracking Systems (ATS), Learning Management Systems (LMS), Career pathways and advisory solutions which enable organizations to receive and process credentials for different purposes.

Solution providers would like to grow their businesses by selling solutions that provide maximum value to their customers. This often requires a sensitive balance of unique features and differentiators while ensuring interoperability to enable maximum utility and value.

The 10 Requirements

These are the 10 categories of functional requirements we have identified:

I. Individual at the center
II. Global
III. Accommodate all work-related information
IV. Assurance, trust & verifiability
V. Compliance (Privacy ++)
VI. Survivability
VII. Open
VIII. Verifiable Presentation of Multiple Credentials
IX. Issuer revocation and change
X. Support Notary

It is noted that a number of items could appear in more than one of the categories, and that the categories could be grouped in alternative ways. Therefore, we ask that you review this set of requirements as a complete collection.

I. Individual at the Center

The trust framework must be centered around the individual.

Assumptions

It is a basic human right in the digital age for an individual to be able to easily and digitally showcase and prove who they are, what they know and what skills and experiences they have attained.

The labor market is global and highly fragmented. With millions of issuers and millions of relying parties, we need an open protocol, like email, that enables everyone to exchange data - this can only happen practically through the individual.

A self-sovereign approach, putting individuals in control of their data, also addresses much of the compliance challenges.

Requirements

- Individuals must maintain ownership and control on their credentials.
- Individuals must have the ability to consolidate their credentials from all issuing bodies into a single wallet of their choice.
- Portability - Individuals should not be confined to a specific wallet and should have the freedom to effortlessly transfer their credentials to other wallets that adhere to the same protocols without losing utility.
- Individuals must be able to universally share their credentials with any relying party, without any restrictions or limitations.
- Individuals must be able to curate and share a broad or limited presentation out of this collection. Solution must support principles of selective disclosure and data minimization.
- The individual must be able to self-assert credentials. Self-asserted credentials must be clearly marked as such yet adhere to the same technical standards and schemas as verifiable credentials and be shared as part of a disclosure, together with other credentials, verifiable or self-reported.

Discussion & Notes

Tanya Troshyna: In a truly decentralized and distributed world, there might be multiple wallets, but individuals should be able to port data from one to another or to connect them together for a holistic view. Individual consent in any exchange of their data is key.

Joan Beets: Right now, individuals get to decide what they do and do not disclose, this should be no different with a digital solution.

Stephanie Winet: As employers, we recognize the importance of empowering individuals with ownership and control over their personal credentials while ensuring the integrity, trustworthiness, and interoperability of the credentialing ecosystem.

Sharon Lue: Should be designed for all users – in addition to centering user workflows around the holder, the system that supports skills-based transactions should be designed to ensure accessibility, inclusivity, and engagement across diverse backgrounds and abilities.

II. Global

The trust framework must be international / global / (Inter-planetary?).

Assumptions

The labor market is highly connected and is becoming more and more global.

- Individuals increasingly move across borders, whether this be because of professional migration or displacement as refugees.
- Work moves. Multinational organizations source and hire talent around the world. They may hire individuals into their sites in different countries, may hire them to work remotely, or engage with them via staffing companies or gig platforms.
- Learning is becoming increasingly global, with organizations offering learning online and remotely such as LinkedIn Learning, Coursera or University of the People.

Individuals would like to move their data/credentials across borders and still have these recognizable and verifiable.

Requirements

- The trust framework must enable individuals to claim credentials in any jurisdiction and share credentials in any jurisdiction.
- The trust framework must support global mobility of Individuals.
- The trust framework should provide global employers with the ability to receive and verify credentials in a consistent method anywhere in the world.
- The trust framework must be flexible to support the unique requirements of different industries and local labor markets.
- Solution must support multi-language

Discussion & Notes

Stephanie Winet: We agree to a globally interoperable, inclusive, and adaptable credentialing ecosystem that empowers individuals and employers alike. However, operational realities demonstrate that building and scaling such infrastructure often benefits from a phased, regionally focused approach.

Sharon Lue: This can be implied if the system is interoperable and based on community developed open standards. Should prioritize the needs of the user in their current and existing context.

