Introduction to Digital Credentials

# Start Here

## Welcome

### Introduction

Welcome to the Introduction to Digital Credentials Course!

This free, self-paced, available on-demand, learning portal has been created to introduce and strengthen learner knowledge in digital credentials, including how to deploy privacy enhancing, legally compliant, and interoperable digital credentials in a sustainable manner.

We anticipate and welcome learners from both private and public sectors with varying levels of experience. Ultimately, the goal of this learning portal is to provide interested audiences with a complete view of digital credentials to make well-informed investment decisions or execute successful digital transformation project plans.

The intent of the course is to build foundation knowledge.

**Course Objectives**

By the end of the course, learners will be able to

* Define commonly used terms and concepts used when discussing digital credentials.
* Explain the key legal, operational, technology and privacy issues as well as opportunities related to digital credentials
* Describe the current compliance and interoperability trends in relation to digital credentials
* Describe essential use cases related to verifiable credential management
* Outline an analysis framework optimally suited to generate compliant and interoperable digital credentials use case solutions.

### What to Expect

**Course Details**

Let’s begin by explaining how the course is designed and what to expect.

The course is broken up into seven units. Each of these units will introduce new topics and concepts. Here is a breakdown:

| **Unit** | **Title** |
| --- | --- |
| 1 | Foundations of Digital Credentials |
| 2 | Digital Credential Concepts |
| 3 | Risk, Privacy, and Barriers to Adoption |
| 4 | Ecosystem Models and Verifiable Credentials |
| 5 | Verifiable Credentials |
| 6 | Design Considerations for Digital Identity Solutions |
| 7 | Technologies and Frameworks |

**What to Expect**

You will be required to begin with unit one, which covers the fundamentals. Once you have completed this first unit, you can progress through the remainder of the course in the order of your choosing.

The course will begin with a pre-assessment. This pre-assessment is designed to test the knowledge you are coming in with. Don’t worry about getting the questions correct, just answer to the best of your ability.

Each unit includes various learning resources, such as links to websites, graphics, explainer videos, interviews, and more. Also included are some ungraded opportunities for you to pause and self-assess. This is to help ensure you’ve grasped the major concepts before you move on. You can take these short self-assessments as many times as you’d like. At the end of each unit there is a graded quiz to assess your understanding of the concepts covered. You can take as long as you like to complete these quizzes, and are encouraged to do so. Keep in mind, you only have one attempt.

At the end of the course you will complete a final assessment, like the pre-assessment you took at the beginning of the course, to see if you met the learning objectives and achieved the course goals. The final assessment also allows for unlimited time.

### Need Help

For assistance with the course, please email: education@idlab.org

### Navigation instructions

You likely have noticed that you can only see this Start Here page and Unit 1. This is intentional. We want you to begin with the basics first before moving on. This is helpful for those new to this content and those who might have many years of experience. There are different ways of describing or defining many of the terms we use frequently in the course. It will be important that there be a general understanding of the terms early on.

Once you complete Unit 1, the other 6 Units become available. You simply select the title of the Unit to reveal the subtopics. You will select the first subtopic and make your way through the content using the Next and Previous arrows found both at the top and bottom of the page.

Again, this course is self-paced so you can stop and restart at any time. The system is set up to monitor the pages that you've visited and will indicate a green checkmark beside the previously viewed page. This will help you pick right back up from where you left off last.

IMPORTANT NOTE: For the remaining units to appear, you must review every page of each subtopic in Unit 1 and complete all quizzes. The green check mark lets you know that you have reviewed a page. If there is no green check mark, go back and review that page.

When you arrive at the end of a Unit, you will no longer be able to click the Next button, an indication that you are on the last page. When this happens, simply select Course from the breadcrumbs and from there, you can navigate to the next Unit you would like to view.

If you have any trouble, please feel faree to email: education@idlab.org

## [Pre-Assessment](https://docs.google.com/document/u/0/d/1L7l3TWO2lEP58v1CLr811VAxFImUa5FpuY_7fcUFvnY/edit)

# Unit 1: Foundations of Digital Credentials

## Introduction

Welcome to the Foundations of Digital Credentials unit! So, you are interested in learning more about digital credentials. In order to do that, you must first understand some core foundational concepts and lexicon. This unit introduces you to these terms and concepts.

For instance, what is identity? What are digital identities and credentials? What are verifiable credentials? If you are fumbling to come up with a clear definition in your mind, don’t worry! This unit will cover the basics clearly and concisely. This is crucial so that you have a clear understanding of the terminology that will allow you to grasp the concepts that will be discussed in the upcoming units.

Defining digital credential concepts in a straightforward manner is important because without a common semantic ground on digital credentials, it is more challenging to unlock economic growth and innovation that can be realized with robust digital credentials.

**Learning Objectives**

* Define credentials, identifiers, entities, and attributes.
* Recognize the interconnection between assertion, validation, and verification.
* Examine the concepts of credentials and authenticators.
* Explore the lifecycle of a digital credential.

## Digital Identity and Credentials, Definitions

### Defining Identity and Credentials

Let’s start with the basics. Take a moment to consider what you think identity is. If someone is sitting next to you right now, ask them how they would define identity. Did you both have similar definitions?

In society you have an identity as an individual, a person independent of the paper, plastic or other form of representation. Your identity is *claim of* *who you are*. It’s who you are, how you proceed through the world, how to interact with it. In that interaction with the world, however, we require the capacity to prove things.

These proofs fall into two categories. **Identification**, a proof that you are who you say you are and **credentials** that prove everything from level of education to permission to operate a motor vehicle.

A digital society will require much of the same of what we need today in the physical world. Your identity is a Digital Identity, and a collection of Digital Credentials enable you to make it through your day. Digital credentials are electronic representations of claims to an identity or attributes of that identity. Digital credentials are what you present to make an identity claim, everything from “I am John Doe”, to “I am John Doe, licensed driver from Manitoba”.

With all the incidence of things like identity theft and data breaches, some might ask why they would want a digital identity in the first place. The intuitive, obvious, answer is the convenience that a digital identity affords us. The identity credential you carry around in your wallet has limitations on the number of transactions you can access with it. Your digital credential can theoretically be used with anyone you wish to transact with as long as they have an online presence. As you reach the end of this learning series you will also see that emerging technologies and standards can result in a digital credential that can be more privacy-enhancing and secure than the physical credential you carry with you.

We should also consider who, or what, can have an identity. While we all intuitively understand that a biological person has an identity, identity can be applicable to other things, such as an organization (e.g., a business or more informal association) or a thing (e.g., your refrigerator in a network of household devices). We will call anything that can be identified in a specific context an **entity**.

Now that you have a basic understanding of what identity and credentials are, let’s peel off a few more layers and dig a little deeper into the concepts.

### People, Organizations, and Agents

Identity is the starting point of any relationship. It is at the core of the authenticity of social interactions. Most commonly, it sets the stage for building trust and confidence in ongoing interactions between individuals, and also between government and businesses and the people or organizations they serve. Identity is also dependent on context. Context can be used to establish such things as permissions, status, rights, or to convey characteristics such as a specific competence or achievement. Within an identity or digital credential context, it is critical to be able to distinguish entities from one another so that services can be delivered to the proper recipient (think trusted digital identity) and maintain the integrity of business processes.

We have talked about an entity being anyone or anything that can be identified. Two other specific terms, and their meanings, should be noted. Throughout this learning series we will refer to specific types of entities, namely **persons** and **organizations**.

| Person | Organization |
| --- | --- |
| For our purposes, we will define “**person”** as a human being, alive or deceased. | **Organization** is most often defined as a legally constituted entity such as a registered business or charity. Formally constituted government entities are also included in most definitions of Organization. However, in some instances, organization has been defined somewhat more loosely to include informally constituted entities. In the realm of identity this is rare, but for the purposes of this learning series, you can regard **organization** as potentially including less formally constituted entities, depending on the nature of the program or service requiring secure digital identity. |

Earlier, we spoke about context. It is important to note that a single identifiable entity, let’s say a Person, may have many different contexts and associated digital credentials. John Doe may be “John Doe the taxpayer” and “John Doe, mechanical engineer at ACME Inc.” and “MEGASTRIKER, the online gaming fanatic”. Each of these contexts is likely to have its own distinct issued digital credential for use in each of these contexts.

There are different types of identity and evidence of identity. **Foundational** identity evidence is built on fact-based foundation events that can be used to establish a foundational identity, or more specifically, the existence of a legally recognizable person or organization. Great examples are birth or immigration for persons, and incorporation for a registered business entity. In Canada, foundational identity is in the exclusive domain of the public sector (i.e., provincial birth registries, incorporation registries, etc.). **Contextual** identity is an identity used for a specific purpose, in a specific context. Evidence of identity created in the process of establishing this type of identity can be thought of as **contextual** evidence. Examples of contextual identity and associated evidence include banking credentials, driver’s licence, or even something as basic as a valid social media account.

There is another entity that fulfills a role in some of the processes related to the use of digital credentials. Often a person or organization will appoint someone to act on their behalf. This is particularly true in the case of an organization where a person must execute a transaction on behalf of a business. These are **agents**.

### Meet Johanna

Let’s look at an example of the creation and use of a business digital credential. We will see how an agent is used and some of the issues unique to the use of business credentials.

<<Johanna Explainer video goes here>>

### Credentials, Identifiers, and authenticators

There are a few more important terms used throughout this learning series that we need to define. These will help your understanding of digital credentials and what a digital credential is composed of.

**Defining credentials and authenticators**

The creation of a digital identity most often goes hand-in-hand with the creation of a **credential** and an **authenticator** that facilitate use of that digital identity by a person, or person acting on behalf of an organization.

A **digital credential** is a digital representation of the set of identity and other information that can be uniquely related to the **subject** (e.g., a person or organization) of an identity. An **authenticator** is something under the control of the **subject** of a digital credential that allows them to claim the digital identity as theirs.

**Credentials vs. Authenticators**

Let’s look at an example to help explain how these things might be different.

When looking to gain access to online banking, the bank has a process that asks you to show up at the branch and produce some supporting evidence of your identity. This evidence allows the bank to conduct its own due diligence to decide whether to create a digital credential. With this process completed, the bank will record the information it deems important to associate with a digital identity and create an **identifier** that allows them to uniquely reference the digital identity. This identifier might be something as simple as a unique client number they generate.

The sum total of this recorded information can be thought of as the **credential**. With the creation of the digital identity, the bank then asks you to create a PIN or password to allow you to access online banking. They may also ask you to choose a few challenge questions and answers to help you when trying to gain access to online banking. The password and challenge questions and answers can be thought of as **authenticators**.

**What does a digital credential contain**?

An **identifier** is an indicator that points towards a specific entity. An identifier may be unique in a defined system, like a Social Insurance Number (SIN) in Canada. Other examples of identifiers include driver’s licence numbers and employee numbers. For organizations, similar examples might include corporate registration numbers (unique) or industry classifications (not unique).

An **attribute** is a property, or characteristic, likely to be shared by many entities. Attributes can be professional (e.g., Lawyer, engineer, architect). Attributes can also be affiliations (e.g. employee of a company, alumni member), physical characteristics (e.g., eye colour, sex, height), and more. Finally, attributes can also be in relation to corporate entities, like business size (e.g., small and medium).

**Binding** an identifier or attribute to an entity generally implies that the entity must have a way to legitimately claim the identifier or attribute. Binding is the action of reliably recording the relationship between a set of identifiers or attributes and the person or organization. A digital credential may contain attributes that are created for the sole purpose of supporting binding.

### Assertion, Validation, and Verification

**Assertion**

With the binding identifiers and attributes to an entity (i.e., persons, organization, and entities), and the issuance of a digital credential, a digital credential can be used to make a claim regarding identity. Examples of this may include access to a service (e.g., a business interacting with a government program, or a person conducting a bank transaction, in person or online) or establishing identity in any number of social interaction contexts.

There are a few more concepts that should be defined. Every time an identity is claimed by someone or something, there is an **assertion** of the existence of that identity and the evidence that supports it. Sometimes this can be a **self-assertion**, and sometimes a trusted third party is leveraged to provide a corroborating assertion.

**Validation and verification**

Later when we look at the processes for the creation and use of a digital credential, we will encounter two more important concepts. These are **validation** and **verification**. Let’s look at these using the following example to provide context.

You encounter a police roadside check on your way home and the officer first asks who you are and where you live. You put forward your name and provide your driver’s licence as proof. At this point you have **self-asserted** your identity and supplied supporting credentials. The officer then returns to their car with your licence and consults the Provincial driver registry to further ensure that you are who you claim to be and the claim is accurate. This secondary check tells the officer that the driver’s licence number exists and a trusted third party (i.e. the driver’s licence bureau) has gone through its own process of verifying the existence of your identity.

The officer has followed some important processes during this interaction.

1. There was a **validation** of the attributes and identifiers used to support the identity claim that your credential represents. **Validation** is the process of *confirming the accuracy of the information presented*. In this case, the name you claimed was checked against the licence. Approximate age and other attributes available on the licence have also been checked to confirm the accuracy of the information presented.
2. **Verification** is the process of *confirming that the identity claimed uniquely belongs to the entity claiming it* (in this case, you). The officer performed an initial verification by comparing the picture on your licence to you, believing that a person’s face is relatively unique. A secondary verification was done when the officer consulted the provincial driver’s licence bureau to ensure the evidence presented was valid, and by extension, they gained the knowledge that a trusted third party had also done their own validation and verification process before issuing the driving licence.

These validation and verification efforts allowed the officer to accept the assertion of identity, as represented by the credential.

### Meet Martin

The following video will dive into a few of these fundamental concepts: identifiers, attributes, identity, self-assertion, validation, and verification. Objective identity, or identity established by binding identifiers and attributes to a person/entity, is also a key concept.

As outlined, identity can apply to many different types of entities. Some of these concepts are illustrated while following *Martin* around during a typical day.

<<Martin Explainer video goes here>>

### Check Your Understanding

Let’s pause a moment and ensure you have grasped the concepts we have covered so far. In this activity, select the correct term to match the listed definition. This activity is not timed, so feel free to take your time completing it.

1. \_\_\_\_\_\_\_\_\_\_\_ prove everything from level of education to permission to operate a motor vehicle.
   1. \*Credentials
   2. Identifiers
   3. Authenticators
   4. Attributes
2. \_\_\_\_\_\_\_\_\_\_\_ are electronic representations of claims to an identity or attributes of that identity
   1. Identifiers
   2. Authenticators
   3. Attributes
   4. \*Digital credentials
3. We call anything that can be identified in a specific context \_\_\_\_\_\_\_\_\_\_\_
   1. a credential
   2. \*an entity
   3. a person
   4. An agent
4. \_\_\_\_\_\_\_\_\_ are appointed to act on behalf of an organization.
   1. Credentials
   2. Entities
   3. Persons
   4. \*Agents
5. \_\_\_\_\_\_\_\_\_\_\_ is something under the control of the subject of a digital credential that allows them to claim the digital identity as theirs.
   1. Identifier
   2. \*Authenticator
   3. Attribute
   4. Digital credential
6. An \_\_\_\_\_\_\_\_\_ allows those, like the bank, to uniquely reference the digital identity.
   1. \*Identifier
   2. Attribute
   3. Binding
   4. Subject
7. A digital credential contains all but which of the following?
   1. Identifier
   2. Attribute
   3. Binding
   4. \*Subject
8. Every time an identity is claimed by someone or something, there is a(n) \_\_\_\_\_\_\_\_.
   1. \*Assertion
   2. Binding
   3. Attribute
   4. Identifier
9. \_\_\_\_\_\_\_\_\_ is the process of confirming the accuracy of the information presented.
   1. Binding
   2. \*Validation
   3. Self-Assertion
   4. Verification
10. \_\_\_\_\_\_\_\_\_\_ is the process of confirming that the identity claimed uniquely belongs to the entity claiming it.
    1. Binding
    2. Validation
    3. Self-Assertion
    4. \*Verification

## Creating a Digital Credential

### Digital Credential Lifecycle

Next, let’s have a look at the lifecycle of a digital credential from its creation to its “death”. Along the way, we introduce a few more concepts related to digital credentials.

For those of you more exposed to digital credentials and the associated standards for secure online service delivery, there is an overwhelming amount of detail on process and definitions of the components of digital credential creation and usage. We will use a more simplified approach to communicate key concepts.

At a high level, the lifecycle of a digital credential consists of three common sense phases from the initial existence of an identity to its use as expressed with a digital credential. These are:

1. The initial existence of an identity or an identifiable **entity** - This may be by virtue of someone being born, or a business being registered. Essentially, this is the coming into this world of someone, or something, to which an identity can be ascribed. This is not yet a digital identity.
2. Creation and issuance of a digital credential - This is called **issuance** or **enrollment**. Issuance consists of the processes required to create a digital credential. This credential is the foundation of enabling an identity claim.
3. Usage of a digital credential - We will use the term **authentication**. Authentication is often thought of as the process of supplying an **authenticator** to *get logged on*. Our intent here is to have authentication encompass the end-to-end process of verifying a digital credential for the purposes of gaining access and permission to conduct a transaction.

In addition to the phases in the lifecycle identified above, and depending on the governance and process rules in place pertaining to the digital credential, a digital credential may exist in a number of other states. For instance, a digital credential may be revoked and rendered unusable.

### The Process of Creating a Digital Credential

There are numerous approaches to creating a digital credential, and those processes will vary depending on the needs and preferences of the creator of a digital credential. Some methods may be dependent on technology or business process preferences. As well, the level of confidence required when relying on the digital credential will significantly affect the methods used. However, in all cases there are some common characteristics such as:

* the assertion of identity
* the production of evidence
* examination of evidence
* the creation of credentials

**Creating a digital credential (issuance)**

Earlier, we defined **issuance** as the set of processes required to issue a digital credential. Issuance, as used here, consists of several distinct processes that we will take a closer look at.

Note that before issuance can be undertaken, the organization responsible for creating a digital credential (let’s call them the **issuer**) must first formalize its process consistent with the intended usage of the created digital credential. This includes asking questions like, “what evidence will I accept?”, “from whom will I accept it?”, and “what is my process for validating and verifying this evidence?”. This is important to ensure that the enrollment process aligns well with the intended usage and does not expose either the presenter of a digital credential (the person or organization to whom the digital credential is linked) or the acceptor of a digital credential (the person or organization relying on the digital credential for service provision) to any undue risk.

The specific activities and level of due diligence will vary significantly depending on intended use. For example, a digital credential created for the purposes of social media or online gaming has significantly different validation and verification processes than one created for the purposes of conducting online financial transactions.

**Issuance in Action**

With the process defined, let’s have a look at its component pieces in action. Earlier, we identified four basic steps in the issuance process. Let’s have a closer look at those and some of the methods used, again, dependent on context and intended use for the digital credential.

Here is an illustration of issuance in action. We'll cover each of these 4 stages one by one:

[authentication cartoon here](https://docs.google.com/presentation/d/1M1405CpKI1wqggJObbdJMJajnGSdEAwK76wgU3MEsZ8/edit#slide=id.gc33538400f_0_0)

1. **The assertion of a claim**

The process begins with a basic assertion of a claim by the person or organization wishing to have a digital credential established. This may be as basic as “I want to be MEGASTRIKER the online gaming fanatic”, or something more precise like “I am Jane Doe of Appleseed Terrace in Halifax, and I want to file my taxes online”. Put simply, there should be a stated intent by a person or organization to have a “real-world” identity, that they initially provide a self-assertion of ownership of, be reflected as a digital credential.

1. **The production of evidence**

Based on issuer-defined process, evidence of the asserted identity will be required. The entity making the claim(s) must produce evidence to support those claims. At this stage, the issuer goes through the processes they deem necessary to assure themselves that the evidence is complete and appears to come from acceptable sources.

In practice, this may include any or all self-assertions from the subject of the proposed digital credential (lowest levels of assurance), production of evidence in the subject’s control (e.g., driver’s licence, birth certificate, passport), and/or consent from the subject to consult with other trusted issuers of digital credentials.

1. **Examination of evidence**

In this phase of issuance, the evidence accepted is evaluated to determine if a digital credential can be created. There are many key elements to this examination that should be identified, perhaps by the questions they answer:

- “Is the evidence presented accurate?”. This is **validation** as we defined it earlier. This process can take many forms. For digital credentials intended for use with lower levels of confidence, this may simply be based on self-assertions and ensuring some level of consistency in the evidence presented. However, for the instances we want most to explore, those requiring higher levels of assurance, the process typically includes ensuring that:

- all user claims match the information recorded for any instances of the evidence presented (e.g., if there is a claim of being 40 years old, does the birth date on a submitted passport agree with that claim?).

- the evidence presented originates from the originating source and has not been altered. In lower assurance level instances, it may be deemed sufficient that evidence is examined by a trained examiner. For higher levels of assurance, consultation with the issuing authority is often required.

- validation, if it includes digital validation with another issuer, is subject to appropriate technological methods to ensure that communication between issuers is tamper-proof and verifiable.

- “Does this evidence relate to the subject?”. This is **verification** as we defined it earlier. The same methods are employed as used in **validation**. Beyond assuring themselves of the accuracy of evidence presented, the issuer must verify that the information or identifiers presented as evidence can be related *uniquely* to the person or organization asking for creation of a digital credential.

- “Based on issuer policy and evidence presented, can I create a digital credential that will resolve to a unique entity?”. This is called **resolution**. Resolution is the process of establishing that the subject of the digital credential can be described in a way that is unique within the set of digital credentials issued.

1. **The creation of a credential**

The final step is the creation of the digital credential that facilitates usage of a digital identity - With successful examination of evidence, the digital credential can be created. Earlier, we defined two terms that will be important as we look at digital identity creation and downstream use. These are **credential** (the sum total claim information and identifiers recorded for the purposes of digital credential) and **authenticator** (a physical or digital artefact used most often to facilitate authentication).

**Using a digital credential**

Now let’s look at a digital credential in action. During **issuance** we create a digital **credential** and an **authenticator**. The digital credential is ready for use, which we have defined as **authentication**.

Let’s explore an example of use of identity with some elements of claims contained in a digital credential.

* At the airport, you check in and get your boarding pass, and you make your way to the boarding area.
* Before being allowed into the boarding area, you are asked for your boarding pass and a government issued ID (you use your passport). The officer checks that the boarding pass information (name, etc.) matches the passport [**validation**] and that the picture in the passport looks like you [**verification**].
* In addition, a scanner reads the electronic information embedded in the passport and displays it for the officer, which assures the officer that the passport has not been tampered with **[verification**].
* Also, depending on the airport and country you are in, there may be a system-to-system secure interaction with the passport office to check if the passport is currently valid [**verification**].

The record at the passport office is the complete **credential**. Some or all of the credential information may have been included in the printed and electronic information embedded in the passport, and the physical passport itself served as an **authenticator**.

### More on Creating a Digital Credential

Finally, a brief introduction to some additional terms that we will use throughout this learning series.

There are different types of credentials and evidence of claims. Foundational evidence is built on fact-based foundation events that can be used to establish a **foundational** credential. Great examples are birth or immigration for people, and the incorporation for a registered business entity. **Contextual** digital credentials are used for a specific purpose, in a specific context. Examples of contextual credentials and associated evidence include banking credentials, driver’s licence, or even something as basic as a valid social media account.

Finally, in later sections of this learning series, we delve into risk associated with use of a digital credential, confidence in a credential, and **levels of assurance**. Intuitively, we understand that using someone’s social media credential gives less confidence that someone is who they claim to be, especially when compared to a valid, government-issued, driver’s licence. Typically, there are formally defined levels of assurance that serve as indicators of the degree of confidence that one can have in a digital credential. This helps the creators and consumers of a digital credential define the **trusted providers** of credentials appropriate to the context of the electronic service they deliver.

### Meet Susan

Let’s try to tie all of this together by illustrating the lifecycle of a digital credential, and some of our defined concepts, in a scenario where a business wishes to register for online tax filing using their accountant as an **agent**. The **issuance** will rely on both **foundational** and **contextual** evidence in a context that requires a relatively high **level of assurance**.

<<Susan Explainer video goes here>>

### Check Your Understanding

Let’s pause a moment and ensure you have grasped the concepts we have covered so far. In this activity, select the correct term to match the listed definition. This activity is not timed, so feel free to take your time completing it.

1. The lifecycle of a digital identity consists of \_\_\_\_ common sense phases from the initial existence of an identity to its use as expressed with a digital credential
   1. One
   2. Two
   3. \*Three
   4. Four
2. There are numerous approaches to creating a digital credential, and those processes will vary depending on the needs and preferences of the creator of a digital credential.
   1. \*True
   2. False
3. There are \_\_\_ basic steps in the issuance process
   1. One
   2. Two
   3. Three
   4. \*Four
4. The issuance process begins with
   1. The examination of evidence
   2. \*The assertion of a claim
   3. The production of evidence
   4. The creation of a credential
5. The final step of the issuance process is
   1. The examination of evidence
   2. The assertion of a claim
   3. The production of evidence
   4. \*The creation of a credential
6. The digital credential is often used for
   1. \*authentication.
   2. A credential
   3. Issuance
   4. Verification
7. Examples of contextual credentials and associated evidence include banking credentials, driver’s licence.
   1. \*True
   2. False
8. “Is the evidence presented accurate?” This is an example of:
   1. Issuance
   2. verification
   3. \*validation
   4. None of the above

## Interviews with Experts

### Interview with Patrick Drolet

We are very happy to be able to draw upon some of the recognized experts in the Canadian Digital Identity landscape to help us in this educational series. In this short interview we speak with Patrick Drolet, VP of Operations and Product Strategy for Notarius, about validation, verification and some of the pressing issues related to digital credentials that we will be exploring in more detail as we progress along our learning journey. Patrick identifies some of the key barriers to digital credential adoption and usage, and some of the exciting developments that will help address these barriers.

<<Patrick Drolet interview goes here>>

## Conclusion

We hope this introduction to the world of digital credentials will provide a foundation for the learning units to come. Certainly it will help with some of the terminology you hear used when people talk about digital credentials.

This introduction touches on the key components of digital credentials and discusses some of the key terms in a complex topic area. In the learning units to come, we introduce concepts that build on the terms introduced here to understand how digital credentials are created, managed, and used.

## Unit 1 Quiz

You have one attempt to take this nineteen (19) question unit quiz. This quiz is untimed, so take your time to carefully review the options.

