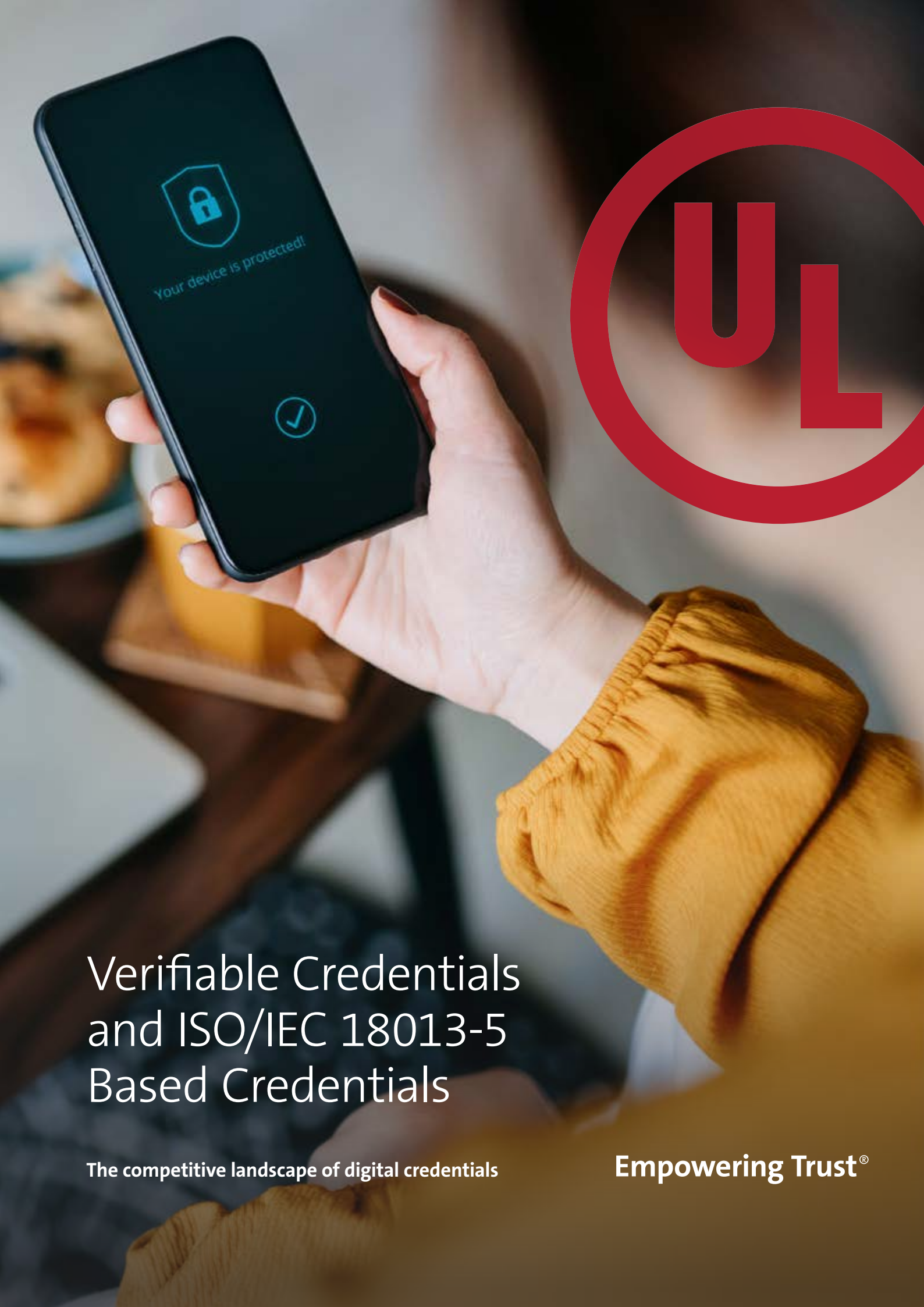


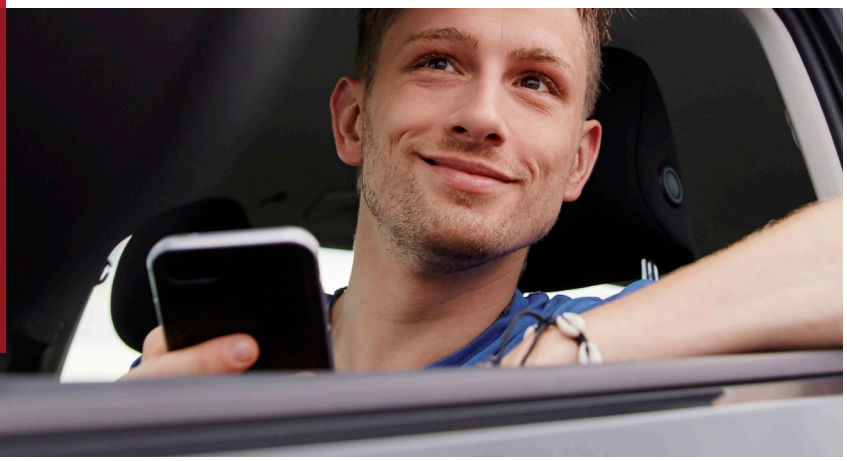
Verifiable Credentials and ISO/IEC 18013-5 Based Credentials

The competitive landscape of digital credentials

Empowering Trust®

Table of contents

Management summary



This UL white paper discusses two types of digital credentials, namely credentials that comply with the ISO/IEC 18013-5 standard for mobile driving licenses and Verifiable Credentials (VCs), which comply with the Verifiable Credential Data Model specification published by the World Wide Web Consortium (W3C). The credentials described in each document have a similar purpose and both approaches aspire to be widely deployed, interoperable and support a broad range of real-world use cases. The ISO/IEC standard and the W3C Recommendation however, differ in scope, origin and motivation. Consequently, while many of the goals are aligned, technical details as well as the scope and maturity of core and supplemental standards differ between the two bodies of work.

