Identity & the Web

25 February 2025

▶ **More details about this document**

Abstract

This document proposes an overview of Digital Identities on the Web and an analysis through different use cases of the systemic impact on both the market side and the human side, as well as the role that Web standardization may play in managing that impact.

Status of this document

This document is intended to capture the current shared understanding of the W3C Team on the current and expected impact of developments linked to identity on the Web and identifying explorations the World Wide Web Consortium and its community have started or ought to be starting to manage that impact. It does not represent any consensus from the W3C Membership, nor is it a standardization document.

The document was authored by Simone Onofri (simone@w3.org), with significant contributions from the W3C Team and people listed in the Acknowledgements section.

This document helps structure discussions on what may be needed at the standardization level to make Identity's systemic impact less harmful or more manageable. It is bound to be incomplete and sometimes wrong — we are gathering input and feedback in GitHub, preferably before October 6, 2024.

If it's not feasible for you to use GitHub, send comments in e-mail to: public-team-report-comments@w3.org. Please put your comments in the body of the message, not as an attachment. Start your e-mail subject line with: [identity-web-impact].

Depending on the feedback received, possible next steps include more in-depth stakeholder interviews, a dedicated W3C Workshop, or developing a standardization roadmap.

Table of Contents

§ 1. Executive summary

Digital Identities have been in development for decades. As governments increasingly consider becoming providers and consumers of these technologies, they more than ever have the potential to change the Web and the concept of identity as we know it.

Given the scope and scale of this innovation, digital identities are significantly impacting the web and, in particular, privacy, altering the assumptions and the balance that have shaped its ecosystem.

This document further develops the concepts described in "*Identity on the Web*" at W3C's Member Meeting of April 2024 [identity-on-the-web]. It reviews the intersections of Digital Identities through their societal, ethical, and technical impacts and highlights several areas where standardization, guidelines, and interoperability could help manage these changes:

- Enabling passwordless credentials for authentication and payments
- Enabling federated identity in the web platform without third-party cookies
- Modeling security, privacy, and human rights threats of decentralized credentials
- Mitigating surveillance, censorship, intrusion, and discrimination and ensuring interoperability by standardizing digital credentials in the web platform
- Mitigating the threats at technological and governance levels

Through exploratory thinking, the following understanding emerged:

- Standards can help, as they have in the past, to drive innovation while mitigating threats and to enable technical progress while having a positive impact on the world.

- The technology stack is composite and broad and needs to be coordinated across standards and Standards Development Organizations (SDOs).
- People, SDOs, and governments are the key actors who need to collaborate to ensure that digital credentials/identities solve more problems than they create because identity is not only technology but also governance.
- It is crucial to pay close attention to the impact on security, privacy, and human rights in general. The proposed method of analysis is threat modeling.

We seek input from the community on proposals that could help progress on these topics and other topics that this document may contribute to identifying.

§ 2. Introduction

Digital Identities have been in development for decades, and at this moment in history, they are about to be implemented government-wide. They can change the Web and the concept of Identity as we know it. There are many opportunities but also threats to society and the Web.

§ 2.1. Terminology

The concept of identity is very broad and covers psychology, social sciences, mathematics, and logic. There is no agreed-upon definition of all the terminology. Let us start with a set of definitions to have a common ground in this paper.

When we think about identity, we often think about our identity as individuals. It is inherent, although we tend to give a different meaning to our identity according to our culture, from the Western "*Cogito ergo sum*" (I think therefore I am) [discourse-on-the-method] to the African "*Ubuntu*" (I am because you are) [what-does-ubuntu-really-mean] or the Eastern "*tat tvam asl*" (that thou art), which express two notions, the man's real self (ātman), and the Cosmic Self (brahman) [a-dictionary-of-hinduism].

Analyzing the etymology, the term **identity** comes from the Latin root "*idem*", which means "*the same*" [oxford-etymology-identity], so while it is an intimate concept, we also use it to distinguish ourselves from others. This is well explained in the Cambridge Dictionary in which the identity is "*the fact of being, or feeling that you are, a particular type of person, organization, etc.; the qualities that make a person, organization, etc. different from others*" [cambridge-dictionary-identity].

Thus, *"from a sociocultural perspective, an individual's identity is socially constructed, forming from early childhood from their interactions and relationships with others"* [constructing-an-identity].

Therefore, our identity is tied to society and the third parties we interact with. These parties often give us an identity and the elements to refer to and prove who we are.

Looking more closely at the Information Technology (IT) domain, the ISO/IEC 24760-1:2019 [ISO-IEC-24760-1] defines **Identity** as "*a set of attributes related to an entity*". Where the **entity** is something "*that has recognizably distinct existence*", and that can be "*logical or physical*" such as "*a person, an organization, a device, a group of such items, a human subscriber to a telecom service, a SIM card, a passport, a network interface card, a software application, a service or a website*". These **attributes** are "*characteristics or properties*" such as "*an entity type, address information, telephone number, a privilege, a MAC address, a domain name*". To complete the definition of *entity* and *identifiers*, it is important to note that they always refer to a **domain** of applicability, the specific *context* where they can be used (e.g., an organization, a country, a university).

Thus, a particularly important point is clear: there are not only identities of people, individuals, or human beings. We can also have identities for organizations, pets, and **Non-Human Identities** (NHI). NHI are all those accounts widely used by "devices, services, and servers" in networking, cloud, and workloads [the-evolving-landscape-of-non-human-identity].

Now, an important logical step. We present **credentials** to claim our identities, whether in the physical or digital world. Just as we do not have a one-size-fits-all definition of identity, we also do not have a one-size-fits-all definition of credential, as it changes according to context. Starting with the definition from the Cambridge Dictionary, a (digital) credential is "*a piece of information that is sent from one computer to another to check that a user is who they claim to be or to allow someone to see information*" [cambridge-dictionary-identity]. While high-level, this definition considers two important aspects: on the one hand, the credential is used to prove our claims, such as who we are, and on the other hand, it can be used to gain access to information:

- The **ISO/IEC 24760-1** definition is very close to the last aspect from the dictionary, where a credential is a "*representation of an identity for use in authentication*" [ISO-IEC-24760-1].
- The **Identification for Development (ID4D)** definition is close to the first aspect: "*any document, object, or data structure that vouches for a person's identity through some method of trust and authentication*" [types-of-credentials-and-authenticators].
- The **NIST SP 800-63-3** definition echoes the first aspect, "*an object or data structure that authoritatively binds an identity—via an identifier or identifiers—and (optionally) additional attributes to at least one authenticator*" [NIST-SP-800-63-3]. It adds the important concept of binding an identity to its attributes—recalling ISO's definition of identity—and using identifiers.
- The **W3C Verifiable Credentials Data Model (VCDM)** definition states, "*a set of one or more claims made by an issuer*" [vc-data-model-2.0]. On the one hand, this definition seems similar to NIST's. However, its framing is in the decentralized versus federated model (which we will

analyze shortly), and thus, to ISO's definition of identity mapping the ISO's attributes to VCDM claims.

> NOTE: Therefore, we will refer to the specific definition of credential in the various sections of the document according to the context.

An additional definition introduced in the NIST blog is **Verifiable Digital Credentials** as a broader term encompassing the ecosystem [nist-verifiable-digital-credential]. This definition was established to resolve a terminological issue. The term "Verifiable Credentials" emerged within the W3C Verifiable Credentials Working Group, and subsequently the `vc` media type. Other SDOs also used the `vc` media type but applied it to a different type of credential, particularly within the IETF OAuth group. The OAuth group later transitioned to using `dc` for "Digital Credentials". Hence the need for an all-encompassing term [digital-credentials-that-can-be-verified].

These definitions introduced important concepts that need clarification, such as *identifiers*, *authentication*, and *trust*.

Identifiers are *pieces of information that uniquely refer to an entity within a specific context*. According to the W3C Decentralized Identifiers, there are various types of identifiers: "*communication addresses (telephone numbers, email addresses, usernames on social media), ID numbers (for passports, driver's licenses, tax IDs, health insurance), and product identifiers (serial numbers, barcodes, RFIDs). URIs (Uniform Resource Identifiers) are used for resources on the Web, and each web page you view in a browser has a globally unique URL (Uniform Resource Locator)*" [did-core].

> NOTE: Although entity, identity, and identifier are related, they are distinct: Identity refers to the essence of who or what an entity is, while an identifier is a specific piece of information used to recognize and refer to that entity uniquely.

Let us then try to understand the *authentication* process and how it differs from identification, verification, and authorization:

- **Identification** is recognizing an entity through the information it provides. For example, we enter our first name, surname, and email address in a social network (and there are different levels of proofing of our real identity).
- **Verification** allows us to confirm that the presented information is valid through further testing. Verification is a generic process that can take different forms and have different effects. For example, we often receive an email with a confirmation link to verify an email address. We confirm that the email address is under our control by clicking on it. This type of verification

demonstrates control over the identifier. Verifying identity information online, such as a specific name and surname, is more complex. When verifying identity information, we use the term *identity verification*.

- **Authentication** is a specific, *formal* verification type that aims to grant access to a resource, service, or information. This process usually involves verifying control of our identifier with something we know (e.g., a password), something we have (e.g., a hardware token), or something we are (e.g., a biometric characteristic). For instance, similar to the email example, we demonstrate control over a username (the identifier of our identity) by entering the corresponding password.
- **Authorization** is another key process that follows authentication. It verifies whether our authenticated identity has the necessary permissions to access a particular resource. This step ensures that we are only granted access to resources we can use even after confirming our identity.

Let us see how these concepts can be applied to **physical credentials**. When we present our passport to cross the border, here is an example of the processes that might be carried out:

- **Identification**: We present our passport to the border control officer, claiming our identity through our credentials and its identifier (the passport ID).
- **Verification**: The border control officer verifies that the passport is genuine, not tampered with, not expired, and issued by a recognized government.
- **Authentication**: In this context, the authentication involves verifying that the person presenting the passport is the rightful holder. This might include checking biometric data stored in the passport against the person's actual biometrics (e.g., fingerprints or facial recognition).
- **Authorization**: Finally, authorization is the process where border control determines whether the authenticated individual has permission to enter the country. This decision is based on various factors, including visa validity, passport not expiring in six months or less, and confirmation that the individual is not on any watchlists, unwanted lists, or other checks.