1. A(n) \_\_\_\_\_\_\_\_\_\_ is an indicator that points towards a specific person. It may be unique in a defined system, for example, a Social Insurance Number (SIN) in Canada.
   1. (Identifier)
   2. Attribute
   3. Identity
   4. Validation
2. A(n) \_\_\_\_\_\_\_\_\_\_ is a property likely to be shared by many persons. They can be professional (e.g. Lawyer or engineer), be affiliations (e.g. employee of a company, alumni member), physical characteristics (e.g. eye colour, sex, height), or be in relation to corporate size (e.g. “Small and Medium Businesses”).
   1. Identifier
   2. (Attribute)
   3. Identity
   4. Validation
3. A(n) \_\_\_\_\_\_\_\_\_\_ is a representation of who you claim to be and who you are
   1. Authenticator
   2. Enrollment
   3. (Identity)
   4. Identifier
4. Validation confirms the accuracy of information presented, while verification ensures it belongs to the entity to whom the identity assertion applies.
   1. (True)
   2. False
5. Identity characteristics may be found in a \_\_\_\_\_\_\_\_\_\_\_\_\_\_
   1. (credential)
   2. level of assurance
   3. verification
   4. validation
6. Making sure that all identity evidence presented is consistent is part of \_\_\_\_\_\_\_\_\_\_\_.
   1. Authentication
   2. Resolution
   3. (validation)
   4. Possession
7. When the border services agent checks the picture on your passport to make sure it looks like you, this is an example of \_\_\_\_\_\_\_\_\_\_\_
   1. (verification)
   2. level of assurance
   3. resolution
   4. identifying
8. Your username is an example of a(n) \_\_\_\_\_\_\_\_\_\_\_\_\_
   1. (identifier)
   2. enrollment
   3. authenticator
   4. credential
9. When you tell someone your name, this is called an authenticator
   1. True
   2. (false)
10. Identity evidence that is not foundational is called \_\_\_\_\_\_\_\_\_\_\_ identity evidence.
    1. (contextual)
    2. possession
    3. authentic
    4. It is always foundational
11. Phase one of the lifecycle of digital credential is:
    1. Creation and issuance of a digital credential (issuance or enrollment)
    2. Usage of a digital credential (authentication).
    3. \*The initial existence of an identity (identifiable entity)
    4. The termination of a digital credential (death)
12. Phase two of the lifecycle of a digital credential is:
    1. \*Creation and issuance of a digital credential (issuance or enrollment)
    2. Usage of a digital credential (authentication).
    3. The initial existence of an identity (identifiable entity)
    4. The termination of a digital credential (death)
13. Phase three of the lifecycle of a digital credential is:
    1. Creation and issuance of a digital credential (issuance or enrollment)
    2. \*Usage of a digital credential (authentication).
    3. The initial existence of an identity (identifiable entity)
    4. The termination of a digital credential (death)
14. Note that before issuance can be undertaken, the organization responsible for creating a digital credential must first formalize its process consistent with the intended usage of the created digital credential. This includes asking questions like, “what evidence will I accept?”
    1. \*True
    2. False
15. Announcing your name and location is typically part of which step in the issuance process?
    1. The examination of evidence
    2. \*The assertion of a claim
    3. The creation of a credential
    4. The production of evidence
16. Examination of identity claim evidence to ensure that the evidence is complete and appears to come from acceptable sources is typically done during what stage of the credential issuance process?
    1. The examination of evidence
    2. The assertion of a claim
    3. The creation of a credential
    4. \*The production of evidence
17. “Is the evidence presented accurate?”, “Does this evidence relate to the subject?”, or “Based on issuer policy and evidence presented, can I create a digital credential that will resolve to a unique entity?” are questions that are typically asked during which phase of the issuance process?
    1. \*The examination of evidence
    2. The assertion of a claim
    3. The creation of a credential
    4. The production of evidence
18. This final step of the issuance process facilitates usage of a digital identity
    1. The examination of evidence
    2. The assertion of a claim
    3. \*The creation of a credential
    4. The production of evidence
19. There is only one type of credential and evidence of claims
    1. True
    2. \*False

# Unit 2: Digital Credential Concepts

## Introduction

In the previous learning unit, we defined some of the fundamental terms used when exploring the world of digital credentials. In this unit, we will define some of the key concepts and terminology used when we look at the design of the systems and processes used to create and exchange digital credentials.

**Learning Objectives**

* Examine authentication factors and multi-factor
* Learn about key digital credential concepts

## Authentication Factors and Multi-Factor

### What are authenticators?

Earlier, we defined an authenticator as something under the control of the **subject** of a digital credential that allows them to claim the digital credential as theirs. What are these? What do they look like?

An authenticator can be:

* Something you know. The most common among these are passwords, PINs, or even the answers to pre-configured challenge questions.
* Something you have. Examples of these include a smart card or access card, your smart phone, or other type of physical token used to gain access to something.
* Something you are. Typically, this is a biometric characteristic, like a fingerprint or retinal scan.

Recently, you may have heard the term two-factor, or multi-factor, authentication. More and more online service providers are implementing processes that demand more than one authenticator to provide an additional level of security. An example of this is the use of your phone or email account to send you a one-time PIN to be used to complete logon with the service provider. In this scenario, you provide your password (something you know) and are then informed that a one-time PIN has been sent to your email address. You retrieve the PIN, enter it, and are then granted access. In effect, this combines an additional something you know (the PIN) with something you have (your email account).

These authentication factors, or authenticators are often alternatively classified as:

* knowledge factors (i.e., something you know)
* possession factors (i.e., something you have)
* inherence factors (i.e., something you are)

### Meet Natalie

Let’s have a look at authentication in action again. The video below takes us through a process to access your tax account using a trusted identity provider, your bank, to provide access to the tax department.

<<Natalie Explainer video goes here>>

## Important Digital Credential Concepts

### Introduction

The terms that follow define a number of key concepts that are important in user-centric methods for the issuance and use of digital credentials that are privacy enhancing, under user control, and are more secure. In this learning unit we will briefly define these terms and explore them in more detail when we look at some of the process and technology approaches to managing digital credentials.

### Verifiable Credentials

At the simplest level, digital credentials are nothing more than the electronic equivalent of physical credentials that we already use today - credit cards, passports, driver’s licences and things like qualifications and awards. Verifiable credentials, as we will describe them in this learning series, imply a specific model for issuance and use of a digital credential. We will explore this in more detail in the learning units to follow.

The [W3C](https://www.w3.org/TR/vc-data-model/) defines verifiable credentials as [*a mechanism to express credentials on the Web in a way that is cryptographically secure, privacy respecting, and machine verifiable*](https://www.w3.org/TR/vc-data-model/). Verifiable credentials can be used to establish trust between parties by using a set of tamper-evident claims and metadata that cryptographically proves the identity of the Holder and its Issuer. More importantly, by using this approach, users can keep their data and simply share the needed information in the form of a verified credential with another party whenever they receive a request. The benefits and advantages created with verifiable credentials, are that the credential provides cryptographic proof that the document is authentic, the information has not been tampered with, and a method to strongly authenticate the Issuer without requiring the Issuer to be part of the exchange.

### Decentralized Identifiers

When we define verifiable credentials and the high-level characteristics of the ecosystem models for the issuance and use of a verifiable credential, we note that the credential is under the control of the Holder of that credential and its use need not involve the Issuer of that credential in any way. To accomplish this, there must be a method that enables cryptographic verification and proof of authenticity of a verifiable credential, without having to consult the issuer of that digital credential. These two important characteristics (i.e., credential control by the Holder and usage of a credential without Issuer consultation) have led to the development of models for digital credential management that are decentralized - credential ownership and storage under the direct control of the individuals to whom the digital credentials are issued, and elimination of the need for consultation with a centralized authority when a credential is used.

This created the need for Verifiers of a verifiable credential, to be able to understand how to authenticate a credential and its Holder, and assure themselves of the origin of a credential. Decentralized Identifiers (DID) are globally unique identifiers that point to DID documents that contain the public keys, and identify the methods that will be required to validate the authenticity of a verifiable credential.

### Distributed Ledger

An important component of decentralized models is the component of the system where DID documents and other broadly available information required for verifying a digital credential is stored. This may be any consensually shared database, synchronized and accessible across multiple sites. There is no prescribed database format or technology required for a distributed ledger, simply that it must be broadly available within the ecosystem in which a digital credential is issued and used. However, most often, in globally available digital identity systems, we see these distributed ledgers being implemented using blockchain technology.

### Check Your Understanding

Let’s pause a moment and ensure you have grasped the concepts we have covered so far. In this activity, select the correct term to match the listed definition. This activity is not timed, so feel free to take your time completing it.

1. \_\_\_\_\_\_\_ can be something you know, something you have, or something you are.
   1. Verifiable credentials
   2. Two factor or multi-factor authentication
   3. \*Authenticator
   4. Distributed ledger
   5. Decentralized identifiers
2. An example of this is the use of your phone or email account to send you a one-time PIN to be used to complete logon with the service provider.
   1. Verifiable credentials
   2. \*Two factor or multi-factor authentication
   3. Authenticator
   4. Distributed ledger
   5. Decentralized identifiers
3. \_\_\_\_\_\_\_\_\_ are a mechanism to express credentials on the Web in a way that is cryptographically secure, privacy respecting, and machine verifiable.
   1. \*Verifiable credentials
   2. Two factor or multi-factor authentication
   3. Authenticator
   4. Distributed ledger
   5. Decentralized identifiers
4. \_\_\_\_\_\_\_\_\_\_are globally unique identifiers that point to DID documents that contain the public keys, and identify the methods that will be required to validate the authenticity of a verifiable credential.
   1. Verifiable credentials
   2. Two factor or multi-factor authentication
   3. Authenticator
   4. Distributed ledger
   5. \*Decentralized identifiers
5. There is no prescribed database format or technology required for a \_\_\_\_\_\_\_\_\_\_, simply that it must be broadly available within the ecosystem in which a digital credential is issued and used.
   1. Verifiable credentials
   2. Two factor or multi-factor authentication
   3. Authenticator
   4. \*Distributed ledger
   5. Decentralized identifiers

### Digital Wallets

A digital wallet is a piece of technology designed to hold your digital credentials. It is important to note that digital wallets used for digital credentials differ from the more purpose-built wallets designed for specific financial purposes (cryptocurrency, payment systems such as Apple Pay or Google Pay, etc.). A digital wallet enables the Holder of a digital credential to interact with digital credential Issuers or Verifiers to exchange credentials in a trusted manner.

### Self-Sovereign Identity

Self-sovereign identity (SSI) is a model for digital credentials that has a number of key concepts that create a privacy-respecting, user-centric, approach to digital credential issuance and use. When you think of the physical credentials you carry with you, the Holder of the credential decides who to share the credential with and for what purpose. With the existence of standardized ways to to express a credential (verifiable credentials), standardized approaches to enabling use of a digital credential (DID and distributed ledgers), and user controlled digital credential storage (digital wallets), it is possible to have a model that sees the user in control of their digital credential.

Some of the features of SSI include direct and sole user control over digital credentials, the ability to decide what to share and one what basis on a case-by-case basis, and the ability to use a verifiable credential without having to consult with the issuer of that credential to verify its authenticity.

In later learning units we explore SSI in more detail.

### Selective Disclosure

Extending the SSI model, there is a concept of selective disclosure that sees that only the absolute minimum information required is shared with a credential verifier. An important element of enhanced privacy protection, and many of the privacy laws in effect, is limiting the personal information shared to only that which is required for the transaction to be undertaken.

The concept of selective disclosure when applied to the use of digital credentials is that users should be able to choose what and how much they share on a case-by-case basis. The availability of tools and techniques that enable SSI (verifiable credentials, distributed identifiers, digital identity wallets, etc.) provide a basis for extending the capability of digital wallets and the tools used by verifiers receiving digital credentials to ask for and share only those pieces of information required for a specific transaction.

Looking at a real-world example, when a person provides their driver’s licence as proof of age, the verifier of a physical driver licence credential also gets to see the address of the credential provider (or Holder). This information is not required to prove age and represents a contravention of privacy principles. With selective disclosure, using advanced cryptographic techniques, the verifier receives only the birthdate from the digital credential.

### Zero-Knowledge Proof

Zero-knowledge proof (ZKP) extends the concept of SSI even further, providing methods to prove possession or knowledge of a piece of information without disclosing the actual value of that information. The examples used in many explanations of ZKP are proving that your birthdate is greater than a certain date (e.g., “I am over the age of 18”) or that you have in excess of a certain amount in a bank account, without revealing the exact amount in the account or the specific date of birth.

ZKP relies on advanced public key cryptography, computations applied to protected information, and digital signature methods to create a cryptographic proof of knowledge of information without sharing the value of that piece of information. In a subsequent learning unit, we expand on ZKP and how it works. In addition to the types of examples cited above, ZKP holds some promise to deliver “password-less” authentication, allowing a user to prove possession of a secret without sharing that secret (i.e., “I can prove I have the issued password and it came from the issuer, but don’t need to send it to you and expose it to malicious actors on the internet”).

### Check Your Understanding

Let’s pause a moment and ensure you have grasped the concepts we have covered so far. In this activity, select the correct term to match the listed definition. This activity is not timed, so feel free to take your time completing it.

1. A\_\_\_\_\_\_\_\_\_\_\_is a piece of technology designed to hold your digital credentials.
   1. selective disclosure
   2. Zero-knowledge proof (ZKP)
   3. \* digital wallet
   4. Self-sovereign identity (SSI)
   5. digital identity wallet
2. A \_\_\_\_\_\_\_\_\_\_\_ enables the Holder of a digital credential to interact with digital credential Issuers or Verifiers to exchange credentials in a trusted manner.
   1. selective disclosure
   2. Zero-knowledge proof (ZKP)
   3. digital wallet
   4. Self-sovereign identity (SSI)
   5. \*digital identity wallet
3. \_\_\_\_\_\_\_\_\_\_\_ is a model for digital credentials that has a number of key concepts that create a privacy-respecting, user-centric, approach to digital credential issuance and use.
   1. selective disclosure
   2. Zero-knowledge proof (ZKP)
   3. digital wallet
   4. \*Self-sovereign identity (SSI)
   5. digital identity wallet
4. The concept of \_\_\_\_\_\_\_\_\_\_\_ when applied to the use of digital credentials is that users should be able to choose what and how much they share on a case-by-case basis.
   1. \*selective disclosure
   2. Zero-knowledge proof (ZKP)
   3. digital wallet
   4. Self-sovereign identity (SSI)
   5. digital identity wallet
5. \_\_\_\_\_\_\_\_\_\_\_\_\_\_ extends the concept of SSI even further, providing methods to prove possession or knowledge of a piece of information without disclosing the actual value of that information.
   1. selective disclosure
   2. \*Zero-knowledge proof (ZKP)
   3. digital wallet
   4. Self-sovereign identity (SSI)
   5. digital identity wallet

## Interviews with Experts

### Interview with Andre Boysen

We are happy to have with us, Mr. Andre Boysen, Chief Identity Officer with Securekey, to talk to us about credentials and some of the important benefits that innovations like verifiable credentials will afford us. Mr. Boysen expands on credentials and helps introduce topics we explore in later learning units (e.g., privacy, fraud prevention, ease of use, important technology and process advances).

<<Andre Boysen interview to be inserted here>>

### Interview with Mathieu Desrosiers

We are pleased to have with us, M. Mathieu Desrosiers, Lead of Everyday Banking, Payments, and Digital Identity with Desjardins. M. Desrosiers has taken time to talk to us about the consumer- business relationship with regard to digital credentials. M. Desrosiers talks about consumer concerns, how they might be mitigated, and some of the key enhancements that are coming our way.

<<Mathieu Desrosiers interview inserted here>>

## Conclusion

The key concepts we have defined in this learning unit will be expanded upon in subsequent units as we start to explore some of the technologies and standards that are used in the implementation of digital credentials.

## Unit 2 Quiz

Choose the best answer in the multiple choice quiz covering the concepts in this learning unit. You have one attempt at this quiz, but take all the time you want.

1. The benefits and advantages created with\_\_\_\_\_\_\_\_\_\_, are that the credential provides cryptographic proof that the document is authentic, the information has not been tampered with, and a method to strongly authenticate the Issuer without requiring the Issuer to be part of the exchange.
   1. \*verifiable credentials
   2. two -factor or multi-factor authentication
   3. authenticators
   4. Decentralized
   5. digital credentials
2. \_\_\_\_\_\_\_\_\_ are often alternatively classified as: knowledge factors, possession factors, inherence factors.
   1. verifiable credentials
   2. two -factor or multi-factor authentication
   3. \*authenticators
   4. Decentralized
   5. digital credentials
3. An important component of \_\_\_\_\_\_\_\_models is the component of the system where DID documents and other broadly available information required for verifying a digital credential is stored.
   1. verifiable credentials
   2. two -factor or multi-factor authentication
   3. authenticators
   4. \*decentralized
   5. digital credentials
4. \_\_\_\_\_\_\_\_\_\_ imply a specific model for issuance and use of a digital credential.
   1. \*verifiable credentials
   2. two -factor or multi-factor authentication
   3. authenticators
   4. decentralized
   5. digital credentials
5. In this scenario, you provide your password (something you know) and are then informed that a one-time PIN has been sent to your email address. You retrieve the PIN, enter it, and are then granted access.
   1. verifiable credentials
   2. \*two -factor or multi-factor authentication
   3. authenticators
   4. Decentralized
   5. digital credentials
6. At the simplest level, \_\_\_\_\_\_\_\_\_\_ are nothing more than the electronic equivalent of physical credentials that we already use today - credit cards, passports, driver’s licences and things like qualifications and awards.
   1. verifiable credentials
   2. two -factor or multi-factor authentication
   3. authenticators
   4. Decentralized
   5. \*digital credentials
7. \_\_\_\_\_\_\_\_\_ can be used to establish trust between parties by using a set of tamper-evident claims and metadata that cryptographically proves the identity of the Holder and its Issuer.
   1. \*verifiable credentials
   2. two -factor or multi-factor authentication
   3. authenticators
   4. Decentralized
   5. digital credentials
8. There must be a method that enables cryptographic verification and proof of authenticity of a verifiable credential, without having to consult the issuer of that digital credential. These two important characteristics (i.e., credential control by the Holder and usage of a credential without Issuer consultation) have led to the development of models for digital credential management that are \_\_\_\_\_\_\_\_\_\_.
   1. verifiable credentials
   2. two -factor or multi-factor authentication
   3. authenticators
   4. \*decentralized
   5. digital credentials
9. Most often in globally available digital identity systems, we see these \_\_\_\_\_\_\_\_\_\_ being implemented using blockchain technology.
   1. self-sovereign identity (SSI)
   2. zero-knowledge proof (ZKP)
   3. digital wallets
   4. \*distributed ledgers
   5. selective disclosure
10. It is important to note that \_\_\_\_\_\_\_ used for digital credentials differ from the more purpose-built wallets designed for specific financial purposes (cryptocurrency, payment systems such as Apple Pay or Google Pay, etc.).
    1. self-sovereign identity (SSI)
    2. zero-knowledge proof (ZKP)
    3. \*digital wallets
    4. distributed ledgers
    5. selective disclosure
11. Some of the features of \_\_\_\_\_\_\_\_\_ include direct and sole user control over digital credentials, the ability to decide what to share and one what basis on a case-by-case basis, and the ability to use a verifiable credential without having to consult with the issuer of that credential to verify its authenticity.
    1. \*self-sovereign identity (SSI)
    2. zero-knowledge proof (ZKP)
    3. digital wallets
    4. distributed ledgers
    5. selective disclosure
12. \_\_\_\_\_\_\_\_\_ relies on advanced public key cryptography, computations applied to protected information, and digital signature methods to create a cryptographic proof of knowledge of information without sharing the value of that piece of information.
    1. self-sovereign identity (SSI)
    2. \*zero-knowledge proof (ZKP)
    3. digital wallets
    4. distributed ledgers
    5. selective disclosure
13. Extending the SSI model, there is a concept of \_\_\_\_\_\_\_\_\_\_ that sees that only the absolute minimum information required is shared with a credential verifier.
    1. self-sovereign identity (SSI)
    2. zero-knowledge proof (ZKP)
    3. digital wallets
    4. distributed ledgers
    5. \*selective disclosure
14. The examples used in many explanations of \_\_\_\_\_\_\_\_\_\_\_ are proving that your birthdate is greater than a certain date (e.g., “I am over the age of 18”) or that you have in excess of a certain amount in a bank account, without revealing the exact amount in the account or the specific date of birth.
    1. self-sovereign identity (SSI)
    2. \*zero-knowledge proof (ZKP)
    3. digital wallets
    4. distributed ledgers
    5. selective disclosure
15. With\_\_\_\_\_\_\_\_\_\_, using advanced cryptographic techniques, the verifier receives only the information that they need from the digital credential.
    1. self-sovereign identity (SSI)
    2. zero-knowledge proof (ZKP)
    3. digital wallets
    4. distributed ledgers
    5. \*selective disclosure

# Unit 3: Risk, Privacy, and Barriers to Adoption

## Introduction

With the definition of many of the terms that one might encounter when exploring digital credentials, we turn our attention to some of the other factors to consider when examining a system or process dependent on digital credentials. In this learning unit we will touch on some of the important considerations such as risk, privacy requirements, and other barriers to the adoption of digital credential-based services.

**Learning Objectives**

1. Define risk, confidence, and levels of harm.
2. List Levels of Assurance (LoA)
3. Examine risk mitigation
4. Analyze Privacy
5. Examine factors affecting adoption of digital credentials

## Risk and Levels of Assurance (LoA)

### What is Risk and LoA?

Earlier, we highlighted concepts such as degrees of confidence and levels of assurance when defining digital credential terminology. The use of a digital credential establishes a level of trust between entities, allowing them to have a degree of confidence in the transaction to come.

How are all of these concepts interrelated? How are they classified and managed? What effect does this have on digital identity and verifiable credentials?

Throughout this learning series, we refer to levels of assurance (LoA). Let’s start there. There are some definitions we should get out of the way first. We talk about “risk”, “assurance levels”, “confidence” and “levels of harm”. To ensure that we are on the same page as we explore these concepts, **risk** is the *probability* of harm if exposed to a specific hazard. We have used levels of assurance and level of confidence somewhat interchangeably, as they are very closely related. The International Standards Organization ([ISO/IEC 29115](https://www.iso.org/standard/45138.html)) defines a **level of assurance** as *describing the degree of confidence in the processes leading up to, and including, authentication*.

### LoA Frameworks

In Canada and around the world, policy and standards often classify levels of assurance (LoA) in a defined framework directly equated with the potential level of harm resulting from a compromised transaction. In other words, the lowest level of assurance implies little confidence in asserted claims and the expectation of minimal or no harm in the case of a compromised transaction. In Canada, most LoA definitions are based on the formalized [LoA definitions used by the federal government](https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=30678&section=HTML).

[Can use the graphic on LoA here - see Slide 7](https://docs.google.com/presentation/d/1M1405CpKI1wqggJObbdJMJajnGSdEAwK76wgU3MEsZ8/edit#slide=id.gc78cff3fbc_0_19)

These are:

* LoA 1 - Little confidence required that an individual is who he or she claims to be. Compromise could reasonably be expected to cause nil to minimal harm.
* LoA 2 - Some confidence required that an individual is who he or she claims to be. Compromise could reasonably be expected to cause minimal to moderate harm.
* LoA 3 - High confidence required that an individual is who he or she claims to be. Compromise could reasonably be expected to cause moderate to serious harm.
* LoA 4 - Very high confidence required that an individual is who he or she claims to be. Compromise could reasonably be expected to cause serious to catastrophic harm.

This classification of LoA provides an important framework for the management and use of digital credentials. For example:

* While **validation** and **verification** of digital credentials are required at some level for every **authentication**, the level of stringency applied to examining digital credentials differs depending on the LoA. Self-assertion may be deemed appropriate as the basis of an **authentication** intended for use in an LoA1 transaction, while an LoA3 transaction may require **verified identity** and **verifiable credentials** for authentication.
* Policy goals can be expressed in terms of LoA. For example - “For LoA 1 transactions, we will establish a digital credential based on contextual evidence, but for LoA 2 transactions, the issued credential must be based on at least one piece of foundational identity evidence”.
* Procedural differences can be expressed in terms of LoA. For example - “For LoA 1 transactions, we will use best-practice password policies and authenticate based on those, but for LoA 2 transactions, authentication must be based on at least two factors or **authenticators**”.
* Standards bodies can set out conformance criteria for compliance certification with increasing levels of stringency and due diligence requirements based on LoA.

### Example of Risk Mitigation

Let’s look at a more specific example to help understand how common definitions and standards can help facilitate online transactions.

Steve lives in Calgary and is working on his engineering degree. Steve has been able to pay for his education to date using savings and income from part-time jobs. However, with university demands on his time increasing, Steve realizes that he will need student loans to help fund his education.

Because Steve uses online services as much as he can to make his busy life easier, he already has registered for a MyAlberta Digital ID (MADI). He also went through the process to make sure his MyAlberta Digital ID was **verified** (by allowing the province to access his driver registry information) so he could get access to more online services that require a higher level of identity assurance.

Steve goes to the Alberta Student Aid website, where he sees that he can apply online after creating an account. To do this, he can request the creation of a new digital identity and credential with Alberta Student Aid, or simply use his existing MyAlberta Digital ID (MADI). He logs in and starts his student loan application. The MADI program developed the **policy** and **procedures** that align with established **standards** for a higher LoA. These were examined and declared conformant. This allows agencies such as Alberta Student Aid to leverage the MADI credential, and its assertions pertaining to validity and veracity, to deliver improved user service in a more efficient way.

The increasing reliance on the digital economy and the ever-increasing value of the transactions to be found online mean that the exposure to risk and the potential for harm will continue to increase as the digital economy matures. The risk-based frameworks that provide the basis for common definitions and commonly understood processes are vital to provide at least one of the key foundations for cohesive, secure, privacy-enhancing usage of digital credentials.

### Meet Mike

Let’s follow Mike as he signs up for, and uses, his digital credential for online banking.

We will see some of the measures used to foster the trust that consumers must have when using their digital credentials. This example also shows the use of more stringent approaches to authentication for transactions that are of higher value and require greater confidence in their authenticity (i.e., the level of assurance required).