Tanya Troshyna: However, for the statement of “Solution must support multi-language”, to enable cross-border data sharing, there may need to be a recommended default language, or minimal set of languages a credential should be available in (i.e. English, Spanish, etc.). This should be provided directly from the source issuer. Credentials in additional languages may be provided by Notary issuers, linking to the original credential.

III. Accommodate all work-related information

Solution must be broad and be able to accommodate all work-related data elements

Assumption

Our assumption is that over time a disclosure of a collection of digital verifiable credentials will displace the traditional resume, LinkedIn profile or application forms. Individuals will curate 10s or even 100s of assertions in the form of verifiable credentials throughout their education and professional life and share single credentials or collections of credentials with relying parties for multiple different purposes.

Requirements

- The trust framework must be flexible enough to support the credentialing of any method of skill attainment:
    - Primary, secondary and post-secondary education
    - Training
    - Work experience, internship, apprenticeship
    - Self-learning
- The trust framework must be flexible enough to support the credentialing of any method of skill assessment and recognition:
    - Assessment
    - Certification
    - License
- Must support credentialing of any information required to meet job requirements in a country, industry or employer:
    - Work experience
    - Attributes such as societies, clubs, activities, affiliations, honors and awards.
    - Right To Work (RTW)
    - Occupational Health records

Discussion & Notes

Joan Beets: All work-related data also sounds a bit too broad. It could be rephrased to relevant, consent-based work-related data. What's important is relevancy. I would love to see a world where we can submit a set of credentials, essentially without a name, date of birth or other elements that you can discriminate against. Aim is to a start line of the race purely based on skills.

Sharon Lue: We need to ensure that when the many issuers issue verifiable credentials, that the fundamental information about how a skill is obtained, what is the definition of a skill and how the work being done is made transparent in a framework that can be comparable.

Stephanie Winet: Some of the credentials would be easily digitalized and recognized, particularly when we have government support. Others may not be easy because there is a subjective element to them. If we want to encompass ALL work-related information, we need to talk about the skills acquired on the job. This would mean that employers would need to issue some sort of credentials or assessment to the holder. How do we convince employers to do that?

IV. Assurance, trust & verifiability

The trust framework must meet the highest level of assurance, trust & verifiability

Assumption

Once a level of trust and confidence in an assertion has been established, and a credential has been issued, there is no way to change it.

A credential of a higher level of assurance can be utilized for the purpose of low-assurance level use-cases. But the opposite is not true. Lower levels of assurance cannot be utilized in use-cases where higher levels of assurance are needed.

The trust framework must meet the requirements of the most highly regulated industries, such as healthcare, aviation, oil & gas, education, even if not all capabilities are required in other use-cases.

Requirements

- The trust framework must define clear legal liabilities of issuers relating to the credentials they issue.
- Individual authentication - Must include authentication methods that enable the issuer to obtain and document rigorous proof required to confirm that the individual is genuinely who they claim to be before issuing them credentials.
- Source Verification – The trust framework must include authentication methods that enable the relying party to obtain and document rigorous proof required to confirm that the issuer of a credential is genuinely the entity they claim to be.
- Source Authority Verification – the trust framework should include methods that enable the relying party to obtain and document rigorous proof required to confirm that the issuer has the authority to assert the claims included in the credential.
- Data Integrity – The trust framework must include methods that enable the relying party to obtain and document rigorous proof required to confirm that the information included in the credential genuinely represents the claims made by the issuer.
- Revocation Status Verification – The trust framework must include methods that enable the relying party to obtain and document rigorous proof required to confirm that the credential was not revoked by the issuer.
- Person Binding – the trust framework must include methods that enable the relying party to obtain and document rigorous proof required to confirm that the credential was issued by the issuer to the individual presenting it.

Discussion

Sharon Lue: Industries have differing levels of assurance. The governance of this ecosystem in implementations can accommodate if the infrastructure enables transparency. Also note potential conflict with first statement.

Stephanie Winet: Assurance, trust, integrity, and legal accountability of digital credentials are non-negotiable.

V. Compliance (Privacy ++)

The trust framework must ensure that participants are compliant with all relevant local regulations.