When we use **digital credentials** on the Internet instead, the issue is more challenging, as illustrated by Peter Steiner's celebrated cartoon published in the New Yorker in 1993: "*On the Internet, nobody knows you are a dog*" [nobody-knows-you-re-a-dog]. Historically, digital credentials have taken various forms, such as:

- The usernames and passwords we use to log in to our favorite social network and communicate with friends.
- The same usernames and passwords from our favorite social network, but used to authenticate on an e-commerce website and make a purchase.

- A digital driver's license in our digital wallet.

> NOTE: The last form of credential, as defined by W3C, has a wider range of use cases than just authentication. One important clarification: it may make sense to use a driver's license to authenticate only on the issuer's systems (e.g., it is good to authenticate ourselves on government websites but not on our personal email provider). Furthermore, additional information (claims) on the driver's license, such as date of birth and, in some cases, home address verified by a trusted entity such as a government, enables interesting use cases.

Therefore, it's important to remember that we can have digital credentials that are not identity documents, such as diplomas, which, in this case, are issued by universities. Several projects exist, such as the Digital Credential Consortium (DCC) and Blockcerts, which are committed to building an infrastructure for academic digital credentials.

We introduce the last topic with the example of credentials that universities can issue. In addition to degree certificates, universities usually have student ID cards containing information such as first name, last name, and photo.

Why can a driver's license and a student ID card, having similar attributes and being cryptographically verifiable, only allow the driver's license to open a bank account?

There are several aspects, first of all, the *context* and *domain* in which the credential lives. The key difference lies in the **trust** we place in the issuers of these credentials. Trust can be defined as "*the belief that someone is good and honest and will not harm you, or that something is safe and reliable*" [cambridge-dictionary-trust]. Essentially, trust is a choice we make; we choose to trust or not trust someone or something [OSSTMM-3], and often, it is not a binary question.

Cryptographic trust, such as verifying the signature of a credential, differs from *human trust* [self-sovereign-identity]. Cryptographic methods ensure that the credentials haven't been tampered with and that they have been issued by a trusted issuer. Human trust involves trusting the entity that issued the credential or, in the case of an issuer chain, trusting the root, and that the issuer provided the credential to the legitimate user.

This is why we also need **governance frameworks** or **trust frameworks**. These frameworks include business, legal, and technical rules that help establish and maintain trust in credential issuers.

This includes establishing the **Levels of (identity) Assurance (LOA)**. Follow as an example the *Identity Assurance Level (IAL)* from NIST-SP-800-63-3 [NIST-SP-800-63-3]:

- **IAL1**: No requirement to prove a specific real life identity, e.g., identity can be self-asserted.
- **IAL2**: Remote or in-person identity proofing with supporting evidence is required.

- **IAL3**: Physical presence is required for identity proofing, with proper verification of evidence.

Having concluded this roundup of terminology, before we delve into the various digital identity management models that have come and gone over time and that we have used in the previous examples, let us try to understand why identities are so important.

2.2. Why identity is important

Human identities are a very special case, particularly those issued by governments. We know that they are not the only type and that the others are also important and have interesting business implications, but human ones have distinctive characteristics. Let us see why.

2.2.1. Human rights

Identity is a fundamental human right that underpins personal *dignity* and *autonomy*. Article 6 of the Universal Declaration of Human Rights states, "*Everyone has the right to recognition everywhere as a person before the law*" [UDHR]. This principle is reinforced by Article 16 of the International Covenant on Civil and Political Rights, which similarly reads: "*Everyone shall have the right to recognition everywhere as a person before the law*" [ICCPR].

Although the term "identity" is not explicitly used here, its concept is inherent in recognizing the identity as a person.

2.2.2. Sustainable development goal

Despite being a right, much work still needs to be done to provide identities for all the population.

However, target 16.9 of the 2030 United Nations Sustainable Development Goals (SDGs) aims to achieve "*legal identity for all, including birth registration*" [SDGS-16].

2.2.3. Identity for Development (ID4D)

Achieving legal identity for all is a challenging goal on several fronts. In response, the World Bank has launched the ID4D initiative, aiming to "*secure a unique legal identity and enable digital ID-based services for all by 2030*" [ID4D-initiative].

§ 2.2.4. Opportunities and threats

Digital identities and credentials are powerful business enablers and offer significant opportunities for individuals, governments, and organizations.

They can guarantee other rights, such as the right to accessibility promoted by the *Marrakesh Treaty* [marrakesh-treaty]. They can also "*empower refugees, stateless individuals, and forcibly displaced persons*" [UNHCR-digital-identity].

These technologies can also be used on a humanitarian level. Referring to the NHIs, the International Committee of Red Cross (ICRC) investigated *Digital Emblems* [ADEM] to identify ICT assets protected under international law [digitalizing-report].

> NOTE: However, like all innovations, these technologies can have downsides. To paraphrase Paul Watzlawick, the innovation of these technologies must not become "*ultra-solutions*" where "*operation successful, patient dead*" [ultra-solutions]. So, the challenge is to enable this technological innovation by being aware of the threats to privacy, security, and human rights.

Therefore, it is necessary to analyze the various threats to mitigate them at their root in designing and implementing these technologies and related standards.

As an example, below is an initial analysis of threats to human rights (Harms) concerning government-issued digital identities using Microsoft's Harms Modeling [harms-modeling]:

- **Opportunity Loss** (*Discrimination*): This complex issue spans multiple areas. *Digital divide*: if digital identities are required for access to public services and no alternatives are present, and if they depend on certain hardware, software, or stable connectivity, it can lead to discrimination for people who do not have availability of these resources. In addition to discrimination within the same country, there is further discrimination if there is no "cross-border" interoperability between the technologies and implementations used by different governments.
- **Economic loss** (*Discrimination*): The availability of digital identities and related credentials, which can contain a lot of information regarding wealth status, can be used to discriminate against access to credit. This can also be generalized - as was identified during a W3C breakout session - and concerns the Javons paradox. The more information available, the more likely it is that collection, particularly in greedy data-driven contexts, is abused.
- **Dignity loss** (*Dehumanization*): For example, if the vocabulary does not correctly describe people's characteristics, this can reduce or obscure people's humanity and characteristics.
- **Privacy Loss** (*Surveillance*): if this technology is not designed and implemented properly, it can lead to surveillance by state and non-state actors such as government and private technology

providers. For example, centralized or federated models are more prone to these threats, while decentralized models are less so, but it depends on how they are implemented. Therefore, it is necessary to provide privacy-preserving technologies and implement them properly.

§ 3. Digital identity management models

With these assumptions, before proceeding, it is important to understand how digital identities are managed and how they have evolved over the years.

Let us start with the example of a person's identity given earlier and break it down. We had:

- Credentials of a social network that are used on the same site.
- Credentials of a social network that are used on a different site.
- Driver's license within a digital wallet application.

These examples represent the evolutionary stages of Internet Identity described by Christopher Allen at the Internet Identity Workshop (IIW). From these developmental stages, the community agrees that there are currently three models of identity relationships [three-models-of-digital-identity-relationships]. Let us analyze them.

§ 3.1. Centralized identity model

In the centralized identity model, also known as siloed or traditional, a single provider offers both the identity (and its credentials, typically a username and password) and the service. This older model was used in the early days of the Internet and the Web and is still used today.

The centralized identity model is the typical scenario when the user logs in to a social network to use it, and the credentials here are used to authenticate.

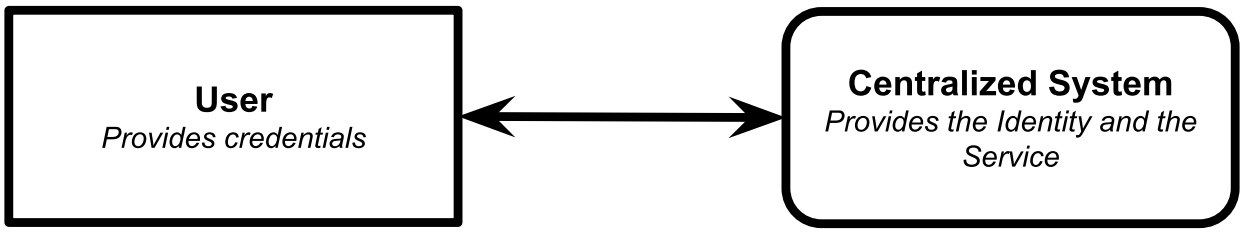

Figure 1 *Centralized Identity Management*

Here is the simplified *Data Flow*:

- **Authentication**: The user authenticates themselves with the centralized system using their credentials.
- **Access Granting**: This system grants access to the resource.

Perspectives:

- **Security**: there are different issues. For the *user*: password re-use in case of compromised password, so the user should use different passwords for different providers; there are also Phishing and Man-in-The-Middle attacks. From the provider's point of view, as the passwords are stored on their systems, they need to implement proper security measures to protect them at rest and during transport.
- **Privacy**: the centralized system can completely track the user.
- **Standards**: Standards intervene at different levels. In how credentials are exchanged and sent: historically, *Basic Authentication* [RFC1945], *Digest Authentication* [RFC2069] (and related updates), and via *HTML forms* with `input type=password` and `Cookies` for maintaining the session information on the Client. Other standards for increasing authentication factors include HOTP [RFC4226] and TOTP [RFC6238]. Also, with SSL/TLS [RFC2246] (and related updates) for credential transport and general traffic protection. . Other standards protecting the credentials at rest such as the (now obsolete) MD5 [RFC1321] and other hashing algorithms by NIST.

> Enabling passwordless credentials for authentication and payments
>
> To mitigate security threats, in particular the use of multiple passwords and phishing, FIDO Alliance created **Passkeys**, "*a replacement for passwords that provide faster, easier, and more secure sign-ins to websites and apps across a user's devices*" [passkeys-101].
>
> The W3C Web Authentication Working Group brought strong authentication to the Web Platform through Web Authentication Level 2 [webauthn-2] and is developing Level 3 [webauthn-3].
>
> Synchronized Web Authentication credentials —passkeys— are well-suited for login authentication but less well-suited for some regulated high-assurance use cases, notably payments. To fulfill additional requirements of payments ecosystems, the W3C Web Payments Working Group is developing Secure Payment Confirmation [secure-payment-confirmation] to support multi-factor authentication and requirements for cryptographic evidence of user consent to the terms of a transaction.