[Mike Explainer video goes here]

## Privacy

### Privacy Concepts and Privacy Law

**The Privacy Act and PIPEDA**

When you think about it, the information contained in a digital credential, when coupled with the transaction in which the credential was used, is usually made up of personal information. In some cases, digital credentials may even contain personal information without a transaction context. To protect this personal information, Canada has two important federal privacy laws, the Privacy Act and the Personal Information Protection and Electronic Documents Act (PIPEDA).

* The Privacy Act addresses how the federal government must handle personal information, and a person’s rights to access and correct their personal information.
  + Provincial governments also have their own laws governing privacy protection in their sphere of operations.
* PIPEDA establishes the legal obligations of private sector organizations engaged in for-profit activities.

**The Personal Information Protection and Electronic Documents Act (PIPEDA)**

PIPEDA applies to private sector organizations that operate in all provinces and territories except Quebec, Alberta, and British Columbia. These three provinces have implemented their own privacy laws (for provincially regulated organizations), which the federal government has examined and deemed equivalent to PIPEDA.

In addition to these broadly applicable laws, several provinces have implemented privacy laws specific to the health sector. In all cases, the personal data protection elements of these laws have also been examined and deemed equivalent to PIPEDA. The provinces that have implemented laws in this area are Nova Scotia, Newfoundland and Labrador, New Brunswick, and Ontario.

The Canadian legal framework continues to evolve with the proposed [Digital Charter Implementation Act](https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00108.html) that will create the Consumer Privacy Protection Act. This law, and a “sister” law (The Personal information and Data Protection Tribunal Act) creating an enforcement body, would replace and extend elements of PIPEDA to form one of the strongest privacy protection laws in existence. As well, the Federal Government is also working towards [a modernization of the Privacy Act](https://www.justice.gc.ca/eng/csj-sjc/pa-lprp/modern.html) that governs its handling of personal information.

What is privacy? What is private? Let’s start by defining the scope of what we are referring to when we talk about privacy. Privacy is about the personal information and the rights of individuals (or **persons**) to have that information protected. PIPEDA defines personal information *as information about an identifiable individual*. PIPEDA lists [10 fair information principles](https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/). These principles provide the guideposts for most of the privacy-related elements of standards that pertain to digital credentials and protection of personal information.

Briefly, these principles are:

* **Accountability** – an organization must appoint someone accountable for compliance with the 10 principles;
* **Identifying purpose** – the purpose for collecting personal information must be disclosed;
* **Consent** – an individual must have knowledge of, and consent to, the collection of personal information;
* **Limiting collection** – only the personal information required can be collected;
* **Limiting use, disclosure, and retention** – personal information can only be used or disclosed for the purposes under which it was collected, and retained only for as long as it needs to be kept;
* **Accuracy** – personal information must be as accurate and current as possible to satisfy the needs under which it was collected;
* **Safeguards** – personal information must be protected in a manner that aligns with its sensitivity;
* **Openness** – policies and practices for the management of personal information must be publicly available;
* **Individual access** – an individual must be informed what information has been collected and how it has been used, if and when they ask. They also have the right to have incorrect information amended;
* **Challenging compliance** – individuals have the right to challenge an organization’s compliance with any of these principles.

These principles, enshrined in legislation/regulation/standards/procedures, dictate that a person should:

* know what is being asked for and why;
* have to be asked to consent to the provision and sharing of personal information;
* know how personal information is used and shared;
* be assured of the protection of personal information; and,
* be assured that only what is required is being asked for and shared.

These safeguards apply to all personal information, not just the **attributes** of a **credential** that may be personal information. This is important for organizations that handle personal information. The protections apply to all transactions that handle personal information.

### Privacy by Design

Privacy by Design is particularly interesting in that it provides a comprehensive, high-level approach to ensure privacy is the first consideration in the design of any system. First developed and published in the early 2000’s, it has since been adopted by many countries as a component of their policies for privacy and personal information protection.

Privacy by Design presents [7 foundational principles](https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf) that lay out a holistic approach to embedding privacy concerns in systems development. These are:

* **Privacy protection is proactive, not reactive - t**hreats to privacy should be anticipated and prevented *before* they happen.
* **Privacy as a default setting** - personal information is automatically protected by default. If an individual does nothing, then their privacy remains intact.
* **Privacy embedded into design** - privacy concerns must be an essential component of the functionality being created, not an add-on to the core.
* **Privacy as a positive sum** - privacy and non-privacy system objectives can usually be met in a positive-sum manner so that all concerns are accommodated.
* **Full lifecycle protection** - privacy measures apply during the full lifecycle of the information, from creation or collection right through to secure destruction.
* **Openness** - all business practices and technology involved operate according to *stated objectives* and are subject to *independent verification*.
* **Respect for user privacy** - a user-centric approach that keeps the interests of the individual at the forefront when developing a system or process design.

### Meet Amanda

Let’s have a look at an example of the *10 fair information principles* in action. We will follow ACME Corporation as it starts down a journey to create an online product offering that depends on digital credentials.

Amanda Explainer video goes here

## Factors Affecting Adoption of Digital Credentials

### The Five Key Factors

What else affects the adoption of digital credentials? What are some of the end-user concerns and how can they be addressed?

We will now shift to identifying some of the other key characteristics that affect adoption, taking a user-centric approach. These are:

* **Reliability** - is a key characteristic that has a direct effect on the trust that users will have in an ecosystem dependent on digital credentials. Proven reliability of the digital credential itself, and the processes that use it, foster the trust required by all participants (persons and organizations) wishing to use the digital credential. Some common areas of concern include:
  + Reliable Service - does the service operate consistently and error-free?
  + Reliable process - do the operational processes align with expected LoA and overall system integrity?
  + Reliable service design - does the service design feature best-practice design and meet end-to-end privacy concerns?
* **Accountability** - the mechanisms that prove some elements of reliability are a key concept here. As well, the standards and laws that we have identified all have requirements to provide traceability for all activities related to digital credential use. Proven accountability is another key to fostering the trust necessary for the broad adoption of digital credentials. Demonstrated accountability provides a basis for ongoing trust in the service being offered. There are many elements to accountability, including:
* acknowledged responsibility for well-communicated policy and procedure. *Who is responsible? Where do I go if I have a problem? What are the mechanisms to dispute policy or procedure?*
* an accountable person responsible to handle privacy concerns and issues is required.
* from an operational perspective, the components of reliability must be demonstrable.
* **Interoperability** - Interoperability between entities is key to a healthy, well-functioning ecosystem that is user-friendly. Consider when a digital credential issued by a trusted issuer is received and safeguarded in a digital wallet, and later submitted to a third-party verifier. In this example, the digital credential has to be interoperable with the digital wallet AND the verification process. Without interoperability, decentralized identity cannot function well and digital identity silos are created, which is why we would characterize interoperability as an absolute requirement. In the digital credential world, this interoperability is achieved based on several key components:
* From a technology perspective, there are numerous organizations that develop standards and technologies to address various aspects of technological interoperability. This work is increasingly taking centre stage and continues to evolve.
* Common procedural requirements dictated by law or regulation.
* Collaboratively developed standards that provide best practice guidance for interoperable processes and technology.
* Policies developed in a jurisdiction (e.g., Canada, Province of BC) or sector (e.g., health, financial services) provide for alignment and interoperability at a policy level.
* **Usability** - partially affected by interoperability, usability (or ease-of-use) is a key concern for end-users of any technology-dependent process. This starts with best-practice design of user interfaces to ensure that:
  + information and processes are organized to make usage as straightforward as possible;
  + the user interfaces are error free and appear to be credible; and,
  + the user interface is adaptable to many device types (e.g., traditional desktop screen AND mobile devices).

There are many sources for best-practice guidelines aimed at solid user experience design. Usability is a field of practice in its own right and is often dubbed “User Experience”, or “UX” for short. If you are involved in a project that aims to offer or modify an online user experience involving digital credentials, you should involve a professional UX resource to ensure you maximize usability.

Beyond effective visual design and process design, there are some other considerations, particularly applicable to the use of digital credentials, that should also be considered. Processes dependent on digital credentials are often somewhat sensitive to privacy and security concerns, and may have a homogeneous target audience that has a defining characteristic (e.g., all potential users are expected to be working in a corporate setting). Dependencies such as these or any device or connectivity requirement should be considered when evaluating usability.

* **Accessibility** - broad adoption of digital credentials, or any technology-dependent process, requires a “nobody left behind” approach that takes into account the needs of potential users that may have barriers to the use of the most common tools to access online services. A significant percentage of the public are persons with disabilities, like mobility impairment or sensory issues (e.g., poor eyesight). There are any number of challenges that may make it difficult or impossible for persons with disabilities to use mainstream devices (e.g., computer screen or smartphone) typically used to access an online service. Any service dependent on digital credentials must provide for all of its potential user base in the design of end-user interfaces. In addition to the needs of the disabled, the following user characteristics should also be considered when evaluating accessibility.

* + Persons that are challenged by the process
  + Persons that are challenged by technology

### Meet John

Let’s put this in practical terms by looking at the thought process that John, manager of the ACME Inc. online portal, has as he looks into the potential causes of poor user adoption of their digital-credential-dependent website.

John Explainer video goes here

### Check Your Understanding

Let’s pause a moment and ensure you have grasped the concepts we have covered so far. In this activity, choose the best answer. This activity is not timed, so feel free to take your time completing it.

1. Risk is the probability of harm if exposed to a specific hazard.
   1. \*True
   2. False
2. In Canada, most LoA definitions are based on the formalized LoA definitions used by the municipal government.
   1. True
   2. \*False
3. Levels of Assurance (LoA) describes the degree of confidence in the process leading up to, and including, authentication.
   1. \*True
   2. False
4. How many levels of assurance are there?
   1. One
   2. Two
   3. Three
   4. \*Four
5. While validation and verification of digital credentials are required at some level for every authentication, the level of stringency applied to examining digital credentials differs depending on the LoA.
   1. \*True
   2. False
6. \_\_\_\_\_\_\_\_\_addresses how the federal government must handle personal information, and a person’s rights to access and correct their personal information.
   1. The Personal Information Protection and Electronic Documents Act (PIPEDA)
   2. Digital Charter Implementation Act
   3. \*The Privacy Act
   4. 10 Fair Information Principles
7. \_\_\_\_\_\_ establishes the legal obligations of private sector organizations engaged in for-profit activities.
   1. \*The Personal Information Protection and Electronic Documents Act (PIPEDA)
   2. Digital Charter Implementation Act
   3. The Privacy Act
   4. 10 Fair Information Principles
8. Privacy by Design presents \_\_\_\_ foundational principles that lay out a holistic approach to embedding privacy concerns in systems development.
   1. 5
   2. 6
   3. \*7
   4. 8
9. The key factors that affect adoption of digital credentials, taking a user-centric approach, include all but which of the following?
   1. Interoperability
   2. Reliability
   3. Usability
   4. Accessibility
   5. Accountability
   6. \*Privacy
10. Personal information is defined as information about an identifiable individual
    1. \*True
    2. False

## Interviews with Experts

### Interview with Catherine Desgagnes-Belzil

We had the opportunity to interview Catherine Desgagnés-Belzil, Executive vice-president and leader of business performance and CIO of Beneva. Catherine brings a unique perspective garnered from her deep experience with digital credentials in both the public and private sectors. Catherine shared with us some of the important considerations affecting interoperability, and some of the keys to achieving seamless interoperability in an ecosystem.

[Insert Catherine interview here]

### Interview with Dr. Ann Cavoukian

We had the privilege of interviewing Dr. Ann Cavoukian, who led the initial development of Privacy by Design and continues to advocate for its adoption.

Insert Ann C interview here

### Interview with Michelle Chibba

We are pleased to be able to include an interview with Michelle Chibba, formerly with the Privacy Commissioner of Ontario, and currently a noted speaker and lecturer on privacy and identity theft. Ms. Chibba will highlight some of key concerns with identity theft and some of the challenges that lay ahead.

[M. Chibba interview to be inserted here]

## Conclusion

This unit identified some of the Important factors to be considered when creating a system that is dependent on digital credentials. Privacy, levels of assurance, usability, reliability, and other factors influencing end user adoption are important determining factors in the adoption of digital credentials.

In the upcoming learning units, we will tie all of the concepts explored to date to describe the larger ecosystem in which digital credentials exist and some of the important technologies and standards used to create and manage digital credentials.

## Unit 3 Quiz

You have one attempt to take this twenty (20) question unit quiz. This quiz is untimed, so take your time to carefully review the options.

1. \_\_\_\_\_\_\_\_\_\_ is not one of the 10 Fair information principles contained in PIPEDA.
   1. Limiting collection
   2. Accountability
   3. \*Reliability
   4. Accuracy
2. “Threats to privacy should be anticipated and prevented before they happen” is part of \_\_\_\_\_\_\_\_\_\_.
   1. PIPEDA
   2. 10 fair information principles
   3. \*Privacy by Design
   4. The Privacy Act
3. The Personal Information Protection and Electronic Documents Act (PIPEDA) principles, enshrined in legislation/regulation/standards/procedures, dictate that a person should do all but which of the following?
   1. know what is being asked for and why;
   2. have to be asked to consent to the provision and sharing of personal information;
   3. have access to change their own private information at any time;
   4. \*know how personal information is used and shared;
   5. be assured of the protection of personal information;
   6. be assured that only what is required is being asked for and shared.
4. Privacy is about the personal information and the rights of individuals (or persons) to have that information protected.
   1. \*True
   2. False
5. \_\_\_\_\_\_\_\_\_\_\_ provides a basis for ongoing trust in the service being offered
   1. Privacy
   2. Usability
   3. Interoperability
   4. \*accountability
6. If you are involved in a project that aims to offer or modify an online user experience involving digital credentials, you should involve a professional UX resource to ensure you maximize \_\_\_\_\_\_\_\_\_\_.
   1. reliability
   2. \*usability
   3. accessibility
   4. Interoperability
7. There are \_\_\_ key factors affecting the adoption of digital credentials
   1. 3
   2. \*5
   3. 7
   4. 10
8. There are three high-level components of reliability. Which of the following is not one of them?
   1. \*Reliability evidence
   2. Reliable service
   3. Reliability process
   4. Reliability service design
9. There are many elements to accountability, including:
   1. acknowledged responsibility for well-communicated policy and procedure.
   2. an accountable person responsible to handle privacy concerns and issues is required
   3. the audit of operational procedure and automated system activity
   4. \*all of the above
10. The seamless integration of all these parties to deliver what appears to be a single service actually requires a high degree of
    1. \*interoperability
    2. Reliability
    3. Accessibility
    4. Usability
11. Proven \_\_\_\_\_\_\_\_\_ of the digital credential itself, and the processes that use it, foster the trust required by all participants (persons and organizations) wishing to use the digital credential.
    1. interoperability
    2. \*Reliability
    3. Accessibility
    4. Usability
12. Broad adoption of digital credentials, or any technology-dependent process, requires a “nobody left behind” approach that takes into account the needs of potential users that may have barriers to the use of the most common tools to access online services.
    1. interoperability
    2. Reliability
    3. \*Accessibility
    4. Usability
13. The International Standards Organization defines a level of assurance as describing the degree of confidence in the processes leading up to, and including, authentication.
    1. \*True
    2. False
14. Little confidence required that an individual is who he or she claims to be. Compromise could reasonably be expected to cause nil to minimal harm is
    1. \*LoA 1
    2. LoA 2
    3. LoA 3
    4. LoA 4
15. Very high confidence required that an individual is who he or she claims to be. Compromise could reasonably be expected to cause serious to catastrophic harm is
    1. LoA 1
    2. LoA 2
    3. LoA 3
    4. \*LoA 4
16. The increasing reliance on the digital economy and the ever-increasing value of the transactions to be found online mean that the exposure to risk and the potential for harm will continue to decrease as the digital economy matures.
    1. True
    2. \*False
17. The 10 fair information principles, enshrined in legislation/regulation/standards/procedures, dictate that a person should: know what is being asked for and why, have to be asked to consent to the provision and sharing of personal information, know how personal information is used and shared, be assured of the protection of personal information; and, be assured that only what is required is being asked for and shared.
    1. \*True
    2. False
18. The 10 fair information principles only apply to the attributes of a credential that may be personal information.
    1. True
    2. \*False
19. PIPEDA applies to private sector organizations that operate in all provinces and territories except Quebec.
    1. True
    2. \*False
20. Canada has two important federal privacy laws, the Privacy Act and the Personal Information Protection and Electronic Documents Act (PIPEDA).
    1. \*True
    2. False

# Unit 4: Ecosystem Models and Verifiable Credentials

## Introduction

In this learning unit we will explore the environment in which a digital credential is created and used. Earlier we saw that a digital credential is an electronic expression of a digital identity. The environment in which this digital credential is used consists of many components such as the allowable participants, their information stores, their processes, and the tools employed to create or use digital credentials. In the context of this learning series, the digital credential is central to the "raison d'etre" for the ecosystem, and we will refer more specifically to a digital identity ecosystem through this unit.

Learning Objectives:

1. Define the ecosystems in which digital credentials are created and used
2. Outline the importance of trust
3. Examine ecosystem models

## Digital Identity Ecosystems

### Define Digital Identity Ecosystem

Earlier in our learning series we referenced the *ecosystems* in which a digital credential is created and used. What do we mean by that? Let’s start with the basics.

The definition of ecosystem we have chosen to use explains that it is:

*a complex network or interconnected system*(Oxford)

or

*something (such as a network of businesses) considered to resemble an ecological ecosystem, especially because of its complex, interdependent parts* (Merriam-Webster).

Later in this unit, we will talk about some of the key high-level activities within an ecosystem (e.g., create digital credentials, use digital credentials) and the life cycle of a digital credential. The all encompassing environment in which a digital credential exists is the digital identity ecosystem.

The ecosystem in which a digital credential is created and used is built upon a tiered foundation of key elements that depend on the foundation(s) below them, as depicted in the figure below. A healthy ecosystem will be based on:

● **Laws and regulations** - these govern privacy and information protection;

● **Standards** – formal and informal standards that foster trust and interoperability;

● **Infrastructure** – the technical foundations upon which digital credential management systems are built;

● **Creators of digital credentials** – those organizations responsible for the creation of a digital credentials;

●  **Managers of digital credentials** – those organizations responsible for managing created digital credentials; and

● **Users of digital credentials** – the subjects of digital credentials and the organizations that depend on digital credentials to deliver services.

The video below gives us some additional insight on these key building blocks for a digital identity ecosystem.

<<The animated build of the pyramid goes here>>

### Key Considerations

With all these entities required for a vibrant, trusted ecosystem, we can see how some of the important concepts presented in earlier learning units are particularly important. Specifically, the adoption and auditable adherence to a common set of technology and process standards is an absolute requirement to ensure the interoperability, security, privacy, and trust necessary for effective use of digital credentials.

Finally, it is important to note that there is not only one ecosystem. There are many. For example, an individual that works in a secure environment dependent on digital credentials, likes to play online games and participate in social media in their spare time, and does the bulk of their banking online, is participating in at least three distinct ecosystems.

Ecosystems may choose to interoperate with each other. For example, your social media credential may also be used within an online gaming community. In this case, one digital credential is recognized in multiple ecosystems.

### Trust

In an earlier learning unit, we looked at some of the legal and regulatory framework in Canada applicable to personal information protection and digital credentials. We have seen that these laws and regulations are an important foundation for a healthy ecosystem.

Another important foundation for a healthy ecosystem is the standards that foster the interoperability and consistent application of security and privacy across all participants in an ecosystem. The key to viable digital credentials is trust. Trust that:

● an individual, organization, or entity is who/what they claim to be;

● the digital credential issuance process is robust;

● identity assertions and other claims or evidence are valid and tamper-proof; and,

● privacy is respected.

Broad-based trust in the digital credential fosters adoption by both the subjects of digital credentials and the organizations that depend on them. Interoperability is enabled by ensuring that the processes and technologies employed in the management of digital credentials are uniform, consistent, and meet the level of assurance required by all ecosystem participants. Collaboratively developed standards are the cornerstone to meeting the goals of reinforcement of trust and interoperability.

## Standards and Frameworks

### What is the Pan-Canadian Trust Framework (PCTF)?

One of the frameworks we have referenced throughout this learning series is the Pan-Canadian Trust FrameworkTM (PCTF).

The PCTF has been developed using a collaborative approach between the Digital Identity and Authentication Council of Canada ([DIACC](https://diacc.ca/)), the Public Sector Chief Information Officer Council ([PSCIOC](https://citizenfirst.ca/councils/public-sector-chief-information-officer-council-pscioc)), and the Public Sector Service Delivery Council ([PSSDC](https://citizenfirst.ca/councils/public-sector-service-delivery-council-pssdc)). The PSSDC and PSCIOC bring together standards and service delivery leadership from across all three (federal, provincial/territorial, and municipal) levels of the public sector in Canada. The DIACC is a non-profit coalition of public and private sector leaders focused on development of a framework for digital identity and authentication.

What is the PCTF? What does it do for us? Let’s have a closer look.

The PCTF seeks to provide enhanced confidence for persons and organizations (i.e., the end users of services dependent on digital identity) that their identity and personal information is properly protected, disclosed, and used. It seeks to provide the basis for governments and private sector entities that depend on reliable digital identity to deliver service using a standardized, high-integrity set of processes that they can rely upon. The PCTF describes the roles, services and requirements to ensure alignment, interoperability and trust of digital credential solutions, which are intended to operate across organizational, industrial and jurisdictional boundaries..

The DIACC identifies 10 requirements for the PCTF, while recognizing that these may be enhanced with additional requirements specific to an individual jurisdiction or industry sector. These are that the digital identity ecosystem must:

* be robust, secure, and scalable;
* implement, protect, and enhance privacy by design;
* be transparent in governance and operation;
* be inclusive, open, and meet broad stakeholder needs;
* provide Canadians with choice, control, and convenience;
* be built on open standards-based protocols;
* be interoperable with international standards;
* be cost effective and open to competitive market forces;
* be able to be independently assessed, audited, and subject to enforcement; and,
* minimize data transfer between authoritative sources and will not create new identity databases.

### Standardized Processes within the PCTF

The PCTF accomplishes this by defining the standardized processes and participant roles within the digital identity ecosystem. These have been described in several PCTF components, as illustrated in the figure below.

These components, and their associated conformance profiles can be found on the [DIACC website](https://diacc.ca/trust-framework/), but briefly, they address the following:

* **Model** describes the PCTF’s goals and objectives.
* **Glossary** provides definitions and examples for commonly used terms.
* **Assessment** describes the operation of the PCTF compliance certification program.
* **Verified Person** specifies the processes and conformance criteria used to establish that a natural person is real, unique, and identifiable.
* **Verified Organization** specifies the processes and conformance criteria used to establish that an Organization exists, and is real, unique, and identifiable.
* **Credentials** define a credential lifecycle and the criteria to assess the degree to which an ecosystem protects the use of digital credentials.
* **Authentication** provides the basis to assure the ongoing integrity of login and authentication processes.
* **Notice and Consent** defines the requirements for informed, accurate, and comprehensive delivery of notice of intent and consent for the collection and use of personal information.
* **Infrastructure** provides the general requirements regarding the trustworthiness of the IT infrastructure supporting automated processes within the digital identity ecosystem.
* **Privacy** defines the general requirements to ensure the ongoing integrity of privacy processes, policies, and controls.

The following video gives us some additional insight on the content of each of the PCTF Profiles. Note that the video has no sound.

<<The animated build of the PCTF graphic goes here>>

The PCTF creates a framework for trust and interoperability of digital identity in Canada. It is also designed for the inevitable evolution of digital identity as we move forward with the adoption of new and exciting developments that further enhance the security and privacy protection of digital identity and personal information. The framework is also designed with flexibility and extensibility as a primary concern. Often, a specific jurisdiction or industry sector will have needs that are unique. The PCTF components, and their conformance profiles, can be adapted and extended to provide an enhanced standard for specific uses.

For instance, the PSCIOC and PSSDC have collaborated to create the [Public Sector Profile of the PCTF](https://canada-ca.github.io/PCTF-CCP/PCTF.html) to address the unique needs of the Canadian Public Sector regarding digital identity. In addition, specific industry sectors have considered the PCTF and potential extension to meet the unique needs within their ecosystems (e.g., Health).

### Other Notable Work in Canada and Around the World

We have talked about the PCTF, focused on the requirements to foster the trust necessary for a digital identity ecosystem. There are two additional Canadian standards bodies that should also be highlighted, as some of their work relates directly to digital identity and digital identity ecosystems. These are:

1. The [*Standards Council of Canada*](https://www.scc.ca/en) *(SCC)* is Canada’s voice on global standards bodies such as the International Standards Organization (ISO) and the International Electrotechnical Commission (IEC). There are several standards in the Information Technology subject category that pertain to digital credentials, including those published by the second standards body we would like to highlight.

1. The [*CIO Strategy Council*](https://ciostrategycouncil.com/) *(CIOSC)* has developed, or is developing, a number of standards related to digital credentials.

When it comes to international standards, there are many. We encourage you to explore the links in this section to learn more.

The [*International Standards Organization*](https://www.iso.org/home.html) *(ISO)* includes a myriad of technology standards specific to the tools that may be used to facilitate processes like authentication (e.g., biometrics, smart cards, signatures, encryption). Please refer to their *Information Technology* section to search for those. As well, there are several standards addressing broader topics such as identity management, privacy, identity-proofing and authentication. ISO/IEC 24760-xx,29115, 29146, 29003, 29100, and 29001 are examples in this area.

The [*World Wide Web Consortium*](https://www.w3.org/) *(W3C)* has been building technical Web standards for as long as Web standards have been developed. Some of these will be touched upon in more detail in a later learning unit. There are two standards often cited when exploring verifiable credentials and decentralized identity. These are the [data model for verifiable credentials](https://www.w3.org/TR/vc-data-model/), and the [specification for decentralized identifiers](https://www.w3.org/TR/did-core/).

US based standards are also important due to the depth and breadth that our economies are interconnected, in both the public and private sectors. In particular, demonstrated compliance with the *National Institute of Standards and Technology (NIST)* standards in the 800 series on cybersecurity are often required to conduct business with US public sector bodies. Within this series, the [800-63 series](https://www.nist.gov/identity-access-management/nist-special-publication-800-63-digital-identity-guidelines) is specifically focused on digital identity.

Another US based standard that is often required when conducting business with US based entities is the Federal Information Processing Standard [FIPS 140-2](https://csrc.nist.gov/publications/detail/fips/140/2/final), or its successor [FIPS 140-3](https://csrc.nist.gov/publications/detail/fips/140/3/final), that addresses cryptography requirements for different levels of security.