Assumptions

Education, skills and employment related credentials are sensitive Personal Identifiable Information (PII) and part of the individual's identity. As such they are governed by privacy regulations. In addition, in many jurisdictions there are legislative requirements relating to this data in the context of education laws, work/employment related legislation and more.

As individuals move their data across jurisdictions they want to make sure they are compliant. When relying parties receive, verify and utilize this data issued by many issuers from many jurisdictions and regulatory conditions, they want to make sure that they are compliant.

Requirements

- Solution must be compliant with all relevant regulations that govern data and information in the labor market, including, but not limited to:
    - Privacy regulations (e.g. General Data Protection Regulation - GDPR)
    - Employment regulations, laws governing employment records and labor market information protections (e.g. California Privacy Rights Act - CPRA)
    - Education regulations (e.g Family Educational Rights and Privacy Act - FERPA)
    - Other relevant regulations (e.g. Fair Credit Reporting Act - FCRA)
- No "Dial Home"

Discussion & Notes

Sharon Lue:	It seems unlikely that privacy principles can be agreed upon across all jurisdictions, so should focus on privacy by design principles of the technology and standards in a way that honors the first statement.
Joan Beets:	For me this is a goal rather than a requirement. If we want it to be global and compliant with every single regulation in the world, it will never happen. Unfortunately, whilst the world has become global, legislation surrounding employment has not. This can be, however, an additional incentive for governments to rethink how they legislate work. One compliance aspect that would be an extra incentive for governments to adapt is if it were able to function as proof of job applications in the cases of someone who receives unemployment benefits. Providing a digital, verifiable solution to a process which is very open to fraud would be of interest to them and make life easier for those unemployed.

VI. Survivability

The trust framework must ensure that credentials are survivable of issuer existence.

Assumptions

Issuers cease to exist. Employers go out of business. Education Institutions shut down. Even states dissolve. Issuing organizations are acquired. They may lose their data as a result of war, catastrophe or being hacked. In some countries individuals have a “right to be forgotten” and request that their data no longer be held by the organization.

And yet in all these cases the individuals want and need the credentials they have earned to continue to be accepted, trusted and verifiable.

Requirement

- Data / Assertions must be accessible and verifiable even if the Issuing body no longer exists or no longer has the data.

Discussion and Notes

Stephanie Winet: Solutions should guarantee the long-term survivability and independent verifiability of credentials, irrespective of issuer continuity. This is essential for risk management, legal compliance, operational resilience, and protecting workforce integrity. The value however may be diminished.

VII. Open

The trust framework must be based on open standards and open-source technologies.

Assumptions

It is critical to ensure that the trust framework is widely adopted and available to the general public.

Solutions based on open standards and open-source software remove the risk of vendor lock-in and improve the ability to generate both interoperability across solutions as well as drive innovation and a broad range of solutions.

Requirements

- The trust framework must serve as an open, public-good infrastructure
- The trust framework must support technical and data interoperability by being based on open technology standards and on open data standards.
- The trust framework must be available via open-source technologies.

Discussion & Notes

Tanya Troshyna: While it's a must, it's also a challenging claim. Open standards continuously evolve, get deprecated or new ones are created. In a truly distributed network, when various parties use different versions of open standards, or even different open standards, it becomes challenging to be inclusive for all.

VIII. Verifiable Presentation of Multiple Credentials

Employers / Organizations must be able to receive a presentation (i.e. “resume”) and verify all its content immediately and digitally.

Assumptions

Verifiable credentials will gradually replace (partially or completely) the current self-reported assertions made by individuals via a resume or a LinkedIn profile.

Although we can’t predict exactly what form this will take (a simple collection of verifiable credentials, a resume with linked verifiable credentials, a formal such as LER-RS etc), the trust framework must allow for individuals to share a collection of verifiable credentials in a single transaction.

It is critical that there will be simple user experience for the individual to select and disclose a set of credentials.

In the use-cases where the relying party would like to verify each of the credentials that have been disclosed in a set, it is critical that the relying party does not need to verify each of the credentials separately, under a different process and from a different sources, but can verify them all in a single transaction and process.

In many cases the Relying Party AI-based solutions will interpret the presentation of verifiable credentials, evaluate, model, and predict fit and success in a role.