§ 3.2. Federated identity model

In the federated identity model, the function of *making available identity information*, also known as a third-party **Identity Provider (IdP)**, is separated from the one *which provides a service to the user* - the **Service Provider (SP) or Relying Party (RP)** [ISO-IEC-24760-1].

The federated identity model is the typical scenario when a user logs into a third-party site using a social network's "Sign in with..." feature or through Single Sign-On (SSO) in enterprise environments.

This model allows users to utilize a single Identity Provider (IdP) to authenticate and access multiple Service Providers (SPs) or Relying Parties (RPs) without needing to create separate accounts for each one.

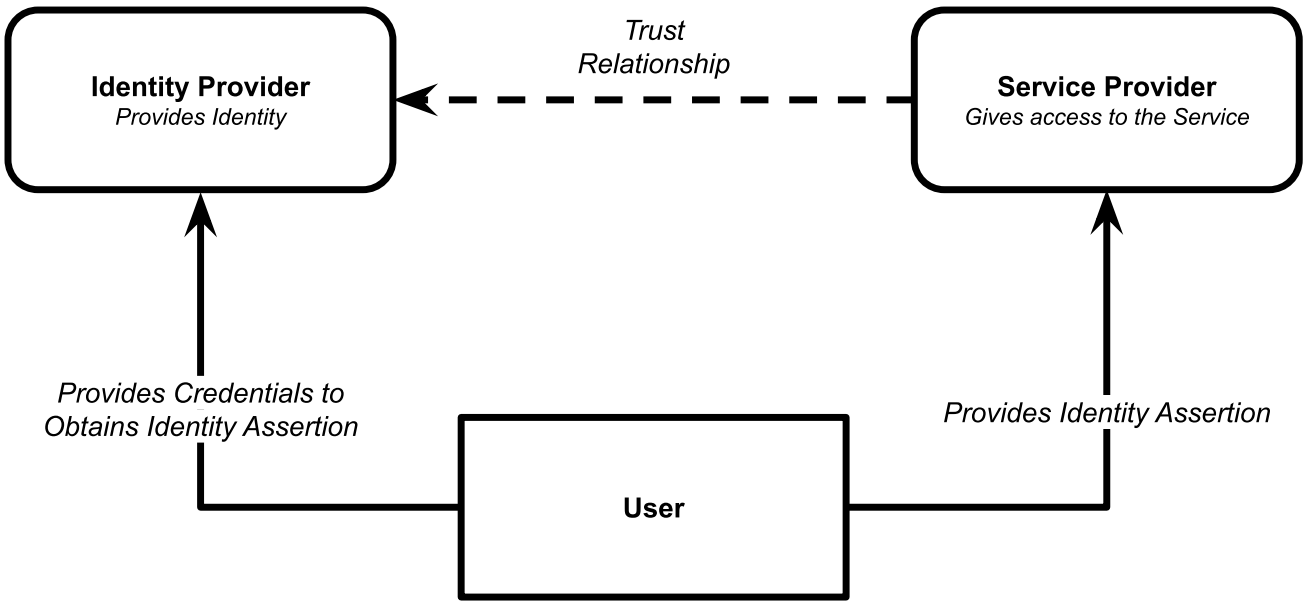

Figure 2 *Federated Identity Management*

Here is the simplified *Data Flow*:

- **Authentication**: The user sends their credentials to the IdP to authenticate.
- **Obtaining Identity Assertions**: The IdP then creates an identity assertion, a verifiable confirmation of the user's identity.
- **Sending Identity Assertions**: The user sends their identity assertion to the SP or RP.
- **Trust and Access**: The SP or the RP, trusting the IdP, accepts the user's Identity Assertion and grants access.

Perspectives:

- **Security**: This model mitigates the user's need to remember multiple passwords and identity fragmentation issues and relieves the need for the SP or RP to manage the authentication aspects.
- **Privacy**: this model still has some implications because the IdP knows what third-party services the user has accessed. Additionally, the technology uses "*third-party (cross-site) cookies that are considered harmful to the web and must be removed*" [third-party-cookies-must-be-removed].
- **Standards**: standards support interoperability between different systems. The most used in this context are OASIS Security Assertion Markup Language (SAML) and OpenID Connect, which underpins OAuth for authorization and different token formats.

> Enabling Federated identity in the Web platform without third-party cookies
> The Federated Identity Community Group was created to resolve these privacy concerns for this model. The Group is working on Federated Credential Management API [FEDCM] and other APIs, such as Login Status API, to implement the Federated Identity Model in the Web Platform. The Federated Identity Working Group also came from this group to proceed with standardization.

§ 3.3. Decentralized identity model

In the decentralized model, also known as the Self-Sovereign Identity (SSI) or three-party model, the user independently administers their identities and is the highest expression of user-centric identity. It is the newest model, and several pilot projects are underway for large-scale implementations.

> NOTE: We will examine the decentralized identity model more closely, as it is the source of new challenges.

§ 3.3.1. Architecture

The decentralized identity model marks a significant shift in architecture. Instead of federated Identity Providers (IdPs) and Service Providers (SPs) or Relying Parties (RPs), the focus now centers on the user.

In this model, the user, also known as *Holder*, *controls* their credentials acquires them from an *Issuer*, stores them in their *wallet*, and presents *them* to a Verifier. Verification activities are mediated by a *Verifiable Data Registry*, containing the necessary information.

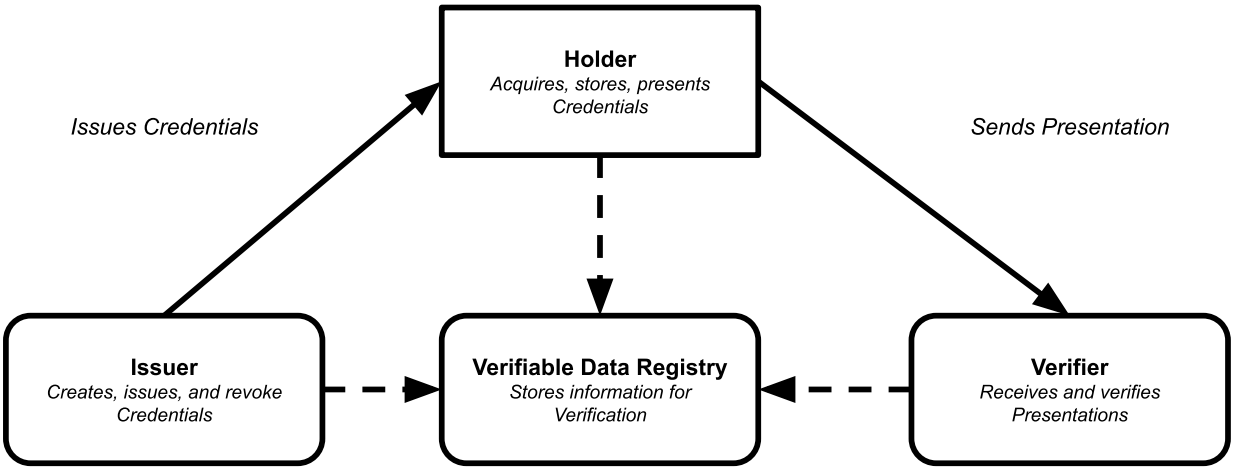

Figure 3 *Decentralized Identity Model, adapted from Verifiable Credentials Data Model (VCDM) [vc-data-model-2.0]*

To best understand the decentralized model and its end-to-end operation, we can refer to the model by the Decentralized Identity Foundation (DIF) [did-faq] build on the Trust Over IP architecture [introduction-toip] [evolution-toip].

This model comprises both technology and governance aspects, sliced into different layers. We will then provide an overview of the various layers, focusing on specific elements related to credentials and identifiers, considered the two pillars of decentralized identities.