**More international work**

Another jurisdiction frequently referenced is the European Union (EU). The EU has developed several technical standards to foster interoperability within the EU. As well, demonstrable compliance with several of their standards and regulations is required for all entities wishing to operate within the EU. Often referenced is the *Electronic Identification, Authentication and Trust Services (eIDAS)*. Current EU work and forward-looking vision is captured in the [Digital Decade](https://digital-strategy.ec.europa.eu/en/policies/digital-compass) strategy. Work on developing an eIDAS-compliant self-sovereign identity implementation is also underway under the auspices of the European Self-Sovereign Identity Framework (ESSIF). Finally, the General Data Protection Regulation (GDPR) is an important legislation in the area of privacy.

International open standards bodies are also key contributors to the development and the standards and frameworks that help govern digital identity ecosystems. As an example, the [*Linux Foundation*](https://www.linuxfoundation.org/) hosts several collaborative efforts developing technical and process standards in areas such as [Hyperledger](http://www.hyperledger.org) and [Trust over IP](http://www.trustoverip.org).

### Check Your Understanding

Let’s pause a moment and ensure you have grasped the concepts we have covered so far. In this activity, you will select the best answer. This activity is not timed, so feel free to take your time completing it.

The \_\_\_\_\_\_\_\_\_\_\_\_seeks to provide enhanced confidence for persons and organizations (i.e., the end users of services dependent on digital credentials) that their identity and personal information is properly protected, disclosed, and used. In other words, a trust framework for digital identity in Canada. (\*PCTF, W3C standards, eIDAS, ISO)

Demonstrated compliance with the EU privacy regulation, \_\_\_\_\_\_\_\_ (acronym) is another requirement for conducting transactions with EU member states, or within the EU. (\*GDPR, eIDAS, PCTF, Verifiable Credentials).

Two standards often cited when exploring verifiable credentials and decentralized identity are the data model for verifiable credentials, and the specification for decentralized identifiers published by the \_\_\_\_\_\_\_ (acronym). (\*W3C, NIST, Standards Council, ISO).

The components of the PCTF include Model, Glossary, Assessment, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, Verified Organization, Credentials, Authentication, Notice and Consent, Infrastructure, and Privacy. (\*Verified Person, Decentralized Identifiers, Identity, Trust)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ digital identity models have many of the same risks of single points of failure, abdication of control over end-user data, and the dangers associated with centralized models. (\*Federated, Centralized, Self-sovereign identity, Decentralized)

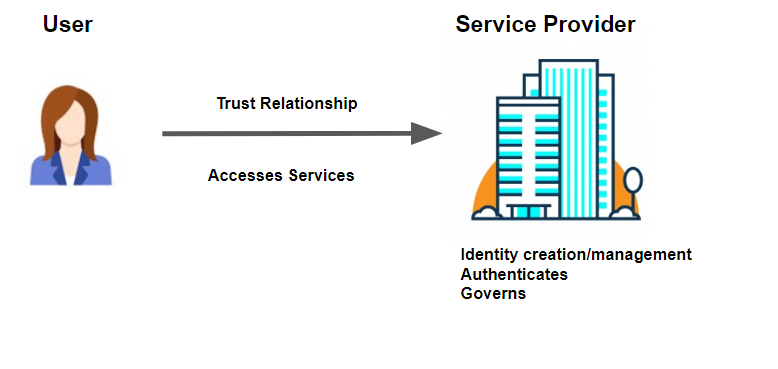
\_\_\_\_\_\_\_\_\_\_\_\_\_\_ is a model that is user-centric, where control over the sharing of information is actively in the hands of the subject of a digital identity. (\*Decentralized identity, Centralized, Federated, PCTF)

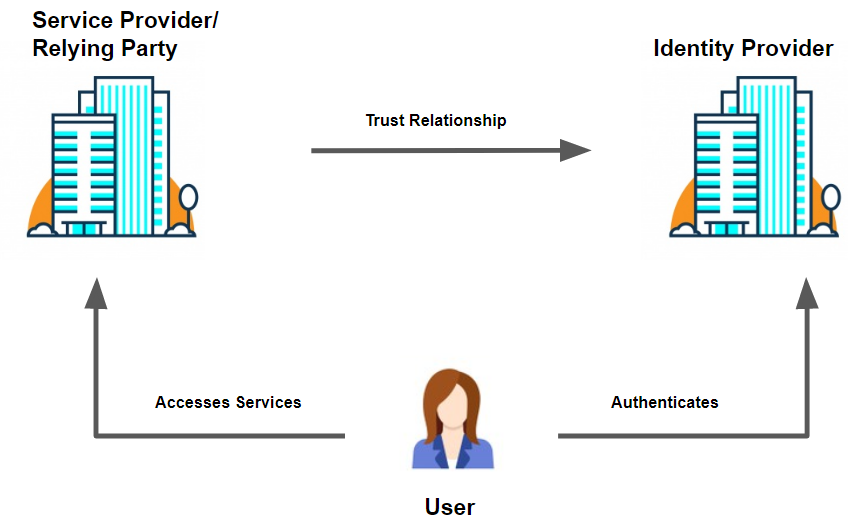
## Ecosystem Models

### Identify Models

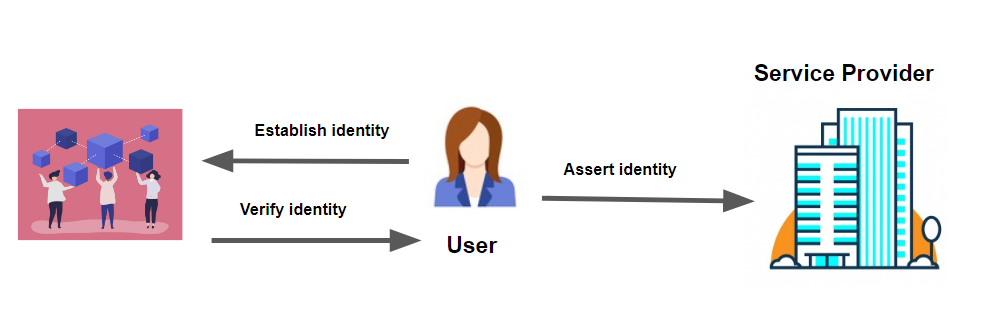
The ecosystems in which digital credentials are created and used are implemented using several different high-level design patterns, or architecture models, that can serve to preordain the capabilities or potential for evolution of an ecosystem. For example, an architectural decision by an organization to provide for all ecosystem services with capabilities that it owns or controls will most often lead to implementation decisions that are proprietary to that organization, which thereby affects the potential for growth and collaboration with partner organizations as the business environment evolves.

Let’s have a look at some of the common architecture models for an ecosystem.

Centralized - in this model, an *account* is created, controlled, and owned by the organization that a person is transacting with. This model is still widely used but is not recommended for reasons we will expand upon later in this section 



Federated - this model sees the introduction of an identity provider. Credentials established and/or managed by one organization are used to gain access to another. This enables single sign-on, which opens up the possibility of a single digital credential being used to access multiple domains.



Decentralized - this model often leverages blockchain technology to utilize distributed ledgers and cryptography techniques to create digital credentials that are network-resident and under the control of the subject of the digital identity. Under this model, no centralized database is required.

### Centralized

By far, the most prevalent models in use today are the centralized and federated models.

Centralized models were the most practical to implement in the past. However, these come with several issues in the longer term, including:

* In the interest of expediency, these systems were often not based on standards. For some legacy systems, appropriate mature standards may not have even existed at the time. Interoperability and integration with other systems as the use of digital credentials proliferate becomes expensive and difficult to maintain;
* Multiple single points of failure result in issues with reliability;
* The requirement for point-to-point integrations between service providers and verifiers significantly hampers scalability on a larger scale (e.g., national, global).
* This leads to the proliferation of authenticators for the end user, as each organization they deal with has their own proprietary platform. End-user risk increases with more onerous management of things like passwords;
* The user, by necessity, gives up control over their personal information;
* Risk is also exponentially increased when there are centralized repositories of digital credential information (e.g., a single successful attack on a repository compromises a massive amount of information). For the centralized model, this risk is higher as the organization’s core competency is usually in the delivery of their business service; and
* Data is often locked into proprietary platforms and technologies, and the form and methods for claims or data exchange may also be proprietary. This significantly reduces the opportunities for evolution to use more standards-based approaches and migration to improved models. The reinvention of systems is required more often as operations mature.

### Federated

Federated identity models have many of the same risks of single points of failure, abdication of control over end-user data, and the dangers associated with centralized repositories. However, this model does offer significant advantages over the centralized model. These include:

* The opportunity to access multiple services using one digital credential;
* These systems are standards-based with consistent methods for information exchange (i.e., claims); and
* While the risk of attack on a centralized information repository still exists, the information is managed by organizations whose primary purpose is the management of digital credentials. The risk remains, but the organization subject to attack is usually better equipped to respond to those attacks.

### Decentralized

Decentralized identity is a model that is user-centric, where control over the sharing of information is actively in the hands of the subject of a digital credential. This approach relies on leveraging technology approaches where information is under the direct control of the subject of a digital credential, and the additional information supporting verification/validation are housed on the network (e.g., distributed ledgers). The distributed ledger enables trust in the network without the control of one central authority. Through the consensus mechanism (the agreements between parties on the status of the ledger), some information is replicated, shared, and synchronized geographically, spread across multiple countries, or organizations.

No central administrator or centralized data storage exists, since the network is formed by peers that have the same grants and transact freely with each other. Public key cryptography allows an appropriate level of security in authorization and sharing of information. It provides data integrity since the data in the transaction are verified, along with the ownership of the transactions themselves. In other learning units we will expand upon this and some of the methods and technologies that have been used in reference implementations of the decentralized model.

These decentralized approaches, when implemented using self-sovereign identity principles, promise to deliver several advantages not possible in traditional models. These include:

* absolute user control of the sharing of digital credentials;
* privacy enhancing methods that make the sharing of only what is absolutely necessary;
* improved protection of data integrity;
* significantly reduced dependence on specific technologies;
* issuers of credentials do not need to integrate with verifiers;
* issuers do not know when their credentials are being used, those transactions remain between the user and verifier (increased privacy protection)
* verification can be performed without using computing power of the issuer. For example, even in cases where revocation must be checked, this can be done by consulting a distributed ledger;
* remove the reliance on centralized or third-party authorities for authentication; and
* significant reduction in the burden of authenticator management, and the security concerns associated with protection of credentials and authenticators.

### Characteristics of healthy ecosystems

The key building blocks for healthy ecosystems can be characterized as follows:

* Goals and principles for an ecosystem should be clearly defined. This establishes a common understanding of the purpose for the ecosystem and establishes some of the guideposts that will determine how an ecosystem is managed, and perhaps even the implementation model.
* Next-level detail that will establish the high-level operating approaches for the ecosystem. This includes decisions on the roles and responsibilities of ecosystem participants, how the ecosystem will be governed, and defining high-level criteria for participation in the ecosystem.
* The requirements or conformance criteria applicable to each of the roles in an ecosystem is then required to ensure a common understanding of the detailed responsibilities of each ecosystem participant. This also serves to set the operational model for management of information and provide a basis for evaluation of ecosystem participants.
* With creation of these detailed requirements, a companion program for audit and assurance of conformity to ecosystem requirements must be established.
* Finally, we will want the ecosystem to be flexible and able to respond to evolutions in the domain of best-practice digital credential creation, management, and usage. The processes governing continuous improvement of the ecosystem is vital to support the long-term viability of a healthy ecosystem.

The previous list defines the high-level items that contribute to a healthy ecosystem. If we take it as a given that there will be a diverse number of participants playing unique roles in an ecosystem, the *personality* of the ecosystem is also important for its long-term viability. These are the principles that define the expectations of contributors to the evolution of an ecosystem. Some of the common characteristics of successful ecosystems include:

* Openness - The ecosystem should be open to any qualified participant that wishes to contribute in some fashion. This may be an operational participant wishing to fulfill a role (subject to enshrined standards and other requirements) or an entity wishing to contribute to the evolution of the ecosystem.
* Flexibility - The ecosystem participants should understand that there will be different perspectives among ecosystem participants and be prepared to embrace those perspectives and learn from them. In many cases, a “sum is greater than the parts” result due to community learning creates a stronger ecosystem.
* Extensible - The ecosystem design does not preclude evolution in its design to incorporate improved best-practice approaches and technologies.
* Collaborative - The process for development and maintenance of the ecosystem should be consciously inclusive, ensuring that all stakeholders have the opportunity to contribute and have their unique perspectives and needs considered.

### Revisiting Martin

Let’s follow Martin as he experiences using digital identity under each of the models (centralized, federated, and decentralized) we have defined above.

<<Explainer video to be inserted here>>

## Interview with experts

### Interview with Joni Brennan

We had the opportunity to speak with Joni Brennan, President of the Digital Identity and Authentication Council of Canada (DIACC), about her experiences and some of the important advances that can be made in the digital identity landscape, made possible by open collaboration between all the key stakeholders we have identified in this section of the learning unit.

<<Joni Brennan interview goes here>>

### Interview with Andrew Johnston

Here to give us some additional insight into the nature of healthy digital identity ecosystems and some of the important work being done to mature identity ecosystems is Andrew Johnston, VP of Standards Development and Industry Relations at 2Keys.

<<Andrew Johnston interview goes here>>

## Conclusion

In this learning unit, we have defined the ecosystem in which a digital credential might be created, managed, and used. We have seen its components, and the high level models used to construct an ecosystem. We have also looked at some of the most referenced standards and ecosystem framework development bodies here in Canada and around the world.

Subsequent learning units will explore some of the open standards and technology foundations used to implement these ecosystems. Stay tuned for more!

## Unit 4 Quiz

You have one attempt to take this seventeen (17) question unit quiz. This quiz is untimed, so take your time to carefully review the options before choosing the best answer.

1. \_\_\_\_\_\_\_\_\_\_\_ is Canada’s voice on global standards bodies such as the International Standards Organization (ISO) and the International Electrotechnical Commission (IEC).

a. DIACC

b. CIOSC

c. SCC\*

d. W3C

2. In the \_\_\_\_\_\_\_\_\_ model, where the subject of a digital credential is dealing solely with the provider of a service dependent on digital credentials, the organization may be the creator/manager/user of a digital credential in addition to operating the technical infrastructure upon which it depends.

a. Decentralized

b. Identity Service Provider

c. Centralized\*

d. Digital Identity

3. The PCTF model describes the key processes for the activities such as authentication and digital credential creation. It describes these as belonging to three broad categories containing all BUT the following role

a. Create and manage digital identities

b. Use digital identity

c. Prevent the use of certain digital identities\*

d. Enable digital identity systems

4. An individual that works in a secure environment dependent on digital credentials, likes to play online games and participate in social media in their spare time, and does the bulk of their banking online, is participating in at least \_\_\_ distinct digital identity ecosystems.

a. One

b. Two

c. Three\*

d. Four

5. Your social media identity may also be used within an online gaming community. This is an example of ecosystems choosing to \_\_\_\_\_\_\_\_.

a. Interoperate\*

b. Create digital credentials

c. Alter processes

d. tier

6. Departmental digital identity ecosystems may exist as an identifiable subset of a larger government ecosystem, leveraging the foundations provided by the government level ecosystem, and extending it to enable it to conduct departmental transactions and activities. This is an example of ecosystems choosing to \_\_\_\_\_\_\_.

a. Interoperate

b. Create digital credentials

c. Alter processes

d. Tier\*

7. Laws and regulations are an important foundation for a healthy digital identity ecosystem

a. True\*

b. False

8. Broad-based \_\_\_\_\_ in the digital credentials foster adoption by both the subjects of digital credentials and the organizations that depend on them.

a. Interoperability

b. Trust\*

c. standards

d. Tiers

9. Strong encryption and advanced security to protect the primary personal information store is a feature of decentralized ecosystem models.

a. True

b. False\*

10. The DIACC identifies \_\_\_ requirements for the PCTF, while recognizing that these may be enhanced with additional requirements specific to an individual jurisdiction or industry sector.

a. 5

b. 10\*

c. 15

d. 20

11. The\_\_\_\_\_ is focused on the requirements to foster the trust necessary for a digital identity ecosystem.

a. PCTF\*

b. SCC

c. ISO

d. CIOSC

12. Issuers of digital credentials must have robust systems in place so their issued credentials can be verified when used.

a. True

B. False\*

13. End user risk is typically highest when participating in a \_\_\_\_\_\_\_\_\_ ecosystem for the issuance and management of digital credentials.

a. Federated

b. Centralized\*

c. Decentralized

d. Regulated

14. Demonstrated GDPR compliance is a requirement for conducting transactions containing personal data with EU member states, or within the EU.

a. True\*

b. False

15. \_\_\_\_\_\_\_\_\_ identities leverage two main capabilities of blockchain: the distributed ledger and the cryptography.

a. Distributed

b. Federated

c. Decentralized\*

d. Centralized

16. In this model, an *account* is created, controlled, and owned by the organization

that a person is transacting with. This model is still widely used but is not

recommended.

a. Distributed

b. Federated

c. Decentralized

d. Centralized\*

17. This model sees the introduction of an identity provider. Digital credentials established and/or managed by one organization are used to gain access to another. This enables single sign-on, which opens up the possibility of a single digital credential being used to access multiple domains

a. Distributed

b. Federated\*

c. Decentralized

d. Centralized

# Unit 5: Verifiable Credentials

## Introduction

Now that we have defined the basic concepts, looked at the lifecycle of a digital credential, and seen some of the ways that a digital credential is created and managed, let’s look at **verifiable credentials**. The [W3C](https://www.w3.org/TR/vc-data-model/) defines verifiable credentials as [*a mechanism to express credentials on the Web in a way that is cryptographically secure, privacy respecting, and machine verifiable*](https://www.w3.org/TR/vc-data-model/).

Verifiable credentials are an open standard for digital credentials and represent a key foundation for the peer-to-peer digital credential models we identified earlier. This learning unit will define verifiable credentials and some of the key concepts supporting verifiable credentials before we move on to other ecosystem design considerations and technologies in subsequent learning units.

Learning Objectives

* Explain verifiable credentials and verified identity
* Analyze verifiable claims
* Describe decentralized identifiers

## Verifiable Credentials and Verified Identity

### Verifiable Credentials

A verified credential is simply a presented credential claim that has undergone successful **validation** and **verification** using trusted processes. In other words, answering questions such as; *Is the information presented accurate?* And in the context of a person’s identity - *Does it belong to the person claiming that identity?*

Earlier we briefly defined verifiable credentials as [*a mechanism to express credentials on the Web in a way that is cryptographically secure, privacy respecting, and machine verifiable*](https://www.w3.org/TR/vc-data-model/). Verifiable credentials are primarily supported by two standards developed by the World Wide Web Consortium (W3C). Specifically, the [Verifiable Credentials Data Model](https://www.w3.org/TR/vc-data-model/) defines a standardized way to express credentials, and the [Decentralized Identifiers](https://w3c.github.io/did-core/) standard provides some of the mechanisms used to verify these credentials.

### How do Verifiable Credentials Work?

Setting aside how these identifiers are managed and consumed for a moment, let’s have a closer look at verifiable credentials themselves.

At the simplest level[[1]](#footnote-0), verifiable credentials are nothing more than the electronic equivalent of physical credentials that we already use today - credit cards, passports, driver’s licences and things like qualifications and awards. In these examples, the traditional way, which many of us are familiar with, is for a user to share information issued by a recognized and approved issuer with a service provider, including highly sensitive personal data and then the service provider may store all or part of that information on their centralized servers and use the information to decide whether they will offer the user some type of service, which may itself include issuing some type of new credential.

Verifiable credentials can be used to establish trust between parties by using a set of tamper-evident claims and metadata that cryptographically proves the identity of the Holder and its Issuer. More importantly, by using this approach, users can keep their data and simply share the needed information in the form of a verified credential with another party whenever they receive a request. The ability to extract the needed information and present only that information to the relying party is called *selective disclosure*. The benefits and advantages created with verifiable credentials, are that the credential provides cryptographic proof that the document is authentic, the information has not been tampered with, and a method to strongly authenticate the Issuer without requiring the Issuer to be part of the exchange. There is also a way to check for revocation. Finally, and maybe the most important, there is not a requirement for a point-to-point integration between the Issuer and Verifier.

In order for verifiable credentials to work, they need to support four different actors - Issuer, Verifier, Subject and Holder.

* Subject: the entity or thing about whom a claim is issued.
* Issuer: the person that creates the claim and associates it with the Subject.
* Verifier: the entity or person verifying the claim about a given Subject.
* Holder: the entity in control of the verifiable credential. A Holder is usually, but not always, the Subject of the verifiable credentials that they are holding.

For example, whenever someone wants to know something about us, we can use the verifiable claim to share a qualification, achievement, quality, or piece of information about an entity or person, such as a name, government ID, payment provider, home address, or university degree.

### How do Verifiable Claims Work?

Let’s have a closer look at how verifiable claims work. There are three key enablers of a verifiable credential. These are:

* A common data format understood by all participants. This is the data format prescribed by the W3C [Verifiable Credentials Data Model](https://www.w3.org/TR/vc-data-model/);
* Cryptography protecting all data and the claims exchanged between participants; and
* Ledgers enabling validation/verification of data and any associated claims.

There are a couple key processes that we will take a look at, at least at a high level, to help illustrate how a verifiable credential is created and consumed. But first, let’s look at the foundation of what makes a credential verifiable. As we have seen, there are two key activities when examining a digital credential’s information. Specifically, **validation** to make sure the information is accurate, and **verification** to ensure it belongs to the entity that is the Subject of a digital credential.

We have also identified cryptography and ledgers as key components to making a claim “verifiable”. This relies on principles rooted in Public Key Infrastructure (PKI) that use public-private keys for encryption, digital signatures, and revocation. If you are unfamiliar with PKI, the Introduction to Cryptography portion of this learning unit gives us some high level examples, and there are [multiple primers available online](https://en.wikipedia.org/wiki/Public_key_infrastructure) to help understand PKI.

Use of cryptography and some form of ledgers allows the following activities between keys actors (Issuer, Holder, Verifier):

* Credentials can be issued and signed by the Issuer, enabling a process of ensuring that the credential was indeed issued by an entity you choose to trust;
* Holder can authenticate the Issuer and the Verifier;
* Holder can prove cryptographically holding a particular credential, without handing over full control of the said credential to the verifier;
* Cryptography is used to ensure that only the intended recipient of any communication is able to decrypt a message (between Issuer and Holder, between Holder and Verifier, etc.); and
* The Verifier of a claim can assure themselves that the data came from a recognized Issuer, that the credential is valid, that that data has not been tampered with. At its option, the verifier can also check that the credential has not been revoked.

### The Issuance and Consumption of Credentials

Let’s have a look at the issuance and consumption of a credential. The figure below illustrates, at a very high level, the issuance and consumption of a verifiable credential and a verifiable claim.

<<animated image to be inserted here - See Unit 5 image posted in Graphics folder on Drive>>

The figure above assumes that the Subject of the digital credential is also the Holder of the issued credential. It also assumes two-way verification of the entities involved in the provision of an identity claim.

This may not always be the case. Systems may feature a third-party Holder that the Subject has chosen to hold and protect the issued credential (*Note: some examples here will include instances where an agent relationship, such as parent-child, might be expected*). Also, while verification of the Subject/Holder is an absolute requirement, some implementations may not include confirmation of the Verifier’s identity.

This model also features a core assumption that all parties and technologies are using a common data format such as the open standard described in the W3C Verifiable Credential Data Model.

Finally, the illustration assumes a Peer-to-Peer ecosystem model as described in an earlier learning unit. The W3C Verifiable Credential Data Model itself does not represent the full set of standards required for a Peer-to-Peer verifiable credential exchange. Standards for the process (e.g., W3C Decentralized Identifiers) and open-source technology standards are also required to construct the complete model. Later in this learning unit we will look at distributed identifiers. We will explore some of the open technology standards that support verifiable credentials in another learning unit.

## Construction of a Verifiable Credential

### Verifiable Credential Issuance

Let’s have a closer look at how a verifiable credential and a verifiable claim are constructed. This will help us understand how a verifiable credential can be [*a mechanism to express credentials on the Web in a way that is cryptographically secure, privacy respecting, and machine verifiable*](https://www.w3.org/TR/vc-data-model/).

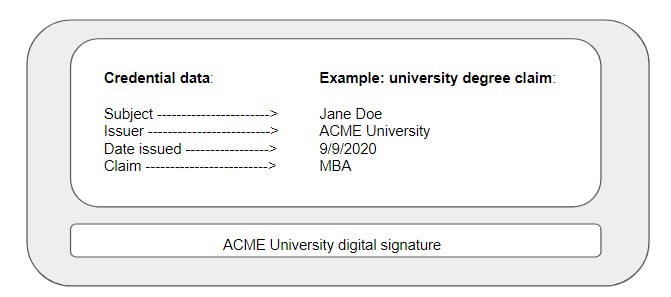
Verifiable credential issuance:

A verifiable credential, like any credential, is subject to validation and verification prior to issuance. When issued, it consists of two components.

1. The credential itself contains the credential metadata, identifiers, and claim (e.g., John Doe provincial driver licence).
2. The credential proof, essentially application of a digital signature to the issued credential assures immutability of the issued credential.

When issued, the credential is created by the Issuer and given to the Holder of the credential. Cryptography is used for encryption and digital signature of the “envelope” containing the credential to ensure that the credential can only be used by the intended recipient (i.e., the Holder) and the Holder can be assured that it comes from the Issuer.