Requirements

- A curated selection of credentials (10s, or maybe even 100s) can be shared by the individual to a Relying Party in a single presentation.
- A complete presentation can be verified by the relying party.

Discussion & Notes

Stephanie Winet: Employers generally agree with the vision of verifiable, digital, curated credential presentations as a powerful modernization of hiring processes. We welcome AI assistance but expect strong governance, transparency, and safeguards to ensure fairness, compliance, and responsible use.

IX. Issuer revocation and change

The trust framework must enable the Issuers to revoke credentials they have issued.

Assumptions

There are use-cases in which issuing organizations must retain the ability to revoke a credential. The most obvious cases are when a credential must be taken away to protect the public, such as in the case of revoking a nursing license from a nurse committing malpractice or a truck driver who has driven under the influence of alcohol. Other cases include when it is discovered that the individual was granted a credential by mistake, when it was unrightfully earned.

An event in which an issue is required to make a change in a credential may practically be performed as a revocation of the old credential and issuance of a new one.

Requirements

- Revocation - An Issuer must be able to revoke a credential held by an individual.
- Change - An Issuer must be able to “update a credential” held by an individual user. This update is a revocation of the former credential and in issuing of a new credential.
- The issuer must notify the individual of any credential revocation or credential change event.
- The individual continues to “hold” and own revoked credentials and can present them if they choose to.

Discussion & Notes

Joan Beets: Even if a credential is revoked, it would be good to still be able to show that you once had it as it shows an awareness of the knowledge/requirements which in some cases can be beneficial. E.g. a managerial job, where you do not do certain activities which require certification, but you do supervise others who do this work.

Stephanie Winet: There are credentials, such as birth certificate, that must not be revoked.

Sharon: This calls a potential conflict with the first requirement of individual control. Do I legally have the right to contest your determination of my credential status?

Weslet Teter: There is a policy framework for applicants seeking recognition that they have a right to appeal.

X. Notary

The trust framework must allow for notary/apostille issuing.

Assumptions

For the foreseeable future there will be primary-sources of education and employment-related credentials that have ceased to exist or are not capable of issuing verifiable digital credentials to their stakeholders.

Notary issuers can provide an invaluable service to the transitioning market by complementing primary source issuers. Notary issuers are organizations who can perform a verification of existing primary-source evidence and issue a verifiable credential which they sign.

Requirements

- The trust framework must enable accredited notaries to issue credentials to individuals based on clear criteria of primary-source verification.

Discussion & Notes

Stephanie Winet: Credentials issued or certified by accredited notaries or with apostilles provide an added layer of legal authenticity and primary-source verification, especially for international or cross-jurisdictional recognition.

Tanya Troshyna: In some cases, a notary issuer may be the only remaining issuer because the primary-source doesn't exist anymore. There is question related to the "value" of those credentials. Background Check Company saying I have a German C1 degree has less of a value compared to my German school saying that. But when my German school doesn't exist anymore, Background Check Company's credentials will become more valuable or less valuable because the primary source doesn't exist anymore? These are use-case specific areas. One solution may not fit all scenarios of Notary issuers, at least in the beginning.

Contributors

Joan Beets - Managing Partner, KennedyFitch

Etan Bernstein – Co-Founder and Head of Ecosystem, Velocity Network Foundation (VNF)

Lyn Brooks - Board Director, Member Advisory Council, Ambassador, Ayra Association

Hennie Bulstra - Business Consultant Policy and Strategy at DUO, and Convenor of the User Group on Diplomas and Credentials at the European Blockchain Partnership

Dror Gurevich – Founder & CEO, Velocity Network Foundation

Stefan Liström - Project Manager, European Digital Identity Wallet ecosystem within the EU Large Scale Pilot DC4EU, Swedish Research Council

Sharon Lue - Executive in Residence, Jobs for the Future (JFF)

Darrell O'Donnell - Executive Director, Ayra Association

Colin Strasburg - Digital Identity Director, Fragomen

Wesley Teter - Specialist, Higher Education, UNESCO

Tanya Troshyna - Chief Product Officer, Affinidi

Rupert Ward - Professor of Learning Innovation, The University of Huddersfield

Stéphanie Winet - Head of Stakeholder Engagement, International Organisation of Employers (IOE)