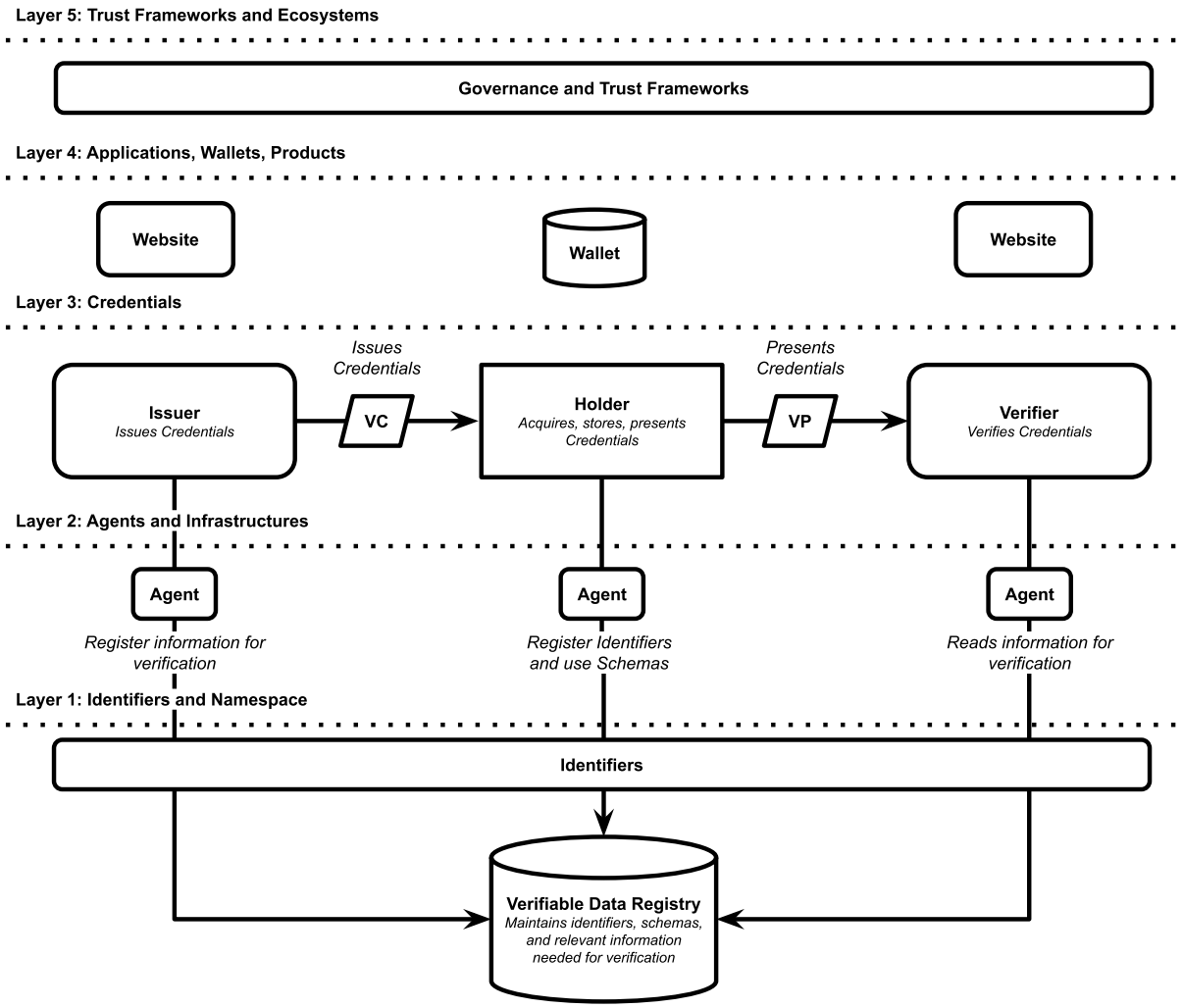

Figure 4 *Decentralized Identity Architecture, inspired and adapted by ToIP [introduction-toip]*

Let us start by looking at the layers.

§ *3.3.1.1. Layer 5: Trust Frameworks and Ecosystems*

At this level, we find compliance and regulation, governance, and trust frameworks, which tell us who we can trust, such as a particular issuer that follows a specific Level of Assurance. These trust elements depend on the context — or domain — of reference. We can have different contexts, such as state, government, and university contexts.

Each context is governed by one or more governance or trust frameworks. For example, for the domain of credentials issued by governments in Europe, we have the EU Digital Wallet, and we can have others related to other states. As well as other domains such as individual organizations, enterprises, or universities. So, a critical issue is interoperability across states.

> NOTE: There are differences between the levels of DIF and the **ToIP Technology Stack**: *Governance* is divided into parallel halves, with specific frameworks for each level.

3.3.1.2. Layer 4: Applications, Wallets, Products

At this level, we find the various applications available to end users:

- **Applications**: These can be Native or Web-based, and it is possible to interact with them differently.
- **Digital Wallets**: These are where the Holder stores their credentials. Just as a physical wallet holds more than just IDs, the digital wallet can store various credentials and information. We can classify the wallets depending on several factors:
  - *Technology*: Wallets can be native applications (e.g., Mobile) or web applications (e.g., Cloud).
  - *Cryptographic Key location*: Custodial (e.g., the key is stored in the Cloud) or Non-Custodial (e.g., the key is stored in a device in possession of the end-user)

  Simplifying, the Wallet structure comprises secure storage and an agent managing interactions.

> NOTE: There are differences between the levels of DIF and with **ToIP Technology Stack**: *Wallets* are at Layer 2. *Layer 4* is for practical applications, which we cover in Use cases.

3.3.1.3. Layer 3: Credential Layer

At this level, the various actors exchange credentials. Let us see what happens using the specific definitions of the W3C Verifiable Credentials Data Model (VCDM) [vc-data-model-2.0].

The actors are:

- The **Issuer** creates and *issues credentials* to the *Holder* and writes the necessary information within the *Verifiable Data Registry*. This can be a trusted third-party entity like governments or universities. In some cases, credentials can be *self-issued* by the user, e.g., to represent informal skills or competencies. This flexibility allows for a broader range of credentials and applications.
- The **Holder** (the *user*), at the heart of this architecture, receives the credentials from the Issuer, stores them in a *Digital Wallet*, and *presents* them to the *Verifier*.

- The **Verifier** receives the presented credentials by the *Holder* and verifies them. This actor is akin to an SP or RP in federated models. This process does not necessarily involve informing the *Issuer*. This decoupling is a key aspect of the decentralized identity model, enhancing privacy and control for the user.

> NOTE: In this model, the definition of a **credential** shifts to a set of *claims* (attributes) linked to *identifiers* controlled by the user. While credentials represent identities, not all claims within a credential are used for identification. They can describe various characteristics, extending the application of credentials beyond mere identification.

The actors exchange:

- **Verifiable Credential (VC)**: When the Issuer sends them to the Holder, who then stores it in their Wallet. The word *Verifiable* refers to the characteristic of a credential (or presentation) as being able to be verified (though cryptographic mechanisms) by a *Verifier*. The addition of technologies, such as digital signatures, makes verifiable credentials more tamper-evident and more trustworthy than their physical counterparts.
    - **Metadata**: of the Credentials, to describe properties such as the *Issuer*, the expiry date and time, a representative image, the *Issuer* public key to use for verification purposes, the revocation mechanism, and so on.
    - **Claim(s)**: one or more assertions where a characteristic of a subject is described (e.g., the subject is a citizen of a certain state, was born in a certain place on a certain day, month, and year, and can drive cars of this type).
    - **Proof(s)**: cryptographic proof of the integrity and the authenticity of the credential, typically via a digital signature. The proof is generated by the Issuer.
- **Verifiable Presentation (VP)**: When the Holder sends a credential to the Verifier, which then verifies it. VC are used to present claims to a Verifier by proving control over credentials that certify them. The basic case is to present the credential as is. However, in many scenarios, the holder may wish to present only a subset of the credential claims to the verifier - this mechanism is called *Selective Disclosure (SD)* - or a combination of information from different credentials. It may contain:
    - **Metadata**: of the Presentation, including the *Issuer* public key to use for verification purposes.
    - **Credential(s)**: information derived or combined from one or more credentials. If *Selective Disclosure* is adopted, no credentials are shown, but only a subset of the credential claims.

- **Proof(s)**: cryptographic proof of the integrity and authenticity of the presentation. The proof is generated by the Holder. It consists in a proof of knowledge of a credential certifying the (dislosed) credential claims. If *Selective Disclosure* is adopted, the proof may be obtained through the use of a cryptographic zero-knowledge proof.

> NOTE: Refer to Ivan Herman's W3C Verifiable Credentials Overview for a comprehensive overview of Verifiable Credentials.

Obviously, the Issuer, the Holder, and the Verifier need a **credential exchange protocol** for VCs and VPs. This is not described in VCDM but is defined by other standards, such as VC API and OpenID4VC.

§ *3.3.1.4. Layer 2: Agent Frameworks and Infrastructure*

At this level, the software responsible for the interaction between the various actors communicates by processing the identifiers in the credentials. Agents retrieve content, resolve it, render it, and facilitate interactions between the various actors and the lower levels.

§ *3.3.1.5. Layer 1: Identifiers and Namespaces*

At this level, we find identifiers and the Verifiable Data Registry (VDR), where referenced information is written, updated, read, and deleted.

As identifiers, we mainly refer to the **Decentralized Identifiers (DIDs)**, a new Uniform Resource Identifier (URI) [RFC3986] type that allows entities and resources to be identified. DIDs, along with Verifiable Credentials, are considered one of the two pillars of decentralized models —

DIDs provide for different methods of referencing resources [did-core], called methods. These methods can rely on various technologies, including blockchains such as Bitcoin or Ethereum, the web, InterPlanetary File System (IPFS), and Domain Name System (DNS) [did-spec-registries], and it is possible to write your method.

Some distinctive properties of DIDs are [did-intro]:

- **Decentralized**: do not depend on centralized registries, identity providers, authorities, etc.
- **Persistent**: once created, it is permanently assigned to the subject.
- **Resolvable**: it is possible to find out a basic set of information on the subject.

- **Cryptographically verifiable**: there is a mechanism to prove identity and ownership cryptographically.

> NOTE: The **ToIP Technology Stack** also includes Identifiers at other layers.

The **Verifiable Data Registry (VDR)** holds the data needed to verify credentials and their status. This can be government databases, distributed ledgers, or other services. By maintaining this information, the VDR, depending on its form, enables verification without direct communication between the *Issuer* and the *Verifier*.

Having concluded this overview of the whole ecosystem of decentralized identities, we can return to focus on the specific level of credentials.

§ 3.3.2. Data Flow

Here is the data flow of credentials from when they are created to when they are revoked.

- **Credential Issuing (CI):**
  1. The *Issuer* requests a certain authentication mechanism from the *Holder*.
  2. After authentication, the *Holder* asks the *Issuer* for the credential or the *Issuer* submits it.
  3. If both parties agree, the *Issuer* sends the credential to the Holder in a specific format.
  4. The *Holder* enters their credential into the *Wallet*.
- **Credential-Presentation (CP)**
  1. The *Holder* requests access to a specific resource or service from the *Verifier*.
  2. The *Verifier* then presents a request for proof to the *Holder*. This can either be done actively (e.g., the Verifier presents a QR code that the Holder has to scan) or passively (e.g., they accessed a web page and were asked to access a credential).
  3. Through the *Wallet*, the holder's user agent determines if there are credentials to generate the required *Proof*.
  4. The *Holder* may use the proof explicitly if they possess it.
  5. The user agent of the *Holder* then prepares the Presentation - which can contain the full credential or part of it- and sends it to the *Verifier*.
- **Credential-Verification (CV)**

1. The user agent of the *Verifier* verifies the *Presentation* (e.g., if the Presentation and the contained Credentials are signed correctly, issued by an *Issuer* they trust, compliant with their policy, the Holder is entitled to hold it, and that it has not been revoked or expired). The revocation check can be done using the methods defined by the specific credential.
2. If the verification is successful, the *Verifier* gives the *Holder* the access.