Our example verifiable credential looks something like this:

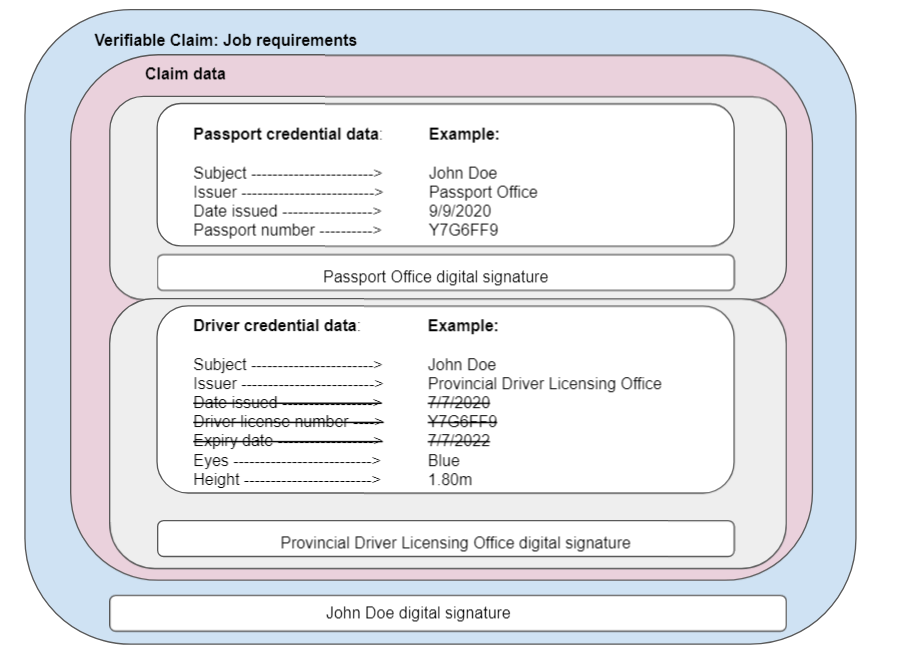


### Verifiable Claims

A verifiable claim consists of credential data extracted from one or more credentials packaged for presentation in a specific context. This is what the Holder presents to the Verifier with whom they wish to establish a digital identity for the purposes of receiving an online service.

Let’s break that down using an example that most of us can relate to.

John is applying for a job that has two strict requirements - that he is a Canadian citizen and he holds a valid driving licence. John has received a verifiable credential from the Canadian passport office with his passport credential. He also holds a verifiable credential from the driver licence bureau in his home province. From his passport credential, his name and his passport number are required. From his driver licence, his name, driver licence number, and date of expiry are required. This information packaged in a unified claim presentation affirming the two requirements (i.e., Canadian citizen and valid licence to drive) will be required. At a high level, this verifiable claim would be constructed something like this:



Much like an individual credential, a claim to a verifier consists of two high level components, the data that makes up the claim, and the signature of the entity making the claim.

One important element of this example to note is that not all the passport data, nor the driver licence data, has been used to construct the verifiable claim being made. For instance, the driver licence credential data includes attributes that say John Doe has blue eyes and is 1.8 metres tall. While this is part of the issued credential, it is possible to include only the information required by the verifier. This will, of course, also have dependencies on how the technology used to construct the verifiable claim or verifiable credential is configured. However, the standards used do not preclude this level of precision in the construction of an identity claim (for more information see Introduction to Selective Disclosure *later in this learning series*).

This is significant from a privacy protection perspective because, rather than sharing the entire credential, only the required information or identity attributes are shared. Another important characteristic is that the Verifier does not end up with full control of the issued credential.

### Verifiable Credentials and Claims in Action

Have a look at the video below for another example of this approach in action.

<<explainer video (5-1) goes here - I was thinking of building an example of registering for a site that requires two pieces of ID, at least one with a picture and one Govt issued with date of birth - show how it works now and then how it would work using a digital wallet and verifiable credentials>>

Let’s circle back to our definition of a verifiable credential and see if the example above meets the criteria of our verifiable credential definition - namely [*a mechanism to express credentials on the Web in a way that is cryptographically secure, privacy respecting, and machine verifiable*](https://www.w3.org/TR/vc-data-model/). Breaking this down, let’s examine each of the requirements of this definition.

* Cryptographically secure – The claim or credential is signed, and encrypted, using the public-private key pairs of the entities that are transacting. This serves three important purposes: the data can only be decrypted by the entity that is the intended recipient, the data is rendered tamper-proof, and there is no doubt that it came from the entity you believe it came from. From a cryptographic perspective, the goals of authentication, integrity, confidentiality, and non-repudiation are met.
* Privacy respecting – In the examples presented, we see the Holder (often also the Subject) of a digital credential in control of the credentials and any claims constructed based on those credentials. Nowhere do we see the absolute requirement for a third-party identity provider responsible for managing the digital credential, nor do we see a Verifier in full control of an issued credential. As well, we see that only the information absolutely required needs to be shared. Finally, we see that the Issuer is not made aware of the credential’s use, further enhancing privacy. These characteristics of verifiable credentials comprise a significant improvement in privacy protection over more traditional methods of managing digital credentials.
* Machine verifiable – Using standards-based approaches that rely on public-private key cryptography techniques, all claims can be systematically decrypted and readily understood without the need for proprietary interfaces between participants in a digital identity ecosystem.

### Decentralized Identifiers

The examples used when describing verifiable credentials are dependent on the W3C Verifiable Credentials Data Model for the schemas aimed at capturing credential data. The examples presented previously also depend on another emerging W3C standard, [Decentralized Identifiers](https://w3c.github.io/did-core/) (DID). This standard, currently (May 2021) in the Candidate Recommendation stage, defines a new type of unique identifier and the architecture for its implementation. Some elements of this architecture were present in the examples used in the previous section on verifiable credentials.

The [stated goals of Decentralized Identifiers](https://www.w3.org/TR/did-core/#design-goals) are:

* Eliminate the requirement for centralized authorities or a single point of failure in identifier management, including the registration of globally unique identifiers, public verification keys, services, and other information.
* Give entities, both human and non-human, the power to directly control their digital identifiers without the need to rely on external authorities.
* Enable entities to control the privacy of their information, including minimal, selective, and progressive disclosure of attributes or other data.
* Enable sufficient security for requesting parties to depend on DID documents for their required level of assurance.
* Enable DID controllers to provide cryptographic proof when interacting with other entities.
* Make it possible for entities to discover DIDs for other entities, to learn more about or interact with those entities.
* Use interoperable standards so DID infrastructure can make use of existing tools and software libraries designed for interoperability.
* Be system (and network) independent and enable entities to use their digital identifiers with any system that supports DIDs and DID methods.
* Favour a reduced set of simple features to make the technology easier to understand, implement, and deploy.
* Where possible, enable extensibility provided it does not greatly hinder interoperability, portability, or simplicity.

The architecture of a DID includes a subject reference (i.e., the subject of the identifier), locators pointing at key resources (e.g., a particular public key associated with the data), the data associated with the identifier such as attributes or information required to locate and utilize resources required to use the identifier, and information identifying the entity allowed to maintain a Decentralized Identifier. This information package is most often stored on a verifiable data registry, however, there are models that feature peer-to-peer communication of a DID as well.

Looking at the goals and architecture components of DID, it is apparent that the standard aims to define identifiers that are self contained and composed of all the information to be used in many digital identity management scenarios. *This is an important point*. Verifiable Credentials and Decentralized Identifiers help define the information and data structure standards to enable digital identity management models like the Peer-to-Peer model we defined in an earlier learning unit. However, these standards *do not* prescribe a particular implementation model or technology. These standards can be used to create an [interoperability bridge](https://www.w3.org/TR/did-core/#:~:text=The%20Decentralized%20Identifiers%20(DIDs)%20defined,identifiers%20using%20systems%20they%20trust.) between legacy centralized or federated digital identity ecosystems with decentralized models, such as the example used in the section on Verifiable Credentials.

To illustrate, let’s look at one component of the architecture of a DID, the *verifiable data registry*. The standards guidance simply defines this as any form of data storage. This can be legacy digital identity systems that have been extended to support DID. Aside from the data requirements defined in the W3C standard, this also means ensuring that the DID is consumable based solely on the method and locator information that is part of the DID itself (i.e., removing any absolute requirement for proprietary systems or identity providers).

In practice, much of the evolutionary work in the world of digital credentials is currently focused on approaches based on self-sovereign identity, which is discussed later in this learning unit, and technologies like Distributed Ledger technology, which includes blockchain that provide a more open inclusive service architecture and promise to provide the enhanced security and privacy protection that are the goals of DID.

### Check Your Understanding

Let’s pause a moment and ensure you have grasped the concepts we have covered so far. In this activity, choose the best answer. This activity is not timed, so feel free to take your time completing it.

1. A verified credential is simply a presented credential claim that has undergone successful validation.
   1. True
   2. \*False
2. Verifiable credentials are primarily supported by two standards developed by the World Wide Web Consortium (W3C).
   1. \*True
   2. False
3. The definition of a verifiable credential is: a mechanism to express credentials on the Web in a way that is cryptographically secure, privacy respecting, and machine verifiable.
   1. \*True
   2. False
4. In order for verifiable credentials to work, they need to support four different actors. Which one is not one of these actors?
   1. Subject
   2. \*Claim
   3. Issuer
   4. Verifier
   5. Holder
5. The Holder of a verifiable credential is always the Subject of that credential.
   1. True
   2. \*False
6. \_\_\_\_\_\_\_\_\_\_\_ is used for encryption and digital signature of the “envelope” containing the credential to ensure that the credential can only be used by the intended recipient (i.e., the Holder) and the Holder can be assured that it comes from the Issuer.
   1. Validation
   2. \*Cryptography
   3. Verification
   4. Identifiers
7. A verifiable claim consists of credential data extracted from one or more credentials packaged for presentation in a specific context.
   1. \*True
   2. False
8. There are a number of stated goals of decentralized identifiers (DID). These include which of the following:
   1. Give entities, both human and non-human, the power to directly control their digital identifiers without the need to rely on external authorities.
   2. Enable sufficient security for requesting parties to depend on DID documents for their required level of assurance.
   3. Make it possible for entities to discover DIDs for other entities, to learn more about or interact with those entities.
   4. Favour a reduced set of simple features to make the technology easier to understand, implement, and deploy.
   5. \*All of these are included in the goals
9. Cryptographic proofs of a verifiable credential are captured in the DID.
   1. \*True
   2. False
10. A DID contains all the important credential attributes for a verifiable credential.
    1. True
    2. \*False

## Interview with Experts

### 

## Conclusion

The two W3C standards we have briefly explored in this learning unit are key components of evolution in the last couple years in the approach to creation, consumption, and management of digital credentials. While the global community continues to develop the best practices, standards, and technologies for the implementation of verifiable credentials, the Verifiable Credential Data Model and Decentralized Identifiers consistently underpin these development efforts. Subsequent learning units will explore some of the frequently used design models and technologies applied to the evolution of best practice implementations of peer-to-peer implementations of digital credentials.

## Unit 5 Quiz

You have one attempt to take this fifteen (15) question unit quiz. This quiz is untimed, so take your time to carefully review the options before choosing the best answer.

1. A verified credential answers questions such as “is the information presented accurate? Does it belong to the person claiming that identity?”
   1. \*True
   2. False
2. A model supporting verifiable credentials must provide for \_\_\_\_\_\_\_\_\_\_\_\_\_ actors or roles.?
   1. 3
   2. 4\*
   3. 5
   4. None of the above
3. The entity or thing about whom a claim is issued.
   1. Issuer
   2. \*Subject
   3. Holder
   4. Verifier
   5. Claimer
4. Verifiable Credentials as defined by the W3C need not be machine verifiable..
   1. True
   2. \*False
5. The entity or person verifying the claim about a given Subject.
   1. Issuer
   2. Claimer
   3. Holder
   4. \*Verifier
6. The entity in control of the verifiable credential.
   1. Issuer
   2. Subject
   3. \*Holder
   4. Verifier
7. A verifiable credential, like any credential, is subject to validation and verification prior to issuance.
   1. \*True
   2. False
8. W3C standards such as Verifiable Credentials Data Model and Decentralized Identifiers do not address any of the technology requirements for implementation.
   1. \*True
   2. False
9. Digital signatures are a requirement of verifiable credentials.
   1. \*True
   2. False
10. Two standards often cited when exploring verifiable credentials and decentralized identity are the data model for verifiable credentials, and the specification for decentralized identifiers published by \_\_\_\_\_\_\_
    1. ISO
    2. \*the W3C
    3. NIST
    4. IETF
    5. DIACC)
11. There is a requirement for a point-to-point integration between the Issuer and Verifier.
    1. True
    2. \*False
12. The ability to extract the needed information and present only that information to the relying party is called \_\_\_\_\_\_\_
    1. \*selective disclosure
    2. Cryptography
    3. Decentralized identifiers
    4. Verified credentials data model.
13. What are some of the benefits or advantages created with verifiable credentials?
    1. The credential provides cryptographic proof that the document is authentic
    2. the information has not been tampered with
    3. a method to strongly authenticate the Issuer without requiring the Issuer to be part of the exchange.
    4. \*All of the above are advantages
14. What makes a credential verifiable?
    1. validation to make sure the information is accurate
    2. verification to ensure it belongs to the entity that is the Subject of a digital credential.
    3. \*Both a & b
    4. Neither a nor b
15. \_\_\_\_\_ means that the claim or credential is signed, and encrypted, using the public-private key pairs of the entities that are transacting.
    1. \*Cryptographically secure
    2. Privacy Respecting
    3. Machine Verifiable

# Unit 6: Design Considerations for Digital Identity Solutions

## Introduction

In this learning unit, we start to look more closely at the specific techniques and design models often used when creating digital credential systems. We will explore some of the key considerations and choices to be made from a systems perspective. In a subsequent learning unit, we will examine some of the common technologies being used to implement designs.

In a world where digital identity is becoming more prevalent, and the value of transactions conducted electronically continues to rise, the threats to our credentials and personal information will continue to rise in lockstep. Building upon our examination of verifiable credentials and decentralized identity, we will look at how the use of cryptographic technologies and techniques supports interoperability between participants creating and consuming digital credentials.

In a previous learning unit, we identified several of the high-level service architecture models that influence the implementation of a digital identity ecosystem. In this unit, we will describe several techniques, technologies, and solution design elements that are increasingly being used to implement digital credential related services.

This list is not exhaustive, we have selected some of the most important techniques available in the public domain to provide a starting point when considering solution design for digital credentials.

## Learning Objectives

1. Examine Cryptography
2. Describe important design models for digital credentials
   1. Selective digital disclosure
   2. Zero-knowledge proof
   3. Digital Wallet
   4. Self-sovereign identity
   5. Trust over IP

## Cryptography

### Introduction to cryptography

We have seen the importance of cryptography used to provide some of the basic capabilities required to secure a digital identity ecosystem. When considering what cryptography to use and how to use it, we should first understand the types of security services that cryptography can support:

* Confidentiality is the fundamental service of cryptography. Sound encryption of sensitive information helps ensure that information is unintelligible to unauthorized entities;
* Data integrity confirms the information has not been altered since its creation;
* Authentication helps confirm that the information has been sent by the expected sender; and
* Non-repudiation ensures that the sender cannot disavow or deny creation of an encrypted message.

Public-key cryptography uses keys to facilitate the signature or the encryption of messages. The longer and more complex a key and the encryption algorithm are, the less likely it is that an unauthorized entity can decrypt or falsely sign a message. Cryptography is based on one of two high level models.

1. Symmetric encryption uses the same key to encrypt/decrypt a message.
2. Asymmetric encryption uses one key to encrypt a message and another mathematically related key to decrypt.

Symmetric encryption is easier to execute, consuming fewer computing resources, which makes this model well-suited for encryption within a closed network or between two parties well known to each other. The disadvantages of this approach include the difficulties with ensuring that both parties have the same key, and the difficulty authenticating the origin of a message received. Also, symmetric cryptography does not scale well. It may work well for exchanges between two parties that have pre-established trust, but as the number of parties grows, the difficulties with key management increase exponentially. Symmetric encryption is often used in closed networks on large volumes of information. Examples include encryption of databases or large volumes of exchanged data on a closed network (e.g., in the financial sector).

In the online world, protected exchanges on the open Internet between parties that do not have a pre-established trust relationship between their systems are prevalent. For this reason, encryption that is largely based on asymmetric cryptography is more often used. Asymmetric encryption features key pairs that are mathematically related. One key is used to encrypt a message, and only the other key can decrypt it. This is the basis of public key encryption. In public key encryption, one of the key pairs is made public, while the other remains private and protected.

It is possible for these key pairs to be self-generated; Public Key Infrastructure (PKI) introduces a trusted certificate authority responsible for issuing digital certificates used to generate key pairs. These certificate authorities play two primary roles.

1. First, they ensure the certificate is issued under a well-established set of validation rules to ensure the certificate is issued to a known entity and installed as intended.
2. Second, they maintain a revocation list that can be consulted at any time to ensure the certificate issued is valid. This is an important role that supports the authentication function within cryptography, essentially creating a trusted third party that can attest to the authenticity of public keys.

NOTE: that we mention certificate authorities and PKI to highlight the origin of the “I” portion of PKI (i.e. infrastructure). Use of public key cryptography in digital credential models does not require certificate authorities in the same way as PKI does.

### Asymmetric encryption in action

Let’s look at an example of asymmetric encryption in action. The video below traces an exchange between John and Sally using public key cryptography to provide the four security services (i.e., Confidentiality, Authentication, Data Integrity, and Non-repudiation), that we identified previously.

<<Explainer 5-2 video goes here>>

### Encryption approaches

Encryption (under any model) is dependent on the algorithm that is used to encrypt information. The algorithm is generally more or less secure based on the length of the key used to “seed” the algorithm.

So why not just make the key as long as possible? Longer key lengths result in a performance trade-off as more computing power is required to encrypt and decrypt information. The most commonly used algorithms today are the Advanced encryption system (AES) advanced by [NIST](https://csrc.nist.gov/projects/cryptographic-standards-and-guidelines), and the [RSA asymmetric encryption algorithm](https://datatracker.ietf.org/doc/html/rfc8017). Both feature the ability to use different key lengths, and therefore the flexibility to adjust your cryptography to different levels of risk or performance needs. Algorithms and the standards for their use are constantly evolving as the capabilities of malicious attacks on security continue to evolve as well.

Finally, there is a mixed model that is often employed in cryptography to leverage the strengths of both symmetric (speed and efficiency) and asymmetric approaches (better trust support). In this approach asymmetric methods are used to establish a trusted foundation for interaction and symmetric keys are generated for use in the transaction being protected.

Let’s look at an example.

One of the most common uses of this approach is the establishment of a secure browser session. To establish a secure browser connection, the browser and webserver identify each other using an asymmetric exchange of keys. This leverages the authentication features of asymmetric methods. During this exchange, a single-use key is generated and shared between webserver and browser. From that point, until the end of the communication session, this generated key and symmetric encryption are used. This has the benefit of leveraging the speed of symmetric encryption for the heavy information exchange between browser and webserver.

### Digital Signatures

Public key cryptography is also used for digital signatures, an important component of decentralized identity models. Digital signatures prove that a digital message was not modified since it was signed. The message to be signed is taken and a short unique message digest is created and encrypted using the sender’s private key. The message digest (or “hash”) generated is unique to the message or document, and changing any part of it will completely change the hash.

When the recipient receives the message and the signature, they can generate their own hash of the message and decrypt the sender’s hash (included in the original message) using the sender’s public key. The recipient can compare the hash they generated against the decrypted hash. If they match, the message has not been modified and the sender is authenticated since only the public key of the sender could have decrypted a hash generated by the sender’s private key.

## Selective Disclosure

### Introduction to selective disclosure

Now that we have explored emerging approaches that feature verifiable credentials and distributed models, the remainder of this unit will define and describe approaches often characterized as “the way forward”. Most of these are not mutually exclusive. Instead, they are elements of an improved global identity ecosystem that institutes improved user control over digital credentials, limited disclosure (as defined in the 10 Fair Information Principles), and decreased reliance on proprietary technologies and service providers.

Selective disclosure, an important capability to facilitate minimum information disclosure, is a term often used when describing best-practice use of digital credentials. Selective disclosure is the ability for a subject to share a selected subset of information, limited to only the information required at the time. From a digital credential perspective, this means the ability to share only the credential **identifiers** and **attributes** required to establish identity within a specific context. The ability to selectively disclose personal information depending on the information truly needed by a relying party is a particularly important enabler of Privacy by Design.

### Selective disclosure example

An example often used to illustrate this concept is the verification of age to enter a club. Let’s have a closer look at that to illustrate the concept of selective disclosure.

In this example a driver licence will be used to verify identity and age. Your driver licence, which is a credential, contains the following information:

* Name
* Address
* Photo
* Height
* Eye colour
* Birth date
* Issuance and expiry dates

At the door to the club, you are asked to prove that you are above a certain age. You produce your driver licence and your picture is used to ascertain whether the credential belongs to you. Your birth date is used to determine if you meet the age requirement for entry. Unfortunately, you have also revealed sensitive personal information that was not required (e.g., your home address). Even more concerning, identity documents are often scanned in this scenario which means you have also given up control of this information.

If selective disclosure were possible in this scenario, you should have been able to expose only your picture and your birth date when asked for your identity for the purposes of entering the club.

From a digital identity perspective, the approach to selective disclosure has largely been focussed on using digital signature techniques to expose only the identifiers or attributes necessary, while keeping extraneous information inaccessible. For example, harkening back to methods discussed in asymmetric cryptography, this would mimic signing of each credential attribute and enabling the selection of these more atomic pieces of data in an identity claim.

There are several prerequisites for enablement of selective disclosure, including:

* construction of a credential in a form that supports selective disclosure;
* technology, cryptography, and processes that enable selective disclosure;
* the ability for credential verifiers to frame the appropriate information request to ask for only what is required (i.e., “I need a photo and confirmation of age from a government-issued identity”; and,
* the ability to verify the received response to the request.

The standards for verifiable credentials and distributed identifiers discussed previously in this learning unit provide a foundation for the implementation of standards-based, open, implementation of selective disclosure.

Let’s return to our example for a moment. We described a scenario where the photo and birth date were shared. In fact, the birth date was not what was really required. What was required was a trusted claim of being over a certain age. The standards we looked at earlier also make it possible to consider the on-demand creation of a verifiable claim of “I am over the required age”. This would require systems that ask the right question (i.e., Is the birth date greater than minimum required?”) and processes that would enable the construction of a verifiable claim that directly responds to the request. In cases where the birthdate, and only the birthdate was shared, this is selective disclosure. A technique we will explore later, called zero-knowledge proof, extends this by constructing a verifiable claim that proves age without revealing the birth date.

Some work in the cryptography technology, and technology process domain is ongoing to mature approaches that would achieve this. However, a prerequisite to broad based use of this ideal approach to selective disclosure will require widespread usage of some of the underlying standards (e.g., Verifiable Credentials, DID) that make approaches like this possible. As well, the technology open standards used to construct and consume verifiable credentials enabling selective disclosure at this level would need to be used to construct the technical solutions accompanying the digital wallet and the Verifier’s internal systems.

We will expand on this in a subsequent learning unit, where we look at some of the technologies used to implement verifiable credentials.

## Zero Knowledge Proof

### Introduction to zero knowledge proof

Many of the transactions we conduct require that we divulge personal information. This is especially relevant to the creation or use of digital credentials. Zero-knowledge proofs provide a means to verify that you know something, without revealing exactly what that something is. This has the potential to circumvent many of the privacy issues present in our online world today. Knowledge is not exposed in its true form over the Internet, while verifiers can gain confidence that the entity they are dealing with has the knowledge, attribute, or secret, they require.

Later we will talk about how this might apply to authenticators like a password, so let’s use that as an example. When you use a password to authenticate, the verifier does not necessarily require that you enter the password - they need to know that you know the password! Zero-knowledge proof provides a mechanism to determine this knowledge without you entering and transmitting that knowledge in an environment that might be subject to malicious actors trying to steal that secret. Another example could be to show you live in Canada without disclosing where you live exactly, or that your credit score is above 600, etc.

There are a few non-digital examples commonly used to demonstrate this concept. The one I prefer is the case where two people, one of whom is colour-blind, have two coloured balls.

The colour-blind person cannot distinguish between the balls, while the other person can. The colour-blind person hides both balls behind their back and randomly chooses whether to exchange them. They then extend their right hand and ask if the balls have been exchanged. The other person can tell from the colour of the ball displayed whether they have been exchanged and respond accordingly. When doing this once, there is a 50% chance that the answer would be correct by advancing a guess. However, if this exercise were repeated, the chances of getting the answer right *every time* would decrease.

With enough repetition of the exercise, the chances of the other person getting it right *every time* would approach zero. This is the essence of zero-knowledge proof. One person demonstrated knowledge of whether the balls had been exchanged without revealing any additional information about the balls. As far as the colour-blind person is concerned, they know nothing more about the balls than when they started, but they do know that the other person has knowledge of the balls and whether they had been exchanged.

### Zero knowledge proof criteria

A zero-knowledge proof must meet three criteria:

* Completeness - When a statement is true, the verifier will be convinced of this fact.
* Soundness - No random guess or other malicious approach to making a true statement is possible, with near-zero certainty.
* Zero-knowledge - If the statement is true, the verifier learns nothing other than the statement is true.

How does all this work in an online world? As we saw earlier, the science behind probability is part of the key. If an answer can be provided that is correct every time, then there can be statistical certainty on the part of a verifier that the person has the knowledge they are asking about. But how is the possession of knowledge revealed without revealing the knowledge itself in an online world?

To accomplish this, some very advanced mathematics and encryption techniques are used. If the inputs to a complex algorithm are the digital value of a secret or knowledge held + a random number, the results of the algorithm can be sent to a verifier and they can determine if the “answer” required possession of the knowledge they want to verify. If this process is repeated enough times and the answer always demonstrates knowledge held, then probability theory allows the verifier to be statistically certain that the person they are dealing with does indeed have knowledge of the secret.

Thinking of a practical use case, this approach can be the foundation of asking a question like, “Are you a resident of Nova Scotia?”, and seeding the algorithm with the value of your postal code to provide a series of responses that could only be possible if your postal code was a valid one, beginning with the letter “B”. In this scenario, the verifier is certain you are a resident of Nova Scotia but does not receive your exact address or any part of it (as is the case in many instances now). Privacy is maximized and the trust necessary for the verifier is satisfied.

One might ask how efficient this process is when it needs to be repeated enough times to provide statistical certainty. Several techniques with a significant degree of complexity are being advanced in this area. We will not get into the details of those here. There is another approach that is applicable when the knowledge is possessed by both parties, and that brings us back to passwords as an example. Both parties will know the value of an authenticator, like a password, but wish to avoid the security concerns associated with passing the value of the password during authentication.

In this case, complex mathematics can be used to generate patterns that are seeded with the value of the password. If several patterns are produced using the same “seed” and compared to one generated by the verifier, that complex math we talked about can be used to determine if all patterns produced must have come from the same seed. This process is significantly more succinct and provides the same level of confidence in knowledge held.