- **Credential-Revocation (CR)**

  1. The *Issuer* can revoke a credential in various ways.

§ 3.3.3. Security and Privacy

It is interesting to reflect on how this model differs from a security and privacy perspective both from previously described models and from the use of physical identity documents, as credentials can enable this use case:

- **Decentralized vs. Federated Model**: Let us analyze one of the privacy issues of the federated model: whoever provides the identity can track the user. This is one of the threats this model wants to mitigate since the identity is in the user's Wallet, and they use it as they wish.

  Does this guarantee its untraceability? One can presume that the answer is *"it depends"*. It depends on how the architecture is defined and implemented and the technologies used. For example, when we present our credentials to log in, the verifier contacts the issuer directly, asking if the credentials are still valid, and we continue to be traceable.

- **Decentralized vs Physical Document**: If we instead think about the case where I have to send my passport online to open a bank account, to date, the most used method is to send the file with the passport scan. The bank usually sends the file to third-party services, often using Machine Learning systems for analysis. In addition, the file could be reused by someone who has access to it, exposing all our data and not only the one needed.

  Presenting a digital credential, which could also support the submission of a subset of the contained claims, can improve the situation. Still, again, we may encounter the problem of the verifier contacting the issuer for verification, a problem that is rarer when sending the file. However, databases of stolen documents do exist, and a verifier could make a request with the passport ID to verify the status.

> NOTE: Architectural change can solve some issues and generate new ones, so a thorough analysis is necessary.

We can take a step back and understand what privacy properties are needed for digital identity, considering that the higher the level of credential assurance, the more threats can impact the user. Over the years, several proposals have been made to understand the properties of digital identities, such as Kim Cameron's 7 Identity Laws and Ben Laure's Privacy Requirements. Analyzing the latter [selective-disclosure]:

- **Verifiable**: Identities, credentials, and various claims must be verifiable, which is possible through appropriate cryptographic proofs. This is part of the security aspects, which include cryptography.
- **Minimal**: This is a privacy aspect. When we send information to the verifier, the information should be minimized as much as possible. For example, if we have to show that we are of age, it is okay to submit all the credentials or even the specific claim of the date of birth, but simply that I am of age.
- **Unlinkable**: This is another privacy aspect of the minimal issue anyway. Suppose any party involved in the interaction, such as the Issuer, Verifier, or even a third party, can link and correlate the information we sent. In that case, this can be done through various techniques, and privacy is compromised.

So we have several properties, both security and privacy, as a starting point. How can we implement them? First, different credential formats have different privacy and security features [verifiable-credentials-flavors-explained]. We can expand the discussion not only to formats but also to all other components of the architecture, which must be aligned to ensure security and privacy.

Modeling security, privacy, and human rights threats of decentralized credentials

Given the levels of complexity, a comprehensive analysis of threats to privacy, security, and human rights is necessary [human-rights-and-technical-standards].

This is especially important for high-assurance credentials, such as those issued by governments, as highlighted by organizations such as the Electronic Frontier Foundation (EFF) [eff-digital-identification] and Access Now [access-now-whyid].

W3C recognized the need for rights-respecting digital credentials and started a joint Threat Model for Decentralized Identities:

- Technical Architecture Group (TAG)
- Privacy Interest Group (PING)
- Federated Identity Working Group (FedID WG)
- Verifiable Credentials Working Group (VCWG)
- Credentials Community Group (CCG)
- Threat Modeling Community Group (TMCG) (open to all privacy, security, and human rights experts).

Threat Modeling is "*a family of structured, repeatable processes that allows to make rational decisions to secure applications, software, and systems*" [threat-modeling-designing-for-security]. This Threat Model is using different frameworks and toolkits to cover the different threat types, such as:

- **Security**: *STRIDE* (Spoofing, Tampering, Repudiation, Denial of service, Escalation of privileges) [STRIDE], and *Guidelines for Writing RFC Text on Security Considerations* [RFC3552].
- **Privacy**: *LINNDUN* (Linking, Identifying, Non-Repudiation, Detecting, Data Disclosure, Unawareness & Inintervenability, Non-Compliance) [LINDDUN], and *Privacy Considerations for Internet Protocols* [RFC6973].
- **Human Rights**: *Harms Modeling* [harms-modeling], and *Access Now #WhyID* [access-now-whyid].

Other approaches include the Self-Review Questionnaire: Security and Privacy and the *OSSTMM* [OSSTMM-3].

The Threat Model also includes a list of various mitigation techniques, particularly those based on cryptography techniques such as Zero Knowledge Proof (ZKP) and additional methods for

> enabling secure and privacy-preserving technology.

§ 3.3.4. Standards

As noted, VCDM and DID define only certain elements of the architecture. Other SDOs define other elements that are essential for the architecture to function. So, coordination between these entities is necessary to ensure smooth operation. Let us examine the standards involved for the various components needed.

To understand the extent of the various standards, we can refer to Michael Palage's Digital Identity Galaxy.

> NOTE: Not all of the technologies indicated are standard, so they should not be considered normative references or endorsements. Some are drafts, and others have been indicated because, although in an embryonic state, they have interesting features.

This is why several Standards Development Organizations (SDOs) such as the World Wide Web Consortium (W3C), the Internet Engineering Task Force (IETF), the OpenID Foundation (OIDF), and the Decentralized Identity Foundation (DIF) are coordinating to standardize the components and how they should communicate:

- **Data Models:** abstract models for Credentials and Presentation such as the Verifiable Credentials Data Model and mDL in ISO/IEC 18013-5:2021.
- **Identifiers**: DIDs and the DID methods, IndieAuth, WebID, X.509, URLs, or URIs.
- **Encoding Schemas:** JSON, JSON-LD, CBOR, CBOR-LD.
- **Securing Mechanisms:** Each mechanism may or may not support different privacy features or be quantum-resistant:
    - **Enveloped Formats (Credential Formats)**: The proof wraps around the serialization of the credential. JSONs are enveloped using JSON Object Signing and Encryption (JOSE), and we can find JWT, JWS, and JWK here. JOSE is *cryptographically agile* (as it can fit different cryptographic primitives) and can also have Selective Disclosure (SD) with SD-JWT (which uses HMAC). New securing mechanisms are coming up, like SD-BLS (which uses BLS) and ongoing efforts to fit BBS. CBORs are enveloped using CBOR Object Signing and Encryption (COSE). Other formats include ISO mDocs, and SPICE. The mechanism to use VCDM with JOSE/COSE is described in Securing Verifiable Credentials using JOSE and COSE.

    - **Embedded Formats (Signature Algorithms):** The proof is included in the serialization alongside the credentials (e.g., BBS, ECDSA, EdDSA). The mechanism is described in Verifiable Credential Data Integrity 1.0. New securing mechanisms are coming up, like [SD-BLS](https://arxiv.org/abs/2406.19035) (which uses BLS), and ongoing efforts to use BBS.
- **Status Information (Revocation Algorithms)**: *Issuers* can implement several ways to keep the credential's status up to date, such as a Revocation List, a Status List (e.g., W3C Bitstring Status List v1.0, Status Assertions, Token Status List), and Cryptographic Accumulators, etc..
- **Communication Protocols**: for the different phases of Issuance and Presentation such as OID4VCI, OID4VP, SIOPv2, ISO REST's API, and Verifiable Credentials API.

> NOTE: This list is representative. For more detailed information, please refer to the Comparison Matrix.

Mitigating surveillance, censorship, intrusion, and discrimination and ensuring interoperability by standardizing digital credentials in the web platform

It's not easy to manage digital identities. In particular, if they are related to humans, it's important to *give people control over the identifying information about themselves they are presenting in different contexts on the web, and be transparent about it* [design-principles].

Given that a *user agent should help its user present the identity they want in each context they are in and should prevent or support recognition as appropriate* [privacy-principles], the Web Platform Incubator Community Group (WICG), incubated the Digital Credentials API [DIGITAL-IDENTITIES], a browser API to mediate the use of Digital Credentials between websites and wallets, to mitigate different threats to the users and promoting interoperability, and it is already working on the Profile for OpenID4VP.

The interoperability is important: if a service supports only a specific format, it excludes and discriminates against users who use a different format due to their government's decisions rather than their own. Consequently, this limitation affects users and restricts the service's business potential.

This API will follow the *users first, developers second, and browser engines third* principle [design-principles], and meeting the needs of regulations (e.g. eIDAS or Children's Online Privacy Protection Rule (COPPA)) [digital-identity-explainer].

For these reasons, the Federated Identity Working Group—which has an API to integrate federated identities and thus has a close implementation link to decentralized ones—is in a rechartering process to adopt the Digital Credentials API, guided by the Threat Model to make the API secure, privacy-preserving, and rights-respecting.

Moreover, the group's new scope proposal has a broader perspective. It can also use the other data flows of the decentralized identity model to enable all possible use cases through the web platform.

§ 4. Uses cases

The world of Digital Identities is quite broad and has different uses in different industries, where it can enhance the user experience and act as a business enabler.

To imagine these use cases, we can play a game: see what is inside our physical or digital wallets.

For example, the driver's license (and the international one), the passport (and the passport also has visas for entry to other countries, or if you have minor children, they can be in your passport), payment cards, cash, association cards, tickets (e.g., events, concerts, boarding passes), loyalty cards (from hotels, airlines, the grocery store), the university card, the badge to get into the office, medical insurance card and health card, emergency contacts, some receipts, public transportation card, my business card and the business cards of some people I met, the card to get into the gym and the library.

If we extend this concept to include those documents that are often too large to be put inside a physical wallet if not unfolded but which we use during the day, we also have employment contracts, house contracts, utility bills, the papers of our pet (which, if it travels, has a chip and a passport), marriage certificate (for those who are married), a power of attorney to sign the documents of a company, the tax return, bank statements, amateur radio license or other licenses, medical prescriptions, exam results (both medical and college), degree, professional qualifications (e.g., medical doctor, lawyer, psychologist), warranty certificates of the items I bought and much more.

> Although this is only a partial list, it already allows us to make several observations:
>
> - The first is that not every credential is suited to every use case. I cannot generally use a college diploma to cross the border to another country.
> - The second is that the value of a credential increases with its interoperability. The fact that passports are recognized across many countries makes them extremely powerful, including for purposes other than establishing national identity (e.g., for proving age).
> - The third is that credential reuse is often tied to the strength of its subproperties. For example, a utility bill may be used to prove our physical address in a KYC context (because it is tied to the mail system) but may not be sufficient in a KYC context to prove our name or surname.
> - We are not the subjects of some credentials, as in the case of pet travel documents.

Let us go ahead and look over the use cases for those organization-related identities.

§ 4.1. Organizations

We can look at organizations from different aspects. On the one hand, they can benefit from their government-issued digital identity; on the other hand, they can issue identities themselves to better manage their identification and access systems, both for people and for identities of specific services, software, or processes. To top it off, they can leverage people's identities for greater assurance, particularly when distributed worldwide.

§ 4.1.1. Organizational Identity

Organizations can also have a digital identity and related identifiers such as the registration number with the government where it was opened and possibly the VAT number, if not the legal entity identifier. Although the organization has an identity of its own, it operates through individuals who, in the bylaws, have various authorizations, delegations, and signing powers. Therefore, when you do any transaction, such as opening a bank account or a business transaction, you need the organization's and the personal documentation of the various individuals involved. The use of digital identity in a wallet, with delegation managed through Verifiable Credentials, certainly streamlines the various transactions both with governments and suppliers and with customers, particularly for those aspects of global transactions where the trust relationship goes through a digital transaction and the Association of Certified Fraud Examiners (ACFE) estimates that organizations lose 5% of revenue to fraud each year [acfe-occupational-fraud-2024].

§ 4.1.2. Identity and Access Management (IAM)

The IAM market is thriving, with an estimated growth of 43 billion USD in 2029 [statista-identity-and-access-management]. Such systems enable an employee's identification, authentication, and authorization on the organization's platforms according to assigned roles and responsibilities. Decentralized identities enable an additional approach, such as Bring Your Own Identity (BYOI), where users can use their identity to interact with corporate assets and not just for human resource management practices.

§ 4.1.3. Global Workforce

Digital Transformation has been a trend for several years and has played a crucial role, particularly in the Workforce, during the COVID-19 pandemic. The pandemic accelerated a variety of phenomena including the trend to remote work. Because remote work implies fewer geography-based constraints, there will be demands for other forms of identification, and for interoperable credentials, in order to meet the demands of a more mobile workforce.

The fact is that, net of a further trend in the last year of "back to the office", remote workers are estimated to be 67 percent in the technology industry, and this approach is preferred by 91 percent of workers [statista-work-from-home].

In a global context, digital identities can help register employees and contractors by verifying their identities and qualifications, which is particularly challenging for a global workforce.

> NOTE: By using together the identities issued by governments to both people and organizations, it is possible to make hiring processes smoother with benefits for organizations and people often subject to scams. To enable this scenario, it's important to have interoperability at both the technical and governance levels.

§ 4.2. Things

Although applications with identities linked to individuals are the most studied cases and are delicate to handle, identities also find fertile ground in the *supply chain* and *IoT* world, which is decentralized and distributed by nature.

§ 4.2.1. Supply Chain

A particularly common and interesting scenario is the use of identities and the identification of physical assets and other organizations in the supply chain as well as in end-user services:

- **Import-export markets**: the "cost of trade" tends to double the cost of a good when it is exported, creating significant barriers to entry, even for small and medium-sized enterprises (SMEs) [edata-verifiable-credentials-for-cross-border-trade]. Digital Identities for other organizations and goods can support the traceability of the supply chain, especially when there are certifications related to sustainable production.
- **Counterfeit-prone markets**: such as luxury goods. Proving that the physical good has a proper digital identity and demonstrating the ownership of its Digital Twin in the form of a credential issued by the producer can benefit the end-user and mitigate fraud.

Identifying physical goods presents unique challenges, such as associating the physical good with the credential. Some solutions include using barcodes, DNA fingerprinting of agricultural products, and radio frequency identification (RFID).

§ 4.2.2. Energy Devices (IoT)

In "Self-Sovereign Identity" [self-sovereign-identity], we find an interesting pilot project in the **Energy Sector** initiated by the Austrian Power Grid (APG) and Energy Web Foundation (EWF) to enable small and medium-sized devices called Distributed Energetic Resources (DER), to participate in frequency regulation of the national power grid

[distributed-energy-resources-for-frequency-regulation]. This response to the UN's Sustainable Development Goal 7 "Ensure access to affordable, reliable, sustainable and modern energy for all".

The challenge is that the transmission grid must maintain a consistent frequency to function properly. Power plants typically coordinate to adjust the input frequency in response to changes in energy consumption. However, this becomes particularly complex when integrating small and distributed devices.

It is necessary to identify small devices correctly to avoid issues throughout the network. Verifiable Credentials are present within the devices' operating systems to ensure the IAM aspect and DIDs to identify them correctly [energy-web-credentials-overview].

§ 4.2.3. Automotive (IoT)

An interesting use case for **automotive** can be found in "Self-Sovereign Identity - Foundations, Applications, and Potentials of Portable Digital Identities" [ssi-foundation-applications-and-potentials].

A car, identified by the Vehicle Identification Number (VIN), interacts with various entities throughout its lifecycle, including:

- **Manufacturer, vendors and workshops**: Tracking maintenance and service history.
- **Governmental Entities**: Registration and tax payment.
- **Owners and Users**: Ownership verification and usage rights.
- **Road Infrastructure**: Toll payments and other interactions during use.
- **Insurance Companies**: Policy management and claims processing.

It could also be opened and closed directly through the owner's Wallet, making the car a *Verifier* during unlocking and a *Subject* in the owner's wallet.

This illustrates the utility of IoT identities and credentials and their integration with governmental and human identities [self-sovereign-identity]. For example, when buying and selling a used car, several elements must be verified, such as:

- The vehicle's characteristics and history.
- Ownership verification of the seller.
- The buyer's creditworthiness.
- Completion of ownership transfer and insurance paperwork.

> NOTE: The automotive case is particularly interesting. Even though it is a Non-Human Identity, being often used by humans could have serious privacy implications, as is currently the case with insurance black boxes.

§ 4.3. Human identities and governments

Let us return to the initial example and analyze human identities, focusing on those issued by the government. These have the most assurance and thus expose the user to the most security, privacy, and human rights threats.

A government issues a citizen a specific set of credentials for the purpose of identification and to outline their attributes:

- Travel documents (e.g., Passports and Entry Visas)
- Personal licenses (e.g., Driver's Licenses, Amateur radio licenses, Professional licenses, Marriage Licenses)
- Permits (e.g., Residence Permit, Work Permit)
- Registration of vehicles, ships, and other property
- Welfare programs
- Proof of residency
- Proof of age

We will conduct a thorough historical analysis.

§ 4.3.1. Physical Identity

Previously, individuals were known and acknowledged based on their physical attributes and voices, particularly in small, close-knit communities where mutual familiarity prevailed. Within such contexts, establishing trust among acquaintances served as an effective means of identification.

> NOTE: Notably, the assurance of our identity in the social realm often relies on a third party, such as society as a collective entity or directly through government authorities.

§ 4.3.2. Textual Credentials

Up until the **1700s-1800s**, when there was a lack of direct knowledge between the parties (and thus trust), such as when traveling, to identify oneself, it began to be necessary to present credentials issued by a trusted third party, such as a government, in the form of a paper with written information proofed by the authority.

> NOTE: A particularly well-known example of textual credentials is the first driver's license, issued in 1888 to Karl Benz so he could use his experimental car [how-might-driver-licensing]. It was a paper signed by the local authority (a trusted party), which was required after neighbors complained about noise generated by his driving, so not for identifying himself.

These credentials are issued by a trusted entity (e.g., a government), carried or presented by the person in question (e.g., the user with a passport), and then verified by those in charge to authenticate (e.g., the border police) and provide something (e.g., permission to cross the border).

> NOTE: the process used by text credentials has the same structure as that used for digital credentials described above.

Even then, there were security problems: on the one hand, counterfeiting—which was mitigated by using stamps, seals, or special paper—and the use of documents by persons other than the one for whom the document was issued, which was mitigated by including a written description of the owner's facial features to bind them to the document as photography had not yet been invented.

§ 4.3.3. Photographic Credentials

The first documented use of photography for identification was in **1876**, thanks to the photographer William Notman, who had used photographs to identify workers and guests at the Centennial Exposition in Philadelphia [the-world-of-william-notman].

However, government-wide use was introduced only in **1915** after the U.S. government discovered that a German spy was using a U.S. passport because he had physical characteristics similar to those described in written words in the passport and could talk in English [how-have-passport-photos-changed-in-100-years].

> NOTE: The primary purpose of photography is to associate the passport with the individual to whom it was issued. It is essential to ensure that only the legitimate holder of the credential can utilize it.

§ 4.3.4. Machine Readable Credentials

As the technology evolved, the idea was to use machines to help read the documents. This would speed up the verification process. But it was necessary to make the documents easy for machines to read.

To address this, particularly for travel documents, ICAO began working on machine-readable travel documents in **1968**, and in **1980**, it published Document 9303, which contained the specification of a machine-readable code to be printed on documents [doc-9303]. It is the code with many "<"s in our passports and on some ID cards.

As an evolution, in **1998**, Doc 9303 also included biometric information transmitted via *RFID* technology. Nowadays, other machine-readable techniques include barcodes and QR codes.

> NOTE: ISO endorsed this document through ISO/IEC 7501-1, making the role of Standard Development Organizations (SDOs) particularly important for interoperability in this field.

§ 4.3.5. Physical Credentials as Digital Credentials

While these practices have certainly sped up reading and verification in physical contexts - when the verifier has access to the original physical document, they are inefficient if used in a digital context, in particular when the verifier has no access to the original document as the physical credential is scanned or photographed and its file is used.

A classic use of government-issued documents on the Internet and the Web is enrollment in financial services.

The user must indeed provide these documents. At the same time, the financial service provider must verify that they comply with Know Your Customer (KYC) and Anti-Money Laundering (AML) practices to Counter the Financing of Terrorism (CFT).