## Digital Wallets

### Digital Wallets

In the physical world, we store most of our credentials in a physical wallet. The purpose of a digital wallet is no different. It is something that is easily accessible to you, can store multiple credentials (e.g., driver licence, credit cards) and authenticators (e.g., keycards), and protects them from immediate line of sight.

Attempts at digital wallets have been around for years. With the advent of enhancements to smartphone technology we have seen an explosion of the use of digital wallets for payment (think Google Pay or Apple Pay). As well, digital wallets are a key component for the management of cryptocurrency. However, many of these wallets are designed for limited types of use (e.g., financial transactions) and many are based on proprietary systems or networks. The concept of a digital wallet, applied to standards-based identity management, features requirements that many financial or cryptocurrency wallets do not meet at present.

### What is a digital wallet and how does it work?

Let’s take a step back for a moment. What is the digital wallet and how does it work?

A digital wallet is software designed to hold and secure information required to conduct a transaction. These may be information like financial information (similar to that contained on your credit card), digital credentials (like those we have discussed throughout these learning units), or cryptographic keys (used to unlock sensitive data). A digital wallet can take many forms, it may be a self-contained physical item with embedded software (e.g., a USB key), or software only that can be housed on a device your have control of (e.g., your computer or smartphone), or software based that you entrust to a service provider for safekeeping. Let’s look at some common real-world examples:

1. Hardware-based - Many wallets designed for managing cryptocurrency come embedded on a USB storage device. This has the advantage of being portable and will work on anything that has a USB interface (computer, phone, etc.). When these wallets hold cryptocurrencies, they are sometimes referred to as “cold storage wallets”.
2. Software-based, local control - The example that will resonate with most people is the Apple Pay or Google Pay digital wallet used for financial transactions. This is typically installed on your smartphone and accessible by authenticators enabled on your smartphone (fingerprint, iris scan, passcodes, etc.).
3. Software-based, housed with a service provider - An example here would be a cryptocurrency broker that provides a digital wallet as part of a basket of related online services (Coinbase is one of many examples here).

For the remainder of this examination of digital wallets, we will assume the most used digital wallet software, one that you install on your smartphone.

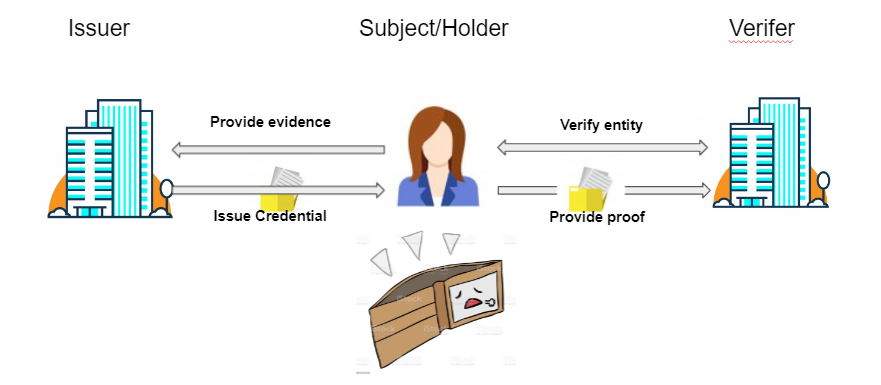
### Digital wallet example

The image below illustrates possible digital wallet use. You will notice it is similar to how we presented the peer-to-peer model for digital credential management in an earlier learning unit. A digital wallet, or similar mechanism, is the essence of a peer-to-peer digital credential model.

In its simplest form, a digital wallet features two basic discrete interactions.

1. Issuance:
   1. A Holder requests a credential and provides identity evidence based on the established procedures of the Issuer.
   2. The Issuer then constructs and issues a verifiable digital credential that the Holder stores in their digital wallet.
2. Presentation:
   1. The Issuer requests credential information from the Holder, Holder consent is required.
   2. The Holder constructs a verifiable claim from the credential(s) in their digital wallet and this is presented to the Verifier.

For a peer-to-peer model to be possible, these credentials must be standards based, using standards such as Verifiable Credentials and Distributed Identifiers discussed earlier. With the credential issued and in the possession of the Holder, it can then be used in an interaction with any Verifier that is equipped to utilize this standards-based credential. When the Holder wishes to access Verifier online services, they simply supply the credential or “proof”, or a portion thereof, to the Verifier. Using the methods we explored with Verifiable Credentials and Distributed Identifiers, along with the public key cryptography described earlier, the Verifier can verify the credential. If the Verifier has chosen to trust credentials definitively issued by the Issuer, then no further verification or third-party consultation is required.



Effective digital credential wallets should have all the following characteristics:

* The wallet is controlled by the Holder and cannot be seen, changed, or taken away without the Holder’s consent. This applies to all, even the wallet maker;
* It is portable;
* It is standards-based;
* It can be filled with any digital good that meets the standards;
* It can be replaced with another wallet and the contents are transferable to any other standards-based wallet;
* The wallet is secured with authenticators that the Holder controls;
* Lost credentials cannot be retrieved, and they must be recreated in an interaction with the Issuer;
* Issuers can revoke credentials, but they remain, in their revoked state, with the Holder; and
* The Holder has complete control over what is shared and with whom.

Earlier, we noted that digital wallets used for the purposes of identity had some characteristics not present with the wallets that initially emerged for financial transaction use or cryptocurrency management. At a high level, these characteristics are:

* The implementation of open standards that underpin verifiable credentials;
* The interaction to request and communicate consent to information sharing;
* The concepts that underpin selective disclosure, or sharing of credential components; and,
* The presence of an agent, a companion software, that can form connections and perform credential exchange based on open standards for verifiable credentials.

### Check your understanding

Instructions: In this activity, you will select either true or false for the associated question. When finished, select Submit at the bottom of the page.

1. Symmetric encryption depends on encryption key pairs. (false)
2. Symmetric encryption/decryption consumes fewer computing resources. (true)
3. Public key encryption or asymmetric encryption describes a method, any encryption algorithm may be used. (true)
4. Selective disclosure means sending only the data needed by the Verifier. (false)
5. Selective disclosure means only revealing the data needed by the Verifier. (true)
6. Zero-knowledge proof tells us that the value of an identity attribute is accurate. (false)
7. Zero-knowledge proof tells us that the Holder’s claim is true without revealing the actual credential attribute value. (true)
8. Zero-knowledge proof provides statistical certainty of the veracity of a claim, not absolute certainty. (true)
9. A digital wallet is always with the Holder, not a provider. (false)
10. Payment or cryptocurrency wallets inherently support verifiable credentials. (false)
11. A digital wallet, or similar mechanism is fundamental to the Peer-to-Peer digital identity ecosystem model. (true)

## Self-Sovereign Identity

### Introduction to self-sovereign identity

Self-sovereign is a term that many will have heard being tossed around recently. This is an approach to digital credentials that puts more control of identity in the hands of the individual.

Several of the concepts we have introduced in this learning unit combine to provide the foundations of Self-Sovereign Identity (SSI). It is generally held that SSI is based on user control of verifiable credentials that cannot be shared without their explicit consent. This implies a few other principles, such as no absolute requirement for centralized authorities that control digital credential management or usage.

SSI is a relatively recent development, generally acknowledged to have been kicked off with the publication of the [10 Principles of Self-Sovereign Identity](https://github.com/WebOfTrustInfo/self-sovereign-identity/blob/master/self-sovereign-identity-principles.md) in 2016. Since then, the global community has been collaborating to further mature the concepts for establishment of SSI based digital identity ecosystems. These collaborative efforts are too numerous to cover in their entirety, but several of those efforts will be cited as examples in this section.

SSI is based on several key building blocks, including:

* The trust and governance frameworks under which SSI operates
* The primary digital identity ecosystem roles required (Issuer, Holder, and Verifier)
* A verifiable credential format
* Distributed identifiers that enable verification without the need for centralized authorities
* Key technology building blocks that enable implementation
  + Digital wallets to securely hold verifiable credentials
  + Agent technology that enables the use of a verifiable credential
  + Distributed ledgers (i.e., blockchain) that serve as openly (and widely) available sources of truth for distributed identifiers and the encryption/decryption keys required to secure information exchanged within the ecosystem.

Let’s have a closer look at each of these building blocks.

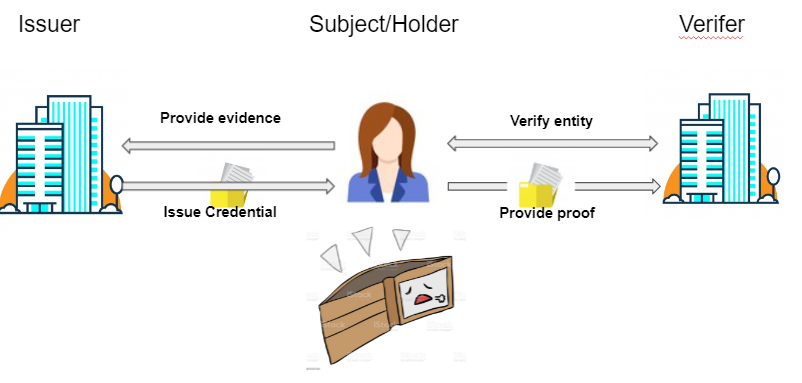
### Governance

As we have learned, a digital identity ecosystem is governed by the set of legal, process, and technology rules that represent the requirements for participation. Some of these are set by regulatory or standards bodies, while others are defined within the confines of the ecosystem itself. The standards and trust frameworks that are the basis of governance form the foundation upon which a healthy digital identity ecosystem is built.

For SSI, many are actively working on developing best-practice requirements for participation in an SSI ecosystem. International collaborative bodies include key influencers like the [Open Identity Exchange](https://openidentityexchange.org/) (OIX), [Decentralized Identity Foundation](https://identity.foundation/) (DIF), and [W3C](https://www.w3.org/). In addition many jurisdictions are actively working to extend and adapt their standards and trust frameworks to encompass SSI. Work on standards and frameworks like the [PCTF](http://www.diacc.ca), eIDAS and its [ESSIF](https://essif-lab.eu/), as well as related technology standards from organizations like [NIST](https://www.nist.gov/) are referenced in other learning units. These jurisdictional activities are ongoing and evolving rapidly.

### Definition of Key Roles

SSI, in its most basic form, defines three primary roles involved in the issuance and use of a verifiable credential.



1. An Issuer responsible for issuing a verifiable credential.
2. A Holder that acquires, stores, and presents a verifiable credential.
3. A Verifier that verifies the credential presented.

The basic model features no centralized authority that has the potential to contravene privacy protection standards or become an attractive point of attack for malicious actors looking to steal identities. Barriers to adoption are also lower because point-to-point integrations between Issuer-Verifier, or an identity service provider, are not required. Later in this section, when we look at some of the basic technology building blocks of SSI, we will see how this is possible.

### A verifiable credential

A verifiable credential is the digital equivalent of a physical credential we carry around in a wallet. This is the basic form and format for a digital credential within an SSI ecosystem. To be useful beyond one discrete digital identity ecosystem, this must follow a standard format where that standard has been widely recognized. In this case, the global digital credentials community has rallied around the W3C Verifiable Credentials Data Model described earlier in this section.

### Distributed Identifiers

A verifiable credential standard tells us how to formulate a credential, essentially the syntax required to express a verifiable credential. This does not create *a standard way to use a verifiable credential*. This is where distributed identifiers come into play.

A standard approach to distributed identifiers allows a scalable approach to enabling the verification of a credential. This includes methods for writing, reading, updating, and deactivating an identifier. Distributed identifiers for SSI have also seemed to rally around a core standard under development, specifically, the W3C Decentralized Identifiers standard described previously in this section. This forms the basis of the approach and several collaborative standards bodies are currently using that as a starting point to extend the model and layer in specific encryption approaches, distributed ledger standards, and blending of other techniques we explored earlier such as zero-knowledge proof and more atomic selective disclosure methods.

Distributed identifiers introduce another absolute requirement into SSI architecture. That is the distributed ledger, which provides a verifiable data registry, typically configured to also be open and accessible. This is most often based on blockchain technology. We will expand on how that works a bit later in this section.

### Digital wallets

Finally, we turn to some of the technology building blocks present in almost every description of the architecture of an SSI-based digital identity ecosystem. These are digital wallets, used to securely store verifiable credentials, software agents that enable standards-based usage of a verifiable credential, and distributed ledgers that are at the core of SSI being able to deliver trusted services without the need for a centralized identity authority or service provider.

From an SSI perspective, there are some [key requirements](https://diacc.ca/wp-content/uploads/2020/12/Making-Sense-of-Digital-Wallets_VF.pdf) that may not be present in all digital wallet products on the market:

* The implementation of open standards for portable verifiable credentials;
* Works with an agent software that enables the exchange and verification of verifiable credentials;
* Should accept any properly formed standards-based verifiable credential;
* Can be installed on multiple devices (computer, smartphone, etc.) and have mechanisms to remain synchronized when installed on multiple devices;
* Can be backed up and moved to another standards-compliant wallet (i.e., no “lock-in”); and,
* Delivers the same basic user experience as any standards-compliant wallet.

The marketplace is in its early stages and some characteristics such as portability and synchronization will continue to evolve as the marketplace matures.

### Agents

The digital wallet is where your verifiable credentials and private cryptographic keys are stored using formats based on adopted standards. However, that is only half the equation. The credential must be managed securely during presentation and verification to be of any use. Further, because SSI does this in a standards-based way, this interaction between Issuer-Holder or Holder-Verifier should be handled consistently no matter which version of a wallet (i.e. its companion agent software) is used.

This is where a digital agent comes into play. With a physical wallet out, one knows intuitively how to handle their own physical credential, you must take them out the wallet, retrieve the correct credential, and present it properly to be inspected. When issued, it must be accepted and placed into the wallet properly so it can be retrieved when needed. With a digital wallet, these tasks are the responsibility of the agent.

Think of the agent as a software “wrapper”, acting on your behalf, with your digital wallet (the software container). At a high level, this software performs two major functions:

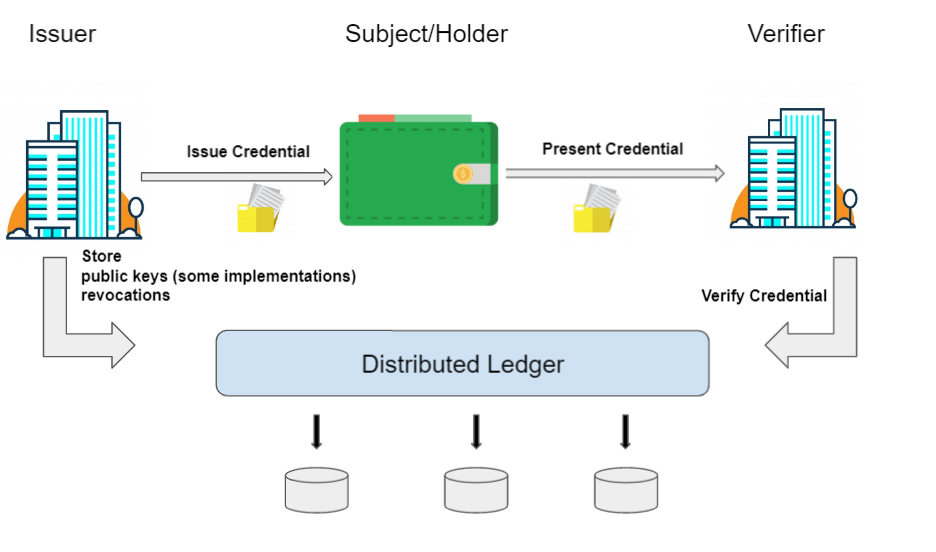
1. Provides the Holder control over its credential, including handing user consent flow, protecting the logical access to the digital wallet and ensure that the Holder, and only the Holder, can add or present a credential;
2. Based on standards, form and manage connections with other actors to exchange credentials. This may be with an Issuer or Verifier trying to issue or consume a credential;
   * Recalling our discussion of selective disclosure, the technology to construct a verifiable claim package that responds to the ideal version of SSI (i.e. exposure of only the atomic information required from multiple credentials) would be a component of agent functionality.

Under SSI, several standards contribute to defining consistent agent behaviour. Standards such as Decentralized Identifiers and several technology and technology protocol standards, to be explored in another learning unit, provide for the basic requirements of agent software.

### Distributed ledger

The distributed ledger is where DIDs are registered so they can be accessed by anyone. In truth this can be any information repository. For proposed implementations of SSI this has most often been based on blockchain technology. We will explore blockchain technology in another learning unit. However, for our purposes here the important characteristics of blockchain are that it is a highly tamper-proof distributed database that is not controlled by any single party.

Let’s have a look at how the distributed ledger enables SSI. The diagram below illustrates the use of a distributed ledger for the issuance and use of a verifiable credential.



The lifecycle from issuance to use of a verifiable credential is as follows:

* The Issuer creates a verifiable credential that is delivered to the Holder. Both Holder and Issuer have established trust and authenticated each other using asymmetric encryption and other public key cryptography methods as described earlier.
* The Issuer stores keys required for signature verification on the distributed ledger.
* When the Holder presents a credential to the Verifier. The Verifier and Holder can establish trust and secure information exchange using public key cryptography methods. Where public keys are required, the distributed ledger is consulted because all actors register their public keys there.
* The Verifier must then ensure that the credential has not been tampered with and is valid. The distributed ledger is consulted to read the issuer public key used to verify the digital signature to ensure origin and that the credential has not been tampered with since issuance. It is possible, but not always necessary, for the Verifier to query the distributed ledger to see if the credential has been revoked since its creation.

### Blockchain and SSI

As mentioned, the distributed ledger identified as a key foundation of SSI, provides the basis for verification of a verifiable credential. While this can be any conformant type of distributed storage available within a digital identity ecosystem, most models being advanced use blockchain technology as the basis for the distributed ledger.

In a later learning unit, we will look more closely at this technology, in this learning unit we will have a look at its functional characteristics and how it fulfills the distributed ledger requirements of SSI.

First, we need to understand a little bit about blockchain. Blockchain stores transactions in sequential blocks of transactions as they occur. Blockchains are stored on distributed networks of blockchain databases, all copies of one another called *nodes* . When a block is added, it is replicated and added to all nodes. If allowed by the particular blockchain network, if a block is ever modified, a majority of the nodes in the network must agree that the change is valid. If a hacker were to try to modify a transaction, or add a new one, that hacker would have to make the same change to 51% of the nodes simultaneously. A near impossible task when each of the nodes are independently operated. This is what allows trust that data on the blockchain has not been altered.

The second important functional characteristic is how blockchain can be used to protect privacy while being able to provide proof that the information received by the Verifier (from the Holder) is authentic and from a known issuer. To do this, public keys used by the Issuer to digitally sign the credential are stored on the blockchain. When the Verifier wishes to examine a credential, these keys can be retrieved to verify the signature. Any modification to the credential after issuance will be detected during this process.

It is important to note that the actual credential information is *never* stored on the blockchain. This important characteristic (i.e, immutability) of blockchain *allow the Verifier to be certain that the information is the information that was issued, from a source that is immutable by design*. Blockchain also makes it possible to perform this verification without introducing the need to consult directly with the Issuer, significantly reducing identity ecosystem complexity. Finally, because the credential information is signed cryptographically, the Holder can store the credential information off the blockchain without any loss of trust in the information itself while maintaining control over whom he/she shares the information with.

In our learning unit that explores some of the more significant technologies in detail, you will find a more involved discussion of how blockchain works.

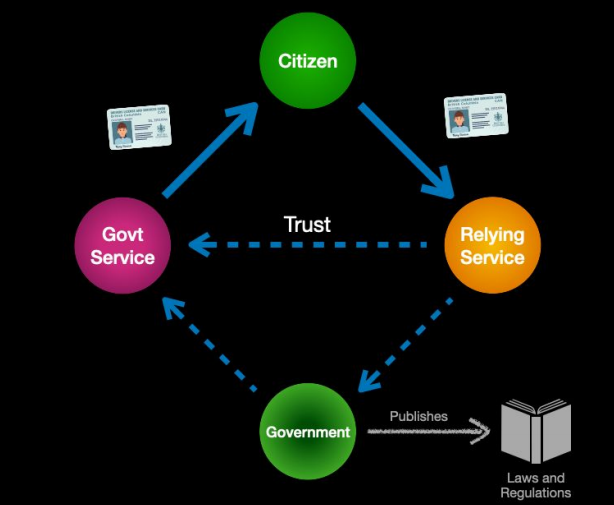
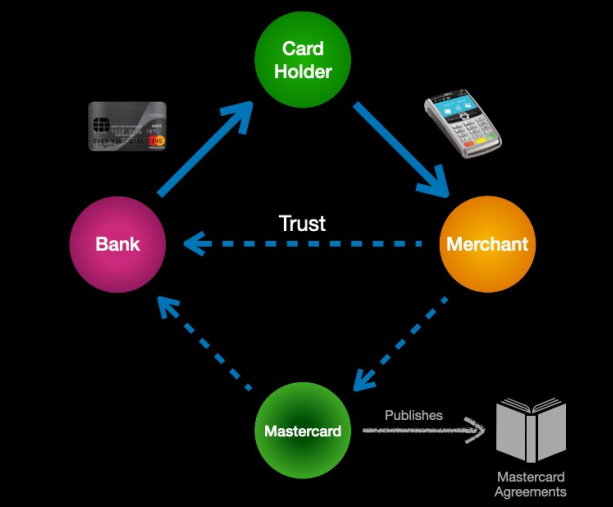
## Trust over IP

### Introduction to Trust over IP

Trust over IP (ToIP) is a holistic approach to try to standardize how online trust is established and maintained. ToIP is driven by the [Trust over IP Foundation](https://trustoverip.org/), a collaborative open-source project under the umbrella of the Linux Foundation.

Earlier in this learning unit, we identified the “triangle of trust” (i.e., Issuer-Holder-Verifier) at the core of digital credentials. An Issuer that establishes some level of trust so that they can issue a credential to a Holder, a Holder that chooses to trust a Verifier enough to present that credential for the purposes of receiving online service, and a Verifier that chooses to trust a credential issued by the Issuer.

The ToIP Foundation further identifies a governance “triangle of trust”. This sees a Governance Authority responsible for the standards (business, legal, and technical) that govern a particular digital identity ecosystem, an Issuer choosing to be governed by those requirements, and Verifiers choosing to trust the soundness of the Governing Authority ecosystem framework and that the Issuer that complies with those governing standards. In their [Introduction to ToIP](https://trustoverip.org/toip-model/) whitepaper, scenarios from a Public Sector service and another from the financial sector are put forward as examples.

[[2]](#footnote-1)

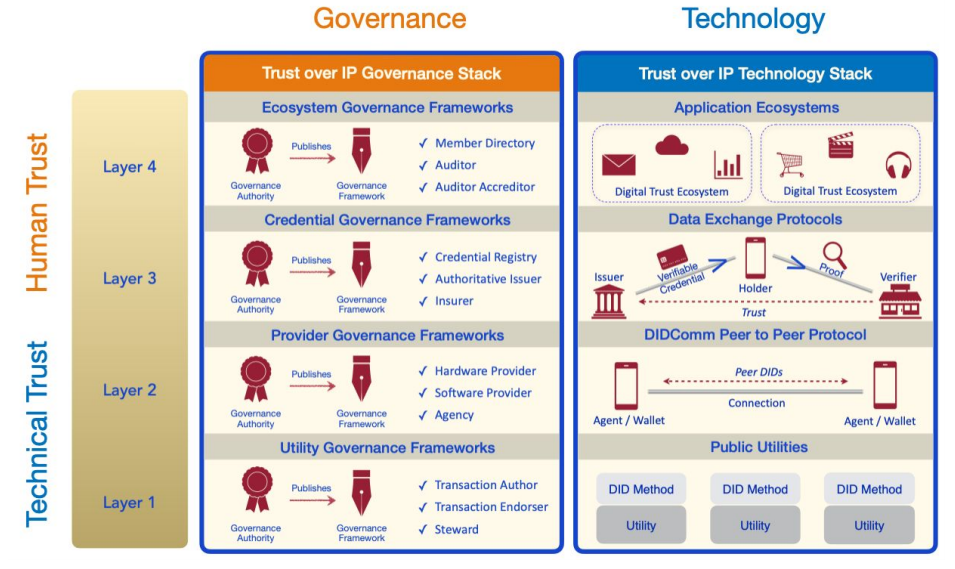
### Trust over IP stack

As we have seen, the centralized (or direct) and federated (or identity provider) models for digital credentials create some inefficiency and challenges, when deployed at scale, particularly when we consider how trust is established in the physical world. In the physical world, you establish trust and a credential is issued (let’s say your driver licence). You store it in your wallet and present it to whom you want, when required. The peer-to-peer model we described earlier, as well as advances in the world of digital identity based on verifiable credentials, distributed identifiers, and SSI, make it possible, for the first time, to mimic this common-sense handling of identity in the online world. That is, where your Issuers do not need to have a legal, or contractual, relationship with each and every Verifier you do business with.

The many initiatives that build this new paradigm of peer-to-peer trust in the online world have focussed on the many pieces that need to be defined to make such an ecosystem possible. Like many initiatives in the online world, this has focussed on inventing the technology pieces, and then figuring out how they all come together process/business wise. ToIP aims to take a more holistic approach by defining a stack of complementary services to deliver trust.

What is a stack? It is a set of services that build upon one another to create an ecosystem that delivers a service. Technologists will know the basic definition of a computing environment stack that goes from the hardware on which everything is installed, to the networks that interconnect everything, right up to the applications that run in the environment. Programmers will be familiar with programming languages stacks that start with a computer operating system, through to the data storage technologies they use, to the programming languages used to create end user applications.

ToIP proposes aligned technology and governance tracks that address trust and governance triangles as depicted above. The [ToIP Foundation](https://trustoverip.org/toip-model/) depicts this as follows:

[[3]](#footnote-2)

The ToIP stack, defined collectively as four layers in each of the Governance and technology stacks, pulls together the standards we have explored into a unified view that presents the set of services necessary to ensure trust within a peer-to-peer digital identity ecosystem.