Then, the user photographs or scans the documents (rendering ineffective the anti-counterfeiting measures inherent in the physical document) and themself (to bind with the document) and sends these files to the financial provider.

Often, the financial provider delegates the process to specialized companies that use Machine Learning and manual control to verify the information.

Thus, we have at least two problems: the entire document is sent to different places, making a data breach more likely, and Machine Learning systems often analyze it. The problem is well described in

"AI & the Web".

Moreover, an additional privacy concern is inherent in this use case - which applies even when the document is used physically. Even if the user uses the document for a specific reason (e.g., proof of address or proof of age), they must send the whole document, thus showing more information than is needed for the specific verification, violating the privacy principle of data minimization.

§ 4.3.6. Pure Digital Credentials

Governments and regulatory bodies have also stepped up to issue digital credentials for citizens. Each government has made its own architectural choices and can offer different services, from centralized or federated authentication to decentralized identities that give citizens a wallet to hold their digital credentials.

Below is a short list with some implementation examples:

- **Canada**: Pan-Canadian Trust Framework™
- **China**: IIFAA Decentralized Trusted Authentication Technical Specification - Part 1: General Requirements.
- **Estonia**: Estonian e-Identity.
- **Europe**: European Digital Identity Architecture and Reference Framework (EUDI-ARF).
- **India**: Aadhaar.
- **Italy**: Italy's Public Digital Identity System (SPID).
- **Nigeria**: Nigeria's eID.
- **Singapore**: Singpass.
- **Spain**: Cl@ve.
- **Switzerland**: Swiss E-ID & Trust Infrastructure
- **United Arab Emirates**: UAE Pass.
- **United States of America**: U.S. DHS on Digital Identities and Mobile Driving Licence (e.g., Maryland, Arizona, Utah, California).

Some governments are doing pilot projects with Decentralized Identities, providing their citizens with Digital Wallets and IDs.

Let us delve into an extensively debated use case requiring a solution: age verification.

The holder has a digital passport in the form of government-issued credentials; these credentials, in their claims, also contain age information. The presentation can be done in different ways, providing different levels of privacy.

- **Full Credential**: It is possible to send the full credential since it also contains the date of birth, from which the verifier can derive the age. However, this doesn't meet the principle of Data Minimization, as I'm sending a lot of other information that can be misused and make us traceable.
- **Selective Disclosure** [selective-disclosure]: Suppose the credential provided supports this privacy feature, which allows us to send individual attributes/claims and hide the others. In that case, we can send only the date of birth, by which the verifier can derive the age. It certainly improves the situation concerning Data Minimization, but it does not solve it totally. To overcome this problem, some credentials have specific attributes with boolean values to present that our age exceeds a certain value (e.g., 16, 18, 21).
- **Range Proof** [range-proofs]: Zero-knowledge range proofs allow a prover to convince a verifier that a secret value lies in a given interval (without showing the credential attribute). If the verifier ask for a specific attribute is within a given range, a range proof-presentation can be sent to the verifier (e.g., the verifier asks us if we are older than 21 years old, we send the result of the computation on the date of birth that proves that our age falls in that range without revealing it).

The problem is that, even in the last two cases, we can present potentially linkable information to us or our issuer, which the verifier can use to make correlations. For example, it is necessary to decouple the signature from the signer and not use the same identifiers in different sessions.

Conversely, the verifier will have to prove that they performed the age verification, further complicating the matter.

Therefore, even in a scenario that may seem trivial, it requires extensive study.

Mitigating the threats at technological and governance levels

In the context of high-assurance credentials, particularly those issued by governments, even the solution to a seemingly simple problem requires a thorough analysis of the impacts these solutions may have on the population.

As we have analyzed, an end-to-end solution requires the conjunction of technological aspects related to the standardization of technologies, their implementation, and their adoption, which is defined by elements of governance that permeate the technological aspects.

In this specific case, we have different stakeholders, such as SDOs, implementers, and governments, who, through regulatory bodies, define the needs, requirements, architectures, and, last but not least, the users impacted by these solutions.

Therefore, it is important for all these stakeholders to work together for joint value creation [stakeholder-relationships-and-responsibilities] and ensure the proper handling of threats to security, privacy, and human rights. Some threats exist at the technology level and can be managed by SDOs and implementers, but governments must manage others at the governance level:

- A centralized system is prone to surveillance. In contrast, a decentralized system with certain technological features and cryptographic methods can mitigate surveillance and respect human rights.
- When a decentralized system is used, issues related to digital wallets arise. On the one hand, it is necessary to balance security and hardware and software requirements that could discriminate. On the other hand, it is important to avoid vendor lock-in and prevent what happened with the Digital Market Act and default browser choice.
- If threats cannot be effectively managed at the technology level, they should be addressed at the governance level. This can involve prohibiting certain uses or removing features that cannot be technically mitigated to reduce the threat.

Active cooperation between governments, SDOs, implementers, and users is essential. SDOs can be a neutral forum to discuss these issues and create value.

§ 5. Acknowledgment

Several individuals contributed to the document. The editor especially thanks Pierre-Antoine Champin, Andrea D'Intino, Giuseppe De Marco, Heather Flanagan, Ivan Herman, Tommaso Innocenti, Ian Jacobs, Philippe Le Hegaret, Coralie Mercier, and Denis Roio.

§ 6. Revision History

- 25 February 2025: Added BBS, Status List (Thanks to Kristina Yasuda)
- 4 November 2024: Clarifying Turst Concept (Thanks to Veronica Cristiano)
- 13 Semptember 2024: Improved definitions of VC and VP (Thanks to Veronica Cristiano), IndieAuth (Thanks to Tantek Çelik)
- 30 August 2024: Added Government Issued use-cases
- 13 August 2024: First publication

§ References

§ Informative References

[A-DICTIONARY-OF-HINDUISM]
Margaret Stutley; James Stutley. *A Dictionary of Hinduism*. 2019.

[ACCESS-NOW-WHYID]
#WhyID. URL: https://www.accessnow.org/campaign/whyid/

[ACFE-OCCUPATIONAL-FRAUD-2024]
Occupational Fraud 2024: A Report To The Nations®. URL: https://legacy.acfe.com/report-to-the-nations/2024/

[ADEM]
Felix Linker; David Basin. *ADEM: An Authentic Digital EMblem*. URL: https://dl.acm.org/doi/10.1145/3576915.3616578

[CAMBRIDGE-DICTIONARY-IDENTITY]
CREDENTIAL | English meaning. URL: https://dictionary.cambridge.org/dictionary/english/credential

[CAMBRIDGE-DICTIONARY-TRUST]
trusT | English meaning. URL: https://dictionary.cambridge.org/dictionary/english/trust

[CONSTRUCTING-AN-IDENTITY]
Constructing an Identity. In: Fan, S., Fielding-Wells, J. (eds) What is Next in Educational Research?. URL: https://doi.org/10.1007/978-94-6300-524-1_8

[DESIGN-PRINCIPLES]
Lea Verou; Martin Thomson; Jeffrey Yasskin. *Web Platform Design Principles*. URL: https://w3ctag.github.io/design-principles/

[DID-CORE]
Manu Sporny; et al. *Decentralized Identifiers (DIDs) v1.0*. URL: https://w3c.github.io/did-core/

[DID-FAQ]
DID FAQ. URL: https://identity.foundation/faq/

[DID-INTRO]
Introduction to Decentralized Identifiers (DID). URL: https://www.youtube.com/watch?v=t8lMCmjPKq4

[DID-SPEC-REGISTRIES]
Manu Sporny; Markus Sabadello. *Decentralized Identifier Extensions*. URL: https://w3c.github.io/did-extensions/

[DIGITAL-CREDENTIALS-THAT-CAN-BE-VERIFIED]
Digital Credentials That Can Be Verified: A Lesson in Terminology. URL: https://sphericalcowconsulting.com/2025/01/20/digital-credentials-that-can-be-verified-a-lesson-in-terminology/

[DIGITAL-IDENTITIES]
Digital Credentials. Draft Community Group Report. URL: https://wicg.github.io/digital-credentials/

[DIGITAL-IDENTITY-EXPLAINER]
Digital Credentials API Explainer. URL: https://github.com/WICG/digital-credentials/blob/main/explainer.md

[DIGITALIZING-REPORT]
Digitalizing the Red Cross, Red Crescent and Red Crystal Emblems: Benefits, Risks, and Possible Solutions. URL: https://dl.acm.org/doi/10.1145/3576915.3616578

[DISCOURSE-ON-THE-METHOD]
Rene Descartes. *Discourse On The Method*. 1637.

[DISTRIBUTED-ENERGY-RESOURCES-FOR-FREQUENCY-REGULATION]
Austrian Power Grid and Energy Web Foundation Launch Proof of Concept to Use Distributed Energy Resources for Frequency Regulation. URL: https://medium.com/energy-web-insights/austrian-power-grid-and-energy-web-foundation-launch-proof-of-concept-to-use-distributed-energy-d9a378f5f5ee

[DOC-9303]
Machine Readable Travel Documents. URL: https://www.icao.int/publications/Documents/9303_p1_cons_en.pdf

[EDATA-VERIFIABLE-CREDENTIALS-FOR-CROSS-BORDER-TRADE]
eDATA Verifiable Credentials for Cross Border Trade. URL: https://unece.org/sites/default/files/2023-08/WhitePaper_VerifiableCredentials-CrossBorderTrade_September2022.pdf

[EFF-DIGITAL-IDENTIFICATION]
Digital Identification Must Be Designed for Privacy and Equity. URL: https://www.eff.org/deeplinks/2020/08/digital-identification-must-be-designed-privacy-and-

equity-10

[ENERGY-WEB-CREDENTIALS-OVERVIEW]
Credentials-Overview. URL: https://energy-web-foundation.gitbook.io/energy-web/ew-dos-technology-components-2023/identity-and-access-management-iam/patterns/credential-lifecycle#credentials-overview

[EVOLUTION-TOIP]
Evolution of the ToIP Stack. URL: https://trustoverip.org/wp-content/uploads/Evolution-of-the-ToIP-Stack-V1.0-2022-11-14.pdf