The ToIP Stack Described:

| Layer | Provides: | Governance components: | Technical components: |
| --- | --- | --- | --- |
| 1 | The foundation of peer-to-peer trust, the management of the Decentralized Identifiers (DID) and public key cryptography that make peer-to-peer trust possible at its lowest level | Governing body that specifies the policies under which utilities delivering DID services operate. | Delivers the DID methods (note that these are technology agnostic). |
| 2 | Standards for the operation of the key components involved in peer-to-peer communication. Referencing SSI, this is all about the digital wallets and agents that form the connections between Issuer/Holder/Verifier. | Governance framework that specifies the standards for privacy, security, and data protection for providers of wallet and agent technology within an ecosystem. | The technology standards embedded in the hardware, software, or cloud services that provide wallet and agent services. |
| 3 | The basis for exchange of credentials and proofs between Issuers, Holders, and Verifiers. | The credential governance framework defines who issues which credentials, under what policies, and which level of assurance. Further, this Layer will define the criteria for the issuance of trustmarks, if any, that allow Verifiers to make their trust decisions. | Credential exchange, secure messaging, or workflow automation. Technologies implementing Verifiable Credential exchange are an example here. |
| 4 | These are the standards that apply to the entire family of applications within the ecosystem. The preceding layers establish the “plumbing” required to guarantee trust for an instance of a verifiable credential, this layer establishes the ecosystem level set of requirements that govern the consistent user experience across the entire ecosystem. | The purpose, principles, and policies that apply across the entire ecosystem. | Ecosystem interoperability and trust services not otherwise addressed in the preceding layers. |

## 

### Check Your Understanding

Instructions: In this activity, you will select either true or false for the associated question. When finished, select Submit at the bottom of the page.

1. Blockchain is an absolute requirement of SSI. (false)
2. The 10 Principles of Self-Sovereign Identity represent an important foundation to current work on SSI. (true)
3. Identity Providers are important players in any SSI model. (false)
4. W3C is the standards body for SSI. (false)
5. Digital wallet agents manage credential exchange in an SSI model. (true)
6. Public keys are retrieved from the distributed ledger in an SSI model. (true)
7. Network security is the key to trust in a blockchain database. (false)
8. Blockchain is primarily used to store credential information. (false)
9. Distributed database nodes are an important blockchain concept used to enhance the immutable nature of blockchain implementations. (true)
10. Trust over IP (ToIP) is primarily about technology standards. (false)
11. ToIP defines a unified view that presents the set of services necessary to ensure trust within a peer-to-peer digital identity ecosystem. (true)
12. ToIP defines complementary governance and technology layers that build upon one another. (true)

## Interviews with Experts

### Interview with Tim Bouma

We had the opportunity to speak with Tim Bouma about the exciting ways that the methods and technologies introduced in this learning unit have resulted in opportunities to re-think our approaches to the delivery of services dependent on digital identity and digital credentials. Tim is the senior advisor on digital identity to the Chief Information Officer for the Government of Canada.

### Interview with Peter Watkins

We're happy to have Peter Watkins with us. Peter is the program executive for Pan-Canadian digital identity with the Institute for Citizen-Centred Service. Peter is a proven innovator in the field of digital identity, with an extensive background as a public servant and change agent with the government of British Columbia. Peter will speak with us about selective disclosure and how selective disclosure has the potential to afford greater protection of personal information.

### Interview with Ian Bailey

We had the pleasure of sitting down with Mr. Ian Bailey, former CIO of British Columbia, to talk about digital credentials.

## Conclusion

In this learning unit we focussed on emerging decentralized ecosystem design concepts related to the Peer-to-Peer digital credential models. We learned that decentralised design is gaining traction for two main reasons:

1. The other models (Centralized and Federated/IDP) feature central authorities that drive some inefficiency when deployed at large scale. Often, these ecosystem designs are proprietary to the ecosystem itself and the needs of the centralized authority. In many cases, some solution technologies leveraged are often based on open standards, however, overall ecosystem design varies significantly.
2. There is growing recognition within the digital identity community that Peer-to-Peer and decentralised models are the next important evolution of digital credential solutions and ecosystems. It is these important evolutions that will enable us to meet the requirements of important privacy legislation and key principles such as those represented in selective disclosure in an automated, guaranteed, fashion.

Our next learning unit will build upon the material here and expand on some of the enabling technologies that will be required to implement user-centric digital credentials as described in this learning unit.

## Unit 6 Quiz

You have one attempt to take this nineteen (19) question unit quiz. This quiz is untimed, so take your time to carefully review the options before choosing the best answer.

1. \_\_\_\_\_\_\_\_uses the same key to encrypt/decrypt a message.
   1. \*Symmetric encryption
   2. Asymmetric encryption
   3. Public-key encryption
   4. None of the above
2. \_\_\_\_\_\_ encryption uses one key to encrypt a message and another mathematically related key to decrypt.
   1. Symmetric encryption
   2. \*Asymmetric encryption
   3. Public key encryption
   4. None of the above
3. Public key cryptography uses \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ cryptography methods..
   1. Symmetric
   2. \*Asymmetric
   3. RSA
   4. AES
4. Proof of the issuance of a credential without revealing the actual credential contents is called \_\_\_\_\_\_\_\_\_\_\_
   1. selective disclosure
   2. \*zero-knowledge proof
   3. a verifiable credentia
   4. self-sovereign identity
5. Distributed ledger technology requires blockchain to work
   1. True
   2. \*False
6. \_\_\_\_\_\_\_\_\_\_\_\_\_ uses keys to facilitate the signature or the encryption of messages.
   1. \*Public-key cryptography
   2. Distributed ledger technology
   3. The Verifiable Credential Data Mode
   4. ToIP
7. With SSI, the credential data is \_\_\_\_\_\_\_\_\_\_\_ stored on the distributed ledger to ensure it remains tamper-proof.
   1. Sometimes
   2. Always
   3. \*never
8. \_\_\_\_\_\_\_\_\_\_\_\_ provide a means to verify that you know something, without revealing exactly what that something is.
   1. public key cryptography
   2. verifiable credentials
   3. decentralized identifiers
   4. \*zero-knowledge proofs
9. Zero-knowledge proof relies on probability theory to be statistically certain that another party possesses some specific knowledge
   1. \*True
   2. False
10. The ability to selectively disclose personal information depending on the information truly needed by a relying party is a very important enabler of \_\_\_\_\_\_\_\_\_\_\_
    1. \*Privacy by Design
    2. decentralized identifiers
    3. ToIP
    4. public key cryptography
11. Blockchain is an absolute requirement of SSI.
    1. True
    2. \*False
12. The 10 Principles of Self-Sovereign Identity represent an important foundation to current work on SSI.
    1. \*True
    2. False
13. Identity Providers are important players in any SSI model.
    1. True
    2. \*False
14. W3C is the standards body for SSI.
    1. True
    2. \*False
15. Digital wallet agents manage credential exchange in an SSI model.
    1. \*True
    2. False
16. Public keys are often retrieved from the distributed ledger in an SSI model.
    1. \*True
    2. False
17. Network security is the key to trust in a blockchain database.
    1. True
    2. \*False
18. Blockchain is primarily used to store credential information.
    1. True
    2. \*False
19. Selective disclosure means sending only the data needed by the Verifier.
    1. \*True
    2. False

# Unit 7: Technologies & Frameworks

## Introduction

In an earlier learning unit, we looked at some of the high-level architecture decisions that govern the approach taken to implement a digital credential service. We also explored some of the commonly used design approaches that help guide the implementation of an architecture model. This learning unit identifies some of the more prevalent technologies and technology frameworks that provide a foundation for an implemented system or service.

The focus will be on the emerging open standards, protocols, and technology patterns commonly used in the implementation of trusted services.

This list is not exhaustive. We identified some of the most important standards, protocols, and technology patterns to provide a starting point when considering solution technology design for digital credentials.

## Learning Objectives

* Identify standards and standards bodies.
* List federated identity technologies.
* Name peer-to-peer identity technologies.
* Recognize when to leverage emerging technologies to deliver selective disclosure.

## Open standards

Much of the technology innovation we see today has its roots in open standards and open-source software. Open-source software is programming source code freely available for people to use, modify, and share with or without any restrictions. Open standards are community-developed standards that can be freely adopted and do not lock implementers into a specific vendor implementation.

The International Organization for Standardization ([ISO](https://www.iso.org)) defines a standard as *a document that provides requirements, specifications, guidelines or characteristics that can be used consistently to ensure that materials, products, processes and services are fit for their purpose*.

When it comes to defining an open standard, there are several definitions. However, most definitions have the following characteristics in common:

* Developed under an open process where any affected stakeholder can contribute.
* Created by a collaboration of domain experts, not an assigned authority.
* Subject to an open and inclusive peer debate and review process.
* Subject to approval processes based on community consensus.
* Do not feature requirements that will purposely “lock-in” adopters to a vendor or technology that is not freely available (e.g., can be implemented using open source or royalty-free technologies).
* Adhere to principles that emphasize voluntary adoption, following a philosophy of market-driven adoption based on merit.

In our definition of a standard, we see that one of the primary goals is to foster consistency in the products or processes that deliver a good or service. Open standards also include primary goals that reduce barriers to adoption, fostering broad based adoption (based on merit). This in turn allows for a more diverse community of both small and large participants to contribute to the standards community and the development of the innovative, and disruptive, technologies based on standards

## Federated identity, commonly used technology standards

**Introduction to Common Technology**

The bulk of the digital identity ecosystems in production today use the federated or centralized digital identity ecosystem models described in a previous learning unit. The technology standards for security, encryption, and other services required to protect and exchange digital identity information evolved to a point where a number of enabling technologies were commonly used in best-practice implementations of digital identity ecosystems. This section will focus on those technologies before we begin to examine more recent technologies supporting the peer-to-peer models and self-sovereign identity.

Examples of the technologies commonly used to support many of the existing centralized or federated digital credential models include Security Assertion Markup Language (SAML), OAuth, OpenID Connect, Security Tokens (e.g., Simple Web Tokens, JSON Web Tokens, and SAML assertions), and various Web Service specifications.

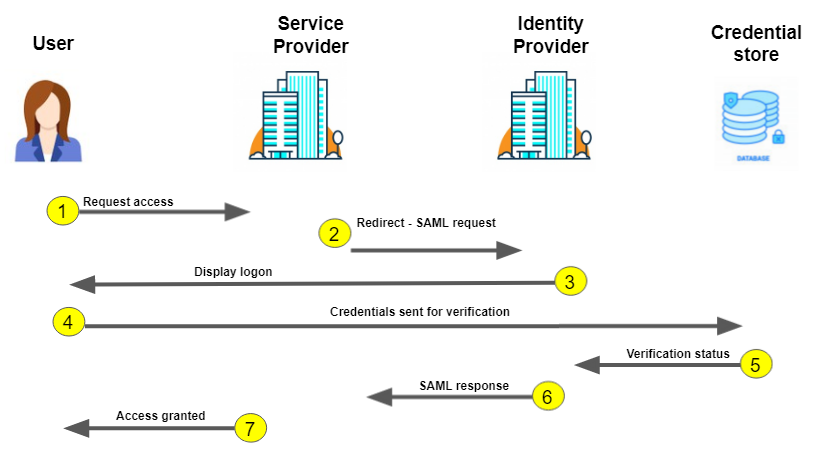
### SAML - Security Assertion Markup Language

SAML (authentication) - [published by OASIS](http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html)

Security Assertion Markup Language (SAML) is an XML-based open standard for passing identity data between an identity provider and the entity providing an online service based on identity. What this facilitates is the use of one identity provider to enable access to multiple independent online services (identified in the standard as Service Providers). The most common example is the single sign-on implemented in most large organizations. From a digital identity perspective across organizations, we see this when using banking or social media credentials to access other services.

SAML provides the link between the authentication of a user’s identity and the authorization to use a service. This federated approach to authentication provides enhanced user service (i.e., they don’t have to maintain logon credentials for each discrete service), and a simplified model for the Service Provider (sometime referred as Relying Party) because they effectively “outsource” complex authentication to a provider (i.e., the Identity Provider) that has a strong and robust authentication function, often with a sizeable base of already enrolled subjects.

SAML implements a secure method of passing user authentications and authorizations between the identity provider and service providers. When a user logs into a SAML enabled application, the service provider requests authorization from the appropriate identity provider. The identity provider authenticates the user’s credentials and then returns the authorization for the user to the service provider, and the user is now able to use the application. The figure below illustrates this process.



SAML is a mature technology that is widely used. The current version of the standard was first published in 2005. More recently, SAML is competing with some alternative technology standards such as OAuth and OpenID Connect technologies that leverage more recent technology approaches to provide federated identity services.

### OpenID Connect

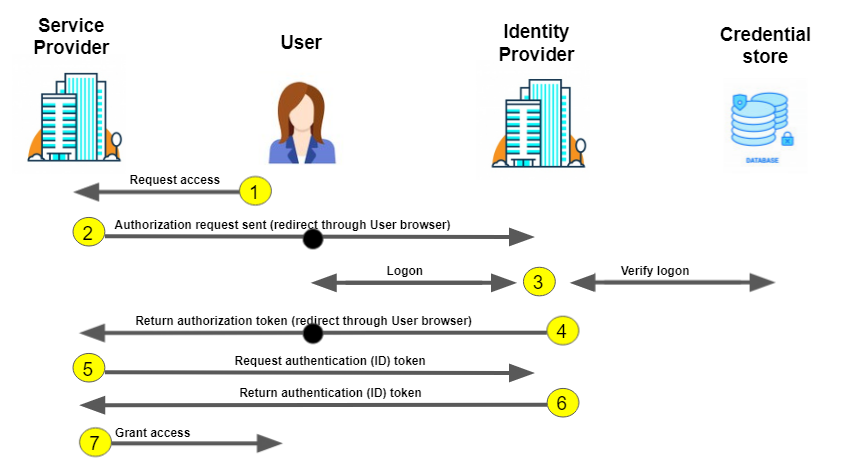
OpenID Connect (authentication) - [published by the OpenID Foundation](https://openid.net/connect/)

OpenID Connect, published in 2014, is an evolution of previous work on OpenID reflected in standards dating back to 2006. OpenID Connect (OIDC) is an identity layer that leverages the framework used for OAuth, described later in this section. OIDC, like SAML, was designed to support standardized authentication interactions between service providers (identified at Relying Party in OIDC) and identity providers in a federated identity model.

If you have ever used your social media credentials to authenticate to a service (e.g., used your Google or Facebook login to access another service outside the Google domain) then you have almost certainly been using OIDC.

OIDC leverages the more efficient framework of OAuth to replace the need to interpret XML (e.g., as is the case with SAML) in favour of using encrypted tokens. This provides enhanced security based on standards and more efficient processing of exchanged information.

Setting aside the intricacies of OAuth and how tokens work for the moment (we will explore those more in the next section), a high-level model of how OIDC works is depicted below. There are several slight variations on this model that we will not go into. However, the basic set of interactions for OIDC enabled authentication are reflected.



### OAuth

OAuth (authorization) - [published by the IETF](https://datatracker.ietf.org/doc/html/rfc6749)

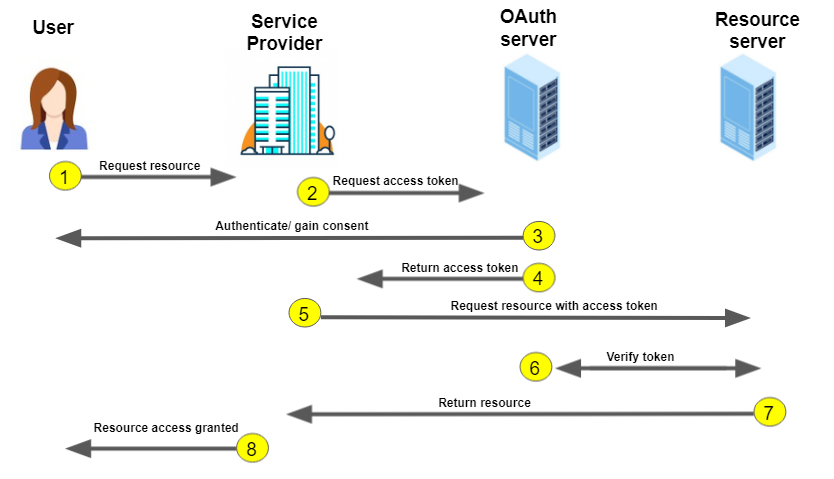
OAuth, published in 2012, is an open-standard authorization protocol that provides authorization to access a service. OAuth is not an *authentication* protocol or standard, it is an *authorization* standard. It grants permission to access something; it does not explicitly provide any information about identity or the fact that an explicit authentication took place. In essence, what OAuth does is provide the basis for a standardized secure interaction that asks, “May I have access to XXX” and a response that says, “Yes, you may”. Assuming the requestor and the organization that holds XXX both understand OAuth, then access to the requested resource is granted.

Used in this way, OAuth can provide a sort of pseudo-authentication. Let’s look at an example to illustrate (*NOTE that what the user sees is very much the same experience as described with OIDC*). A website asks to use your social media account to log on to its service - the service provider then formulates an OAuth request to access the social media’s authentication status (the identity provider) - this request is routed by the user’s browser to the identity provider - the identity provider confirms authentication and sends back an authorization message, usually with a time limit for validity. The service provider then *chooses* to take this as confirmation of authentication. Previously, we said that OIDC extended OAuth for the purposes of authentication. The essence of this is an addition to the process that results in the further creation and exchange of an authentication token that confirms that an authentication took place.

If you have ever been asked a question like, “this application would like to access your camera” on your mobile phone, or asked, “This application wants access to your Google account, and be allowed to view your email messages and settings” - you have been exposed to OAuth in action.

The figure below illustrates the high-level OAuth process. There are a few things to keep in mind as you look at the illustration:

1. Built into the OAuth standard is the concept of a “scope”. The scope is the specific resource to which access is being requested. In the Google example, “email messages” would be an example of scope.
2. Consent is also an integral component. Explicit consent from the User to access the requested resource of theirs from another server must be embedded in exchanged messages before an access token can be issued.
3. Tokens have a defined, usually short, lifespan and can facilitate access to only the specific resource (or scope) requested.
4. The access token in the illustration below can be thought of as being synonymous with the authorization token we identified when describing OIDC.
5. OAuth is used in many different use cases, we have referenced two in this section. The Google mail messages are the resource to which access is being requested in the social media example. In the “pseudo-authentication” example, the requested resource could simply be the dashboard page one would see on an application after logging in.

As was the case with OIDC, there are some process variations in the use of OAuth. We will not go into those here, but there is a good collection of information resources on the [OAuth 2.0 standard page](https://oauth.net/2/).

### Web Tokens

In describing OIDC and OAuth, we referenced the use of tokens (meta information referencing or representing something else) to enable access. With OIDC, we see two types of token, the authorization or access token, and an identity token. There are many different implementations of token schemes and standards, but for our purposes we will have a look at JSON Web Tokens (JWT) to gain an understanding of the use of tokens in a federated digital identity ecosystem.

JWT (commonly pronounced “jot”), [another IETF standard](https://datatracker.ietf.org/doc/html/rfc7519), was published in 2015. This standard defines a container used to transfer information securely. A JWT is digitally signed to support validation of origin/authenticity, and optionally encrypted.

A JWT at a high level contains three important components:

1. The header that identifies the signature and encryption methods used, providing the information required to “unpack” a JWT.
2. The payload that contains the information exchanged.
3. The signature.

The payload contains what the JWT standard calls a claim. In the context of a JWT payload, this is one or more name/value pairs. There are different types of claims.

* A registered claim uses names that are universally recognized. There are about ten of these types of names for commonly used data such as who issued the JWT, who it is about, and when it expires. For instance, “iss” names the issuer (e.g., the payload would contain “iss” : “John” as one of its claims). Information about the claim name (e.g., “iss”) can be referenced in a publicly available registry to provide context to understand the names.
* There can be public claims that use defined names unique in a certain context. For instance, a specific digital identity ecosystem may define reserved claim names to be used in the context of information exchanges among the participants in that digital identity ecosystem. These defined names are also registered.
* Private or custom claims can be anything the creator of a JWT wants to include. These claims do not have a registry component and the assumption is that the recipient of the JWT understands the context for each of the claim names.

To create the signature part, you must take the encoded header, the encoded payload, a secret, the algorithm specified in the header, and sign that. This is used to verify whether the JWT was modified in transit. It can also be used to verify that the sender is who they say they are.

Digital signatures provide a basis to ensure authenticity of the message, encryption of the entire JWT renders it unreadable to any third-party during transmission. While any signature or encryption methods can be used with JWT, there are two other standards most commonly used. [JSON Web Signature](https://datatracker.ietf.org/doc/html/rfc7515) (JWS) and [JSON Web Encryption](https://datatracker.ietf.org/doc/html/rfc7516) (JWE). These are two complementary IETF standards that provide signature and encryption support for JWTs.

For anyone seeking more information on JWT, in addition to the standards pages linked in this section, [jwt.io](https://jwt.io/) provides a good set of more detailed references.

### Check Your Understanding

Instructions: In this activity, you will select either true or false for the associated question. When finished, select Submit at the bottom of the page.

1. Open standards help software vendors by promoting their products. (false)
2. Open standards are collaboratively developed and maintained. (true)
3. SAML is an authentication standard. (false)
4. OAuth is an authorization standard (true)
5. OAuth relies heavily on XML for authentication messages. (false)
6. OAuth includes a consent component. (true)
7. JWT is required to have your system use Web Tokens. (false)
8. Digital signatures provide a basis to ensure authenticity of the message in JWT. (true)
9. SAML is an open standard for passing identity data. (true)
10. OIDC is completely independent of OAuth. (false)
11. Tokens are a significant requirement in OAuth and OIDC standards. (true)
12. JSON Web Signatures are required in a JSON Web Token. (false)

## Peer-to-peer digital credential models, commonly used technology standards

Previously, we defined peer-to-peer models as featuring the Subject/Holder of a digital identity at the centre of the ecosystem exerting direct control over their digital credentials and how they are shared. We delved a bit further into this, introducing Verifiable Credentials and Decentralized Identifiers and how approaches such as self-sovereign identity (SSI) and selective disclosure could work within peer-to-peer models.

The standards for this type of ecosystem model are not as mature as the one presented earlier in this module, but gaining significant traction in the last few years. As a result, there are many technology approaches evolving to support peer-to-peer models. Contrasting this with standards often used in federated models, SAML is approximately two decades old and went through the same disjointed evolution as the community put forward their best attempts at technology standards and frameworks to best support the then-new approach of federated identity models. Eventually, SAML based approaches became de-rigueur, used by most. That is, until better approaches based on standards such as OIDC and OAuth emerged about a decade later. Current work with new or renewed federated digital identity ecosystems tend to focus on these technologies. We can expect that same process of community consensus emerging around preferred technologies, followed by significant maturation of supporting tools, in the peer-to-peer domain.

The sections that follow are by no means exhaustive, but rather, represent an attempt to identify some of the technologies that have started to gain some traction when implementing verifiable credentials and moving towards self-sovereign identity.

We will examine several different technology standards or frameworks that have been used in reference implementations of verifiable credentials. We will look primarily at how verifiable credentials are expressed, and how they are digitally signed and proven.

### JSON and JSON-LD

The Verifiable Credentials standard has published [implementation guidelines](https://www.w3.org/TR/vc-imp-guide/#introduction) that present scenarios that use JSON and JSON-LD (LD = “Linked Data”) as potential syntax for expressing the data in a verifiable credential.

JSON is a language independent syntax for storing and expressing information. It essentially consists of name-data pairs that would look like this is expressing information about a vehicle:

{

make : Chevrolet

model : Corvette

}

[JSON](https://datatracker.ietf.org/doc/html/rfc7159) is widely used in many application contexts. It is simple, straightforward to process, uses human readable text and technology agnostic. It does have some drawbacks though. The syntax does not inherently convey any information context. This means that context must be either widely understood, or some other mechanism must be created to convey context. Using the example above, there is no guarantee that the recipient of this message understands what “make” and “model” mean.

[JSON-LD](https://www.w3.org/TR/json-ld11/) was developed to provide this context by extending JSON syntax something like this:

{

@context : “http://schema.url/”,

@type : manufacturer

make : Chevrolet

@type : vehicle model

model : Corvette

}

JSON-LD identifies a schema that would contain the context of what this data is part of. In this example, the schema would present the information structure that makes it clear that some higher-level construct such as “motor vehicle” might have related information such as the manufacturer, model name, year of manufacture, etc. The @type information provides references to the overall information schema, meaning that the recipient can better understand “make : Chevrolet” by understanding that it refers to the “manufacturer” data element that is part of a larger information object described in the schema to be found at the address in the “@context”.

At present, JSON-LD seems to be gaining popularity as a more complete syntax for expressing a verifiable credential. The contextual information enables the Verifier to ensure that they understand the meaning of the data attributes contained in a verifiable credential simply by interpreting the message while referencing the identified schema that provides the full context of all that could be included in the credential.

| [EXAMPLE 1](https://www.w3.org/TR/vc-data-model/#example-1-a-simple-example-of-a-verifiable-credential): A simple example of a verifiable credential  {  **// set the context, which establishes the special terms we will be using**  **// such as 'issuer' and 'alumniOf'.**  "@context": [  "https://www.w3.org/2018/credentials/v1",  "https://www.w3.org/2018/credentials/examples/v1"  ],  **// specify the identifier for the credential**  "id": "http://example.edu/credentials/1872",  **// the credential types, which declare what data to expect in the credential**  "type": ["VerifiableCredential", "AlumniCredential"],  **// the entity that issued the credential**  "issuer": "https://example.edu/issuers/565049",  **// when the credential was issued**  "issuanceDate": "2010-01-01T19:73:24Z",  **// claims about the subjects of the credential**  "credentialSubject": {  **// identifier for the only subject of the credential**  "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",  **// assertion about the only subject of the credential**  "alumniOf": {  "id": "did:example:c276e12ec21ebfeb1f712ebc6f1",  "name": [{  "value": "Example University",  "lang": "en"  }, {  "value": "Exemple d'Université",  "lang": "fr"  }]  }  },  **// digital proof that makes the credential tamper-evident**  **// see the NOTE at end of this section for more detail**  "proof": {  **// the cryptographic signature suite that was used to generate the signature**  "type": "RsaSignature2018",  **// the date the signature was created**  "created": "2017-06-18T21:19:10Z",  **// purpose of this proof**  "proofPurpose": "assertionMethod",  **// the identifier of the public key that can verify the signature**  "verificationMethod": "https://example.edu/issuers/keys/1",  **// the digital signature value**  "jws": "eyJhbGciOiJSUzI1NiIsImI2NCI6ZmFsc2UsImNyaXQiOlsiYjY0Il19..TCYt5X  sITJX1CxPCT8yAV-TVkIEq\_PbChOMqsLfRoPsnsgw5WEuts01mq-pQy7UJiN5mgRxD-WUc  X16dUEMGlv50aqzpqh4Qktb3rk-BuQy72IFLOqV0G\_zS245-kronKb78cPN25DGlcTwLtj  PAYuNzVBAh4vGHSrQyHUdBBPM"  }  } |
| --- |

### Verifiable credential containers

Now that we understand the options for the basic syntax of expressing the information in a verifiable credential, there is a second syntactical consideration. Specifically, how the credential data packaged such that its authenticity and integrity can be verified.

Earlier, when we described tokens, we introduced JWT as a method that can be applied here to the packaging of a verifiable credential. Verifiable credential data, expressed in either JSON or JSON-LD form, may be packaged as a JWT.

In December 2020, a draft of a proposed specification for [Linked Data Proofs](https://w3c-ccg.github.io/ld-proofs/) (LD-Proofs) was published that defines another method. Much like the impetus for the creation of JSON-LD, LD-Proofs seeks to embed additional context to help the receiver of a claim interpret it. In essence, LD-Proofs proposes a method and syntax for embedding all the information needed to perform signature verification. It does this by defining a standardized JSON-LD format for the expression of the information to decrypt and perform signature verification. Information such as proof type, verification method, purpose of the credential, and the proof values that are to be interpreted are brought together in one standardized information package.

| [EXAMPLE 2](https://www.w3.org/TR/vc-data-model/#example-2-a-simple-example-of-a-verifiable-presentation): A simple example of a verifiable presentation  {  "@context": [  "https://www.w3.org/2018/credentials/v1",  "https://www.w3.org/2018/credentials/examples/v1"  ],  "type": "VerifiablePresentation",  **// the verifiable credential issued in the previous example**  "verifiableCredential": [{  "@context": [  "https://www.w3.org/2018/credentials/v1",  "https://www.w3.org/2018/credentials/examples/v1"  ],  "id": "http://example.edu/credentials/1872",  "type": ["VerifiableCredential", "AlumniCredential"],  "issuer": "https://example.edu/issuers/565049",  "issuanceDate": "2010-01-01T19:73:24Z",  "credentialSubject": {  "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",  "alumniOf": {  "id": "did:example:c276e12ec21ebfeb1f712ebc6f1",  "name": [{  "value": "Example University",  "lang": "en"  }, {  "value": "Exemple d'Université",  "lang": "fr"  }]  }  },  "proof": {  "type": "RsaSignature2018",  "created": "2017-06-18T21:19:10Z",  "proofPurpose": "assertionMethod",  "verificationMethod": "https://example.edu/issuers/keys/1",  "jws": "eyJhbGciOiJSUzI1NiIsImI2NCI6ZmFsc2UsImNyaXQiOlsiYjY0Il19..TCYt5X  sITJX1CxPCT8yAV-TVkIEq\_PbChOMqsLfRoPsnsgw5WEuts01mq-pQy7UJiN5mgRxD-WUc  X16dUEMGlv50aqzpqh4Qktb3rk-BuQy72IFLOqV0G\_zS245-kronKb78cPN25DGlcTwLtj  PAYuNzVBAh4vGHSrQyHUdBBPM"  }  }],  **// digital signature by Pat on the presentation**  **// protects against replay attacks**  "proof": {  "type": "RsaSignature2018",  "created": "2018-09-14T21:19:10Z",  "proofPurpose": "authentication",  "verificationMethod": "did:example:ebfeb1f712ebc6f1c276e12ec21#keys-1",  **// 'challenge' and 'domain' protect against replay attacks**  "challenge": "1f44d55f-f161-4938-a659-f8026467f126",  "domain": "4jt78h47fh47",  "jws": "eyJhbGciOiJSUzI1NiIsImI2NCI6ZmFsc2UsImNyaXQiOlsiYjY0Il19..kTCYt5  XsITJX1CxPCT8yAV-TVIw5WEuts01mq-pQy7UJiN5mgREEMGlv50aqzpqh4Qq\_PbChOMqs  LfRoPsnsgxD-WUcX16dUOqV0G\_zS245-kronKb78cPktb3rk-BuQy72IFLN25DYuNzVBAh  4vGHSrQyHUGlcTwLtjPAnKb78"  }  } |
| --- |

## Blockchain

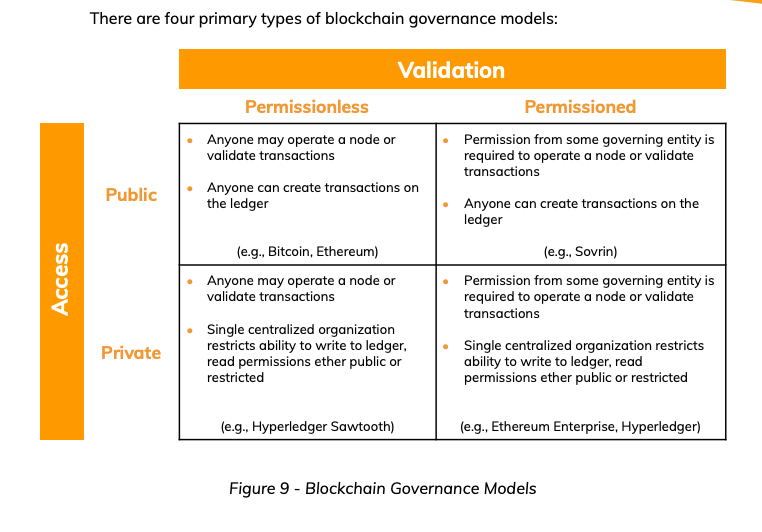
We have previously identified blockchain technology as the common implementation of the distributed ledger used in a decentralized ecosystem. We have said that this form of information storage can be made widely available and is immutable, and therefore its integrity as a database inherently trustable.

How is this possible? Let’s explore how blockchain works, then we will apply it to how it is used for digital identity.

First, we need to understand that there are several types of blockchain implementations. The blockchain approach for cryptocurrency ( Bitcoin, etc.) is significantly different to that used for digital credentials. Blockchain networks can be *permissionless* or *permissioned*. In permissionless implementations, anyone with the computing resources can become a *node* (i.e., maintain a copy of the blockchain database) in the network. When something is added to this type of blockchain implementation, significant computing resources are applied to find a mathematical proof of the validity of a transaction, or a block of transactions. The Bitcoin miners you may have heard of perform this function.

### Permissioned Implementation of Blockchain

Blockchain as implemented for digital credentials is most often based on a permissioned implementation of blockchain. This means that certain activities require access permission. A network is described as closed when all activities performed on the blockchain, including its access (read) and the ability to add (write) to the blockchain, requires permission. As we will see in this section, the model being used for most globally accessible digital credentials implements a model where (read) access is open, while permission to modify (write) the blockchain is limited. For example, only a recognized trusted issuer should receive permission, based on the blockchain network’s governance principles and procedures, to issue credentials that will be supported within the network. Blockchain node operators must similarly be permissioned to operate a node. While only trusted issuers can write to the blockchain, anybody can verify. Not that dissimilar to what we experience today - only recognized motor vehicles offices can issue valid driver’s licenses, but anybody can verify them. The illustration below, from [SOVRIN](http://sovrin.org), identifies the common types of blockchain implementations and examples of where each have been used.



In this type of permissioned implementation, there are different types of blockchain nodes. Some nodes are simply there to provide access points for the reading of data from the blockchain. This supports the broad decentralization of the blockchain and distributes the workload such that no one copy of the blockchain is overloaded with network traffic. This protects against common types of attacks such as denial of service and provides limitless scalability for this type of blockchain implementation.

There are a smaller number of nodes that perform the key function of validating whether something can be written to the blockchain. These are often referred to as *stewards*. The number of stewards is limited because a form of consensus must be achieved among the stewards before data is written to the blockchain. Too many stewards and this process becomes inefficient (i.e., takes too long, consumes too many resources), too few and the value of multiple independent parties agreeing to record a transaction is lost. Experimentation with Hyperledger Indy (more on that later) seems to indicate that approximately 25 stewards is optimal.

When there is a transaction to be written to the ledger, stewards are responsible for ensuring that it is valid and can be recorded. Elements of this include whether it is properly formed, and comes from an authorized source. The stewards must achieve a consensus agreement that the transaction is valid and recorded in the right order. One of the commonly used methods is called [Plenum](https://hyperledger-indy.readthedocs.io/projects/plenum/en/latest/main.html), we will not explore it inner workings in detail - suffice to say that a quorum of stewards must agree the transaction is valid and recorded in the right order before it is written, and the definition of quorum and how it is achieved varies with the consensus method employed.

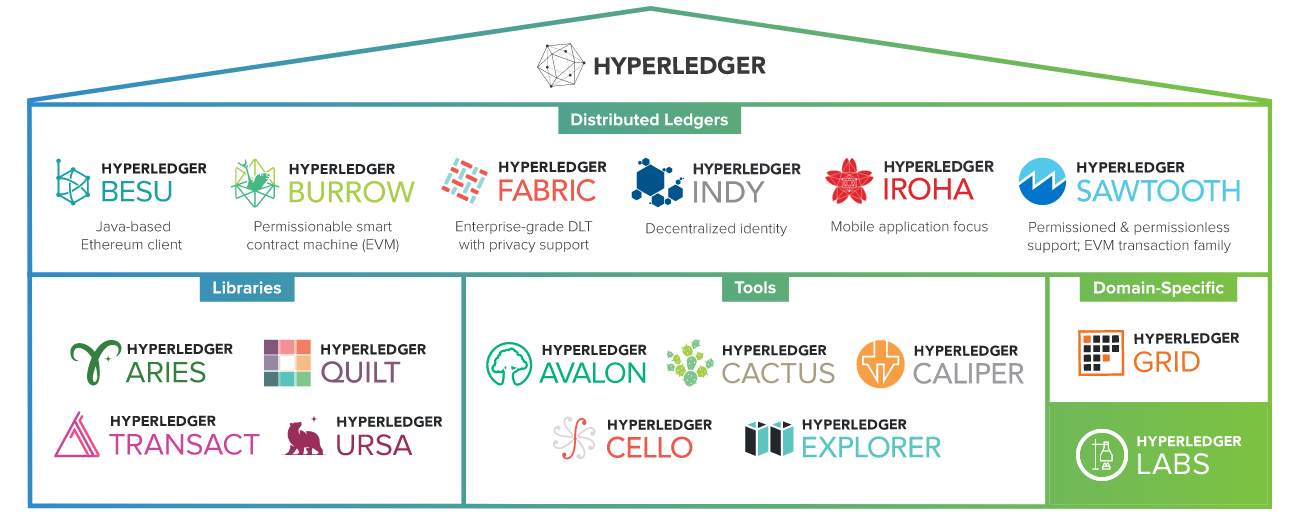
### More on Blockchain

Now that we have a sense of how data is stored on the blockchain, how can we say it is immutable? This relies on a technique called hashing. Hashes are used to verify if something has changed. Cryptography algorithms are used to generate a hash value. The hash value for data of any size is always the same length. The most popular at the moment is based on SHA256 and generates a 32 character hash. One word fed into the algorithm, or the content of a full novel, will generate a unique 32 character hash. The number of possible unique values for this hash is approximately 10 followed by another 77 zeros. This means the hash is statistically unique. This is really important because one can trust that if *any character of data in a block changes, then its hash will be different*. In the type of permissioned blockchain networks we are examining, the hashes are generated using a technique called [*Merkle Tree*](https://en.wikipedia.org/wiki/Merkle_tree). Essentially a series of interdependent hashes such that changing one transaction results in a different set of hashes. When these are present in every node on the network, compromised data (i.e., nodes) can easily be recognized and removed from the blockchain network until the node is re-synchronized with valid data. It is virtually impossible that all nodes could be compromised at the same moment in time.

Note to Bruce - we should have a few lines about best practices adopted by the identity industry when using blockchain - > no personal data stored on the blockchain.

### Hyperledger

The evolution of the blockchain technology used in digital credential solutions is largely contained in a family of emerging standards projects under the umbrella of [Hyperledger](https://www.hyperledger.org/about), hosted by the Linux Foundation. The projects hosted by Hyperledger are identified in the figure below.



There is a subset of these projects that should be highlighted as you will probably hear their names when reference implementations of decentralized identity and approaches such as selective disclosure and zero-knowledge proof are described.

**NOTE**: that this is not an all-inclusive list of open standard development projects in the realm of blockchain for digital identity, simply a list of a few of the more active efforts used as the basis for implementations of blockchain technology for digital credentials.

Hyperledger Indy - is at the centre of Hyperledger’s identity ecosystem. This implements the base distributed ledger technology and consists of two main code libraries. The *indy-node* is the blockchain “shared database”, or distributed ledger, component of Indy, and the indy-sdk is a software development kit that enables interaction with the distributed ledger and other storage components such as digital wallets. This is a purpose-built blockchain implementation for digital identity tuned to the management of verifiable credentials and architecture models such as those we identified in previous learning units (Peer-to-Peer, triangle of trust, digital wallets, etc.).

Hyperledger Aries - provides a standardized set of protocols that enable communication with the distributed ledger and communication with a digital wallet. This is a standards-based foundation for the all-important *agents* we described in an earlier learning unit. The indy-sdk provided a consistent set of methods for performing operations such as read-write to the distributed ledger, or information storage in an implementation of a digital wallet. However, when it came to creating the agents that transact with the ledger and each other, there was a proliferation of purpose-built implementations that did not usually transact with agents built by others. This led to the creation of Aries to develop the standards that will allow agents to interoperate. Aries is focussed on the operations to transmit, store, and use verifiable credentials. Some of the original capabilities in the Indy project are being migrated to Aries.

Hyperledger Ursa - is a result of acknowledgement that the cryptography libraries in Indy should really be a distinct project to maximise cryptographic capability reuse and facilitate maintenance. Usage by other projects, under the Hyperledger umbrella or not, became easier. The cryptographic elements of the Indy project were migrated from Indy to form the initial Ursa library.

## Selective disclosure

### Introduction to Selective Disclosure Technology

In an earlier learning unit, we defined selective disclosure, which discloses only what needs to be disclosed for the purpose at hand. Further, we presented the most complex scenario where a subset of attributes from multiple credentials were required to execute selective disclosure to a Verifier.

The technologies we have introduced so far do not by themselves support selective disclosure. In order to preserve the security and integrity necessary in a digital identity ecosystem, the Verifier must be able to be certain of a credential’s origin and that the Holder who is presenting those credentials is who they say they are. The technologies presented so far assume that the entire credential is signed by the Issuer. In a selective disclosure scenario, it is necessary to present only a subset of the credential. Breaking apart a credential in this manner would invalidate the Issuer’s signature and result in the Verifier not being able to systematically assure themselves of the credential’s origin.

To implement selective disclosure, there are a few more technologies and methods we should describe.

### Multi-message Digital Signatures

To enable selective disclosure, it is necessary *that the Issuer sign any individual piece of information that may be used independently*. For selective disclosure, this means every individual attribute in the credential. Traditional digital signature schemes are based on signing a message in its entirety, not the individual pieces.

Recently, a specification called [BBS+ Signatures](https://w3c-ccg.github.io/ldp-bbs2020/) was published as a draft specification that enables the signing of an array of messages. In the case of a verifiable credential, each of the attributes of an issued credential can be signed.

There are other multi-message signing methods out there. We have highlighted BBS+ Signatures because it also incorporates cryptography that delivers zero-knowledge proofs to the Verifier. Essentially, the ability to parse a credential into its component pieces AND present it in such a way that the credential value is not necessarily transmitted, simply an immutable proof of its issuance.

This provides the missing piece to enable effective selective disclosure without compromising the ability of the Verifier to assure themselves of the origin of the credential claim. This capability, combined with the inherent capability of JSON-LD syntax to deliver information context, allows for the extraction of pieces of credentials into a cohesive presentation while ensuring that the context for each of the attributes accompanies the data - thereby enabling the Verifier to interpret the claim.

### Example of Selective Disclosure

Now that we have identified most of the important technologies, let’s look at selective disclosure in action.

As an example, when challenged for proof of age, currently we provide something like a driving licence that shows our picture (so it can be determined if the licence belongs to the Holder) and the birth date. However, the Verifier also gets to see home address and the rest of the credential’s information. Information that is not required for their purposes. Selective disclosure would show only the two necessary pieces of information to the Verifier.

Let’s step through the issuance and use of a verifiable credential that is suitable for selective disclosure. As noted earlier, there are multiple technology methods that have been experimented with to enable selective disclosure. For the purposes of our example, we will assume the use of [JSON-LD](https://www.w3.org/TR/json-ld11/) with [BBS+ Signatures](https://w3c-ccg.github.io/ldp-bbs2020/) as that approach seems to be gaining some traction as the best option for achieving selective disclosure, with the added benefit of implementing Zero-Knowledge Proof (ZKP).

1. Creation and Issuance:

The Issuer will go through their business process and decide to issue a credential. This credential will use the W3C Verifiable Credential Data Model to construct our credential. The use of JSON-LD will provide enhanced syntax that embeds context with information in the issued credential.

The next step is to digitally sign the created credential. This is where the first important requirement occurs. The signing method must be one that supports selective disclosure. BBS+ Signatures is one such method that gives us *multi-message signing* capability. Multi-message signatures enable the downstream parsing of a credential such that only required identity attributes are exposed to a Verifier. A multi-message signature scheme is required with credential issuance, If the credential is not signed in a manner that supports selective disclosure it does not matter if the Holder’s digital wallet can construct a selective disclosure claim or the Verifier can interpret a selective disclosure claim.

Of course, the public keys used for signing must be made available. The most popular approach is to use DID(s) as defined in the Decentralized Identifiers standard being developed at W3C. Created DIDs may be stored either on the distributed ledger (if required to be widely available) or with the Holder (if required only for a specific credential exchange).

During construction of the credential, the issuer will use a public key made available by the Holder to inextricably link the credential to the Holder and enable downstream proof of the trustworthiness of the issuance process. In our example, each of the credential attributes are then digitally signed using BBS+ Signatures. The use of JSON-LD and its embedded contextual information helps us understand that this set of individually signed claims can be combined into a higher-level construct - in this case a driving licence.

The credential is then issued to the Holder and they place it in their wallet. There is another implied assumption here, specifically, that the Issuer and the Holder’s wallet technology both understand the secure methods for this connection and verifiable credential transfer. There are several methods to accomplish this that we will not address in this learning series.

1. Presentation and Use of the Verifiable Credential:

Our Holder now has a selective-disclosure-ready verifiable credential in their digital wallet.

The Verifier must inform the Holder what information is required. There is a collaborative community development effort underway to mature a standardized set of methods to exchange a verifiable credential presentation, the first step of which is to formulate and understand a request for information. You can reference this work on a verifiable credential [Presentation Exchange](https://identity.foundation/presentation-exchange/) protocol being undertaken at the Decentralized Identity Foundation ([DIF](https://identity.foundation/)).

The Holder’s wallet then assembles a claim from a subset of the signed attributes received from the Issuer, and digitally signs the claim package. This presentation of a verifiable claim is given to the Verifier. For our purposes, we will assume the method used here is a secure method that preserves trust in the integrity of the exchange.

The Verifier now has a verifiable claim consisting of a message (or claim presentation) (signed by the Holder) that contains individual claims signed by the Issuer. The Verifier, leveraging public keys stored on the distributed ledger can now verify the Holder’s signature(s) to ensure that the message has indeed been sent by the Holder they think they are dealing with, and uses the Issuer’s public keys to assure themselves that the credential came from the expected Issuer.

Further, the use of JSON-LD with BBS+ Signatures enables the option for the verifiable credential presentation to deliver only the information required for a ZKP , and not the identity attribute data values.

This use case has been presented at a relatively high level. Significant study will be required to fully understand the intricacies of how this works at the lowest technology levels. The standards required are available by following the links in this learning unit. In addition the following two resources were useful references when the drafting of parts of this learning unit.

[Verifiable Credentials explained](https://www.lfph.io/wp-content/uploads/2021/02/Verifiable-Credentials-Flavors-Explained.pdf), published by the [Covid-19 Credentials Initiative](https://www.covidcreds.org/) and a short [simplified explanation of selective disclosure and multi-message signing](https://learn.mattr.global/concepts/selective-disclosure) published by [MATTR](https://learn.mattr.global/).

### Check Your Understanding

Instructions: In this activity, you will select either true or false for the associated question. When finished, select Submit at the bottom of the page.

1. Linked Data standards are used to link credentials from different Issuers. (false)
2. JSON-LD extends JSON syntax to provide information context. (true)
3. A JWT, containing a verifiable credential, must use JSON-LD. (false)
4. Blockchain technology for digital identity is usually different from the one used for cryptocurrency. (true)
5. BBS+ Signatures is a required component of selective disclosure. (false)
6. Hash values are used to provide sequential linking of data blocks in a blockchain database. (true)
7. Standards for peer-to-peer digital identity ecosystem models are not yet mature and widely adopted. (true)
8. The proposed LD-Proofs specification seeks to embed all information required to perform signature verification. (true)
9. LD-Proofs replace the need for JSON-LD. (false)
10. DIDs are primary containers for credential information. (false)
11. Multi-message signatures of some sort are required to attempt a selective disclosure system. (true)

## Interview with Experts

### Interview with Kaliya Young (Identity Woman)

Here to give us some additional insight into the sea-change that some of these technologies can represent for us is noted advocate for evolution in the world of digital identity Kaliya Young. Kaliya is an expert in self-sovereign identity and identity on the blockchain. She is the co-author of a Comprehensive guide to Self-Sovereign Identity, and a co-founder of the annual Internet Identity Workshop.

<<Kaliya Young interview goes here>>

### Interview with John Jordan

We had the opportunity to speak with John Jordan, executive director of the BC Digital Trust Service. Mr. Jordan has been at the forefront of innovation in the delivery of services dependent on digital credentials.We speak with John about some of the emerging technologies in the area of digital credentials and how the Public Sector in Canada can position themsleves to leverag these important advancements..

## Conclusion

This learning unit has described some of the technologies commonly used to implement standards-based digital credentials. However, as we noted several times, there are many emerging standards developed or under development. We have attempted to identify and describe those that we feel are most important. However, if your learning quest is one where your goal is to become a digital credential expert, you should view this material as a good starting point in your journey and study the more detailed material linked to throughout this learning series.

In this learning unit, we identified some of the most commonly used open standards embedded in systems used to deliver federated credential models. As well, we have identified some of the most prominent among the emerging technologies and open standards supporting peer-to-peer models and verifiable credentials.

As noted in this learning unit, federated approaches to digital credentials are the most prevalent models currently in place and operating. However, peer-to-peer approaches that are maturing are gaining traction and appear to be the next wave in the evolution of digital credentials, an evolution that systematically implements the privacy enhancing principles outlined in previous units in this learning series.

## Unit 7 Quiz

1. OpenID Connect is an \_\_\_\_\_\_\_\_\_\_\_ (interoperability, authorization, **authentication**, encryption) standard.
2. Cryptographic hashes are susceptible to reverse engineering and this must be guarded against. (True, **False**)
3. One of the first broadly adopted XML-based open standards for passing identity data between an identity provider and the entity providing online service was called \_\_\_\_\_\_\_\_\_\_\_. (XACML, SGML, **SAML**, IDXML)
4. Linked Data standards extend existing technology standards to provide \_\_\_\_\_\_\_\_\_\_ for the data being exchanged. (better security, enhanced interoperability, **context**, other methods)
5. A Verifier of a verifiable credential must consult the credential Issuer to ensure the credential is valid. (True, **False**)
6. Oauth is an \_\_\_\_\_\_\_\_\_\_\_ (interoperability, **authorization**, authentication, encryption) standard.
7. One of the foundational technology requirements for implementing selective disclosure is (choose BEST one) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. (JWT, Oauth, **multi-message signatures**, blockchain)
8. OpenID Connect leverages Oauth approaches to message exchange. (**True**, False)
9. Oauth processes XML messages faster. (True, **False**)
10. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ is a collaborative community development effort underway to mature a standardized set of methods to exchange a verifiable credential claim in a way that supports selective disclosure. (JSON-LD, BBS+ Signatures, **Presentation Exchange**, ZKP)
11. ZKP is a key component of selective disclosure. (True, **False**)
12. One of the key functions of a DID document is to store the \_\_\_\_\_\_\_\_\_\_ required to verify credentials. (private keys, credential attributes, SAML assertions, **public keys**, linked data)
13. The distributed ledger is used to securely store credential data from verifiable credentials. (True, **False**)
14. In a verifiable credential scheme, the \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ enables verification of a credential without having to consult directly with the Issuer. (linked data, **distributed ledger**, JSON-LD, multi-message signature, JWT)
15. JWT is an example of a \_\_\_\_\_\_\_\_\_\_\_\_\_\_. (credential, digital signature method, message exchange standard, **security token**)
16. JWT, JWE, and JWS are standards published by \_\_\_\_\_\_\_\_\_\_\_\_\_. (**IETF**, ISO, OASIS, W3C)
17. \_\_\_\_\_\_\_\_\_\_ includes the concepts of including explicit consent to access a resource in the message exchange. (SAML, **Oauth**, BBS+ Signatures, JWT)
18. \_\_\_\_\_\_\_\_\_\_\_\_\_ is an identity layer that leverages the framework used for OAuth
    1. Security Assertion Markup Language (SAML)
    2. OAuth
    3. \*OpenID Connect (OIDC)
    4. Security Tokens
19. To enable selective disclosure, it is necessary that the Issuer sign any individual piece of information that may be used independently
    1. \*True
    2. False
20. Blockchain as implemented for digital credentials is most often based on a permissionless implementation of blockchain.
    1. True
    2. \*False
21. \_\_\_\_\_\_\_are used to verify if something has changed
    1. JSON
    2. LD-Proofs
    3. Blockchain
    4. \*Hashes

1. Matt McKinney, “Understand Verifiable Credentials in 10 Minutes”, <https://www.arcblock.io/blog/en/post/2020/04/15/verifiable-credentials> [↑](#footnote-ref-0)
2. ToIP Foundation, “Introducing the Trust over IP Foundation”, <https://trustoverip.org/wp-content/uploads/sites/98/2020/05/toip_introduction_050520.pdf> [↑](#footnote-ref-1)
3. ToIP Foundation, “Introducing the Trust over IP Foundation”, <https://trustoverip.org/wp-content/uploads/sites/98/2020/05/toip_introduction_050520.pdf> [↑](#footnote-ref-2)