[FEDCM]
Nicolas Pena Moreno. *Federated Credential Management API*. URL: https://w3c-fedid.github.io/FedCM/

[HARMS-MODELING]
Harms modeling. URL: https://learn.microsoft.com/en-us/azure/architecture/guide/responsible-innovation/harms-modeling/

[HOW-HAVE-PASSPORT-PHOTOS-CHANGED-IN-100-YEARS]
Justin Parkinson. *How have passport photos changed in 100 years?*. URL: https://www.bbc.com/news/magazine-30988833

[HOW-MIGHT-DRIVER-LICENSING]
Scott McLachlan. *How might Driver Licensing and Vehicle Registration evolve if we adopt Autonomous Cars and Digital Identification? [preprint]*. URL: https://www.researchgate.net/publication/358738434_How_might_Driver_Licensing_and_Vehicle_Registration_evolve_if_we_adopt_Autonomous_Cars_and_Digital_Identification

[HUMAN-RIGHTS-AND-TECHNICAL-STANDARDS]
Human rights and technical standard-setting processes for new and emerging digital technologies : report of the Office of the United Nations High Commissioner for Human Rights. URL: https://digitallibrary.un.org/record/4031373?v=pdf

[ICCPR]
International Covenant on Civil and Political Rights. URL: https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

[ID4D-initiative]
Sustainable Development Goals. URL: https://www.worldbank.org/content/dam/Worldbank/Governance/GGP%20ID4D%20flyer.pdf

[IDENTITY-ON-THE-WEB]
Heather Flanagan. *Identity on the Web*. 2024. URL: https://www.w3.org/2024/04/AC/talk/identity

[INTRODUCTION-TOIP]
Introduction to Trust Over IP. URL: https://trustoverip.org/wp-content/uploads/Introduction-to-ToIP-V2.0-2021-11-17.pdf

[ISO-IEC-24760-1]
IT Security and Privacy — A framework for identity management — Part 1: Terminology and concepts. 2019. URL: https://www.iso.org/obp/ui/#iso:std:iso-iec:24760:-1:ed-2:v1:en

[LINDDUN]
LINDDUN: PRIVACY THREAT MODELING. URL: https://linddun.org

[MARRAKESH-TREATY]
Sustainable Development Goals. URL: https://www.wipo.int/marrakesh_treaty

[NIST-SP-800-63-3]
Types of credentials and authenticators. URL: https://doi.org/10.6028/NIST.SP.800-63-3

[NIST-VERIFIABLE-DIGITAL-CREDENTIAL]
Digital Identities: Getting to Know the Verifiable Digital Credential Ecosystem. URL: https://www.nist.gov/blogs/cybersecurity-insights/digital-identities-getting-know-verifiable-digital-credential-ecosystem

[NOBODY-KNOWS-YOU-RE-A-DOG]
Peter Steiner. *On the Internet, Nobody Knows You're a Dog*.

[OSSTMM-3]
Open Source Security Testing Methodology Manual v3. URL: https://www.isecom.org/OSSTMM.3.pdf

[OXFORD-ETYMOLOGY-IDENTITY]
T. F. Hoad. *Identity - The Concise Oxford Dictionary of English Etymology*. 2003. URL: https://www.oxfordreference.com/display/10.1093/acref/9780192830982.001.0001/acref-9780192830982-e-7482

[PASSKEYS-101]
Passkeys 101. URL: https://fidoalliance.org/passkeys/

[PRIVACY-PRINCIPLES]
Robin Berjon; Jeffrey Yasskin. *Privacy Principles*. URL: https://w3ctag.github.io/privacy-principles/

[RANGE-PROOFS]
Miranda Christ; et al. *SoK: Zero-Knowledge Range Proofs*. URL: https://eprint.iacr.org/2024/430

[RFC1321]
R. Rivest. *The MD5 Message-Digest Algorithm*. April 1992. Informational. URL: https://www.rfc-editor.org/rfc/rfc1321

[RFC1945]
T. Berners-Lee; R. Fielding; H. Frystyk. *Hypertext Transfer Protocol -- HTTP/1.0*. May 1996. Informational. URL: https://www.rfc-editor.org/rfc/rfc1945

[RFC2069]
J. Franks; et al. *An Extension to HTTP : Digest Access Authentication*. January 1997. Proposed Standard. URL: https://www.rfc-editor.org/rfc/rfc2069

[RFC2246]
T. Dierks; C. Allen. *The TLS Protocol Version 1.0*. January 1999. Historic. URL: https://www.rfc-editor.org/rfc/rfc2246

[RFC3552]
E. Rescorla; B. Korver. *Guidelines for Writing RFC Text on Security Considerations*. July 2003. Best Current Practice. URL: https://www.rfc-editor.org/rfc/rfc3552

[RFC3986]
T. Berners-Lee; R. Fielding; L. Masinter. *Uniform Resource Identifier (URI): Generic Syntax*. January 2005. Internet Standard. URL: https://www.rfc-editor.org/rfc/rfc3986

[RFC4226]
D. M'Raihi; et al. *HOTP: An HMAC-Based One-Time Password Algorithm*. December 2005. Informational. URL: https://www.rfc-editor.org/rfc/rfc4226

[RFC6238]
D. M'Raihi; et al. *TOTP: Time-Based One-Time Password Algorithm*. May 2011. Informational. URL: https://www.rfc-editor.org/rfc/rfc6238

[RFC6973]
A. Cooper; et al. *Privacy Considerations for Internet Protocols*. July 2013. Informational. URL: https://www.rfc-editor.org/rfc/rfc6973

[SDGS-16]
Sustainable Development Goals. URL: https://sdgs.un.org/goals/goal16#targets_and_indicators

[SECURE-PAYMENT-CONFIRMATION]
Rouslan Solomakhin; Stephen McGruer. *Secure Payment Confirmation*. URL: https://w3c.github.io/secure-payment-confirmation/

[SELECTIVE-DISCLOSURE]
Ben Laurie. *Selective Disclosure (v0.2)*. URL: https://www.links.org/files/selective-disclosure.pdf

[SELF-SOVEREIGN-IDENTITY]
Alex Preukschat; Drummond Reed. *Self-Sovereign Identity*.

[SSI-FOUNDATION-APPLICATIONS-AND-POTENTIALS]
Strüker, Jens; et al. *Self-Sovereign Identity - Foundations, Applications, and Potentials of Portable Digital Identities*. URL: https://www.researchgate.net/publication/354653404_Self-Sovereign_Identity_-_Foundations_Applications_and_Potentials_of_Portable_Digital_Identities

[STAKEHOLDER-RELATIONSHIPS-AND-RESPONSIBILITIES]
Chiara Civera; R. Edward Freeman. *Stakeholder Relationships and Responsibilities: A New Perspective*. URL: https://doi.org/10.4468/2019.1.04civera.freeman

[STATISTA-IDENTITY-AND-ACCESS-MANAGEMENT]
Alexandra Borgeaud. *Identity and Access Management - statistics & facts*. URL: https://www.statista.com/topics/10552/identity-and-access-management/

[STATISTA-WORK-FROM-HOME]
Ahmed Sherif. *Work from home: remote & hybrid work - Statistics & Facts*. URL: https://www.statista.com/topics/6565/work-from-home-and-remote-work/

[STRIDE]
STRIDE model. URL: https://shostack.org/files/microsoft/The-Threats-To-Our-Products.docx

[THE-EVOLVING-LANDSCAPE-OF-NON-HUMAN-IDENTITY]
Heather Flanagan. *The Evolving Landscape of Non-Human Identity*. 2024. URL: https://sphericalcowconsulting.com/2024/04/05/the-evolving-landscape-of-non-human-identity/

[THE-WORLD-OF-WILLIAM-NOTMAN]
Hall, Roger; Gordon Dodds; Stanley Triggs. *The World of William Notman*.

[THIRD-PARTY-COOKIES-MUST-BE-REMOVED]
Amy Guy; Daniel Appelquist; Hadley Beeman. *Third Party Cookies Must Be Removed*. URL: https://www.w3.org/2001/tag/doc/web-without-3p-cookies/

[THREAT-MODELING-DESIGNING-FOR-SECURITY]
Adam Shostack. *Threat Modeling: Designing for Security*.

[THREE-MODELS-OF-DIGITAL-IDENTITY-RELATIONSHIPS]
Timothy Ruff. *Three Models of Digital Identity*. URL: https://medium.com/evernym/the-three-models-of-digital-identity-relationships-ca0727cb5186

[TYPES-OF-CREDENTIALS-AND-AUTHENTICATORS]
Types of credentials and authenticators. URL: https://id4d.worldbank.org/guide/types-credentials-and-authenticators

[UDHR]
Universal Declaration of Human Rights. URL: https://www.un.org/en/universal-declaration-human-rights/

[ULTRA-SOLUTIONS]
Paul Watzlawick. *Ultra-Solutions: How to Fail Most Successfully*.

[UNHCR-digital-identity]
UNHCR Strategy on Digital Identity and Inclusion. URL: https://www.unhcr.org/blogs/wp-content/uploads/sites/48/2018/03/2018-02-Digital-Identity_02.pdf

[VC-DATA-MODEL-2.0]
Manu Sporny; et al. *Verifiable Credentials Data Model v2.0*. URL: https://w3c.github.io/vc-data-model/

[VERIFIABLE-CREDENTIALS-FLAVORS-EXPLAINED]
Kaliya Young. *Verifiable Credentials Flavors Explained*. URL: https://www.lfph.io/wp-content/uploads/2021/02/Verifiable-Credentials-Flavors-Explained.pdf

[WEBAUTHN-2]
Jeff Hodges; et al. *Web Authentication: An API for accessing Public Key Credentials - Level 2*. URL: https://w3c.github.io/webauthn/

[WEBAUTHN-3]
Tim Cappalli; et al. *Web Authentication: An API for accessing Public Key Credentials - Level 3*. URL: https://w3c.github.io/webauthn/

[WHAT-DOES-UBUNTU-REALLY-MEAN]
Nkem Ifejika. *What does ubuntu really mean?*. 2006. URL: https://www.theguardian.com/theguardian/2006/sep/29/features11.g2