This white paper discusses the origins and goals of the ISO/IEC 18013-5 standard[1] as well as the VC data model, as stated in these documents themselves in **Chapter 2**.

Chapter 3 compares the two types of digital credentials on the following:

- **Specified scope –** Whereas the VC Data Model only describes a data model, ISO/IEC 18013-5 also specifies communication protocols, data encodings and security mechanisms.
- **Architecture –** The roles and interactions specified in both standards are similar. In particular, the role of the Verifiable Data Registry (VDR) in a VC ecosystem can be compared to the role of the optional Verified Issuer Certificate Authority List (VICAL) in an ISO/IEC 18013-5 based ecosystem. We argue that the VICAL is, in fact, a possible implementation of a VDR, alongside more common choices such as a blockchain or distributed ledger. However, the VICAL is optional and is, in any case, not required during every single transaction.
- **Data model –** In particular, the way in which ISO/IEC 18013-5 can be used as a basis for another type of digital credential besides the mobile driving license. This can be done by defining a new document type and/or a new namespace for data elements of the new credentials.
- **Communication protocols –** In particular, the communication protocols specified for use by ISO/IEC 18013-5. As noted, the VC Data Model does not prescribe any specific communication protocols.
- **Security aspects –** This white paper discusses and compares the two specifications' different security mechanisms. ISO/IEC 18013-5 specifies a number of mandatory security mechanisms for each of the interfaces within the scope of the standard. These mechnaisms are designed to mitigate a wide range of threats, from loss of authenticity to cloning credentials. On the other hand, the VC Data Model requires that the authenticity of a verifiable credential is ensured by means of cryptographic proof, but it does not require any specific proof mechanism, leaving the choice to implementers.
- **Privacy aspects –** Both specifications allow the holder of the digital credential to be in full control of the credential. In particular, within the scope of the specifications, the issuer cannot disclose the credential to a verifier without the holder's knowledge and consent. Furthermore, both specifications support privacy-enhancing measures, such as data minimization and selective disclosure. ISO/IEC 18013-5 requires the use of an indirect signature using multiple levels of hashing to ensure the possibility of selective disclosure. The VC Data Model points out that the same property can also ensure this by using an appropriate zero-knowledge proof (ZKP) mechanism.

From the comparison above, it is clear the VC Data Model does not have the intention to specify all aspects necessary for interoperability between different implementations of the standard. In particular, the lack of common communication protocols, data encodings and security mechanisms means different implementations will generally not be interoperable. For each use case, protocols for establishing connections, requesting and transferring credentials and other credential-based interactions must additionally be addressed in related documents. UL therefore believes that parties wishing to create a verifiable credential will benefit from combining their new credential with some of the mechanisms specified in ISO 18013-5. **Chapter 4**, therefore, discusses four possible ways in which a verifiable credential can be combined with ISO/IEC 18013-5. These possibilities range from storing a verifiable credential in an application that also supports documents based on ISO/IEC 18013-5 without changing the VC in any way, to implementing the verifiable credential as a document that complies with ISO/IEC 18013-5, thereby changing its

format completely. This white paper outlines some of the advantages and drawbacks of each possibility and closes by highlighting a few areas in which further standardization by both ISO/IEC and the W3C would be beneficial.

1 – Introduction

1.1 – Credentials

Abilities and experiences, or credentials, can make us suitable for a particular job or activity. These credentials can manifest in many areas of our lives, such as:

- Education, e.g., having attending high school
- Capabilities, e.g., the ability to drive a heavy goods vehicle
- Personal history, e.g., birth date and location, veteran status
- Medical information, e.g., having a disability, vaccination status
- Legal or professional status, e.g., citizenship with another country, member of the press, diplomat
- Membership or patronage, e.g., with a library, sports club, insurance company
- Human relationships, e.g., being a person's parent or legal custodian

The word 'credential' also has a second meaning. Apart from signifying an ability or experience, it can also be used to indicate a document or statement that proves that a person has that ability or experience. After all, anyone can claim to have an ability or experience, but in many cases, proof is necessary. This typically comes in the form of a document issued by an authority. For example, one can prove citizenship with a passport issued under the responsibility of the relevant government. To be accepted by a university, evidence of prior learning or experience may have to be signed by a representative of an educational institution. A doctor or hospital may give a person a medical record that allows them to prove they have specific medical needs.

This white paper will use the word "credential" in this second sense, i.e., as proof of an ability or experience. Such a credential is provided to the subject or holder by an issuer.[2] A verifier — sometimes called a "relying party" — will accept that the holder does, in fact, possess the abilities or experiences asserted in the credential, as long as they can validate the credential is authentic and the issuer is trustworthy.

A credential typically contains the following:

- Information on the **subject**, such as their name, portrait or signature. This is used to bind a credential to its subject, who is often also the credential holder.
- Information on the **credential itself**, such as a description of the credential type, a document number or a validity period.
- Information on the **issuer** of the credential, such as their name and qualifications.
- Information on the specific abilities or experiences — often called **attributes** — of the subject, which the issuer is asserting by means of the credential.

A typical example is the so-called Visual Inspection Zone (VIZ) of an international passport, as standardized by the International Civil Aviation Organization (ICAO). This is depicted in Figure 1. Information binding the subject to the holder is indicated with a blue background, credential information is in red, issuer information in gray and attributes in green.[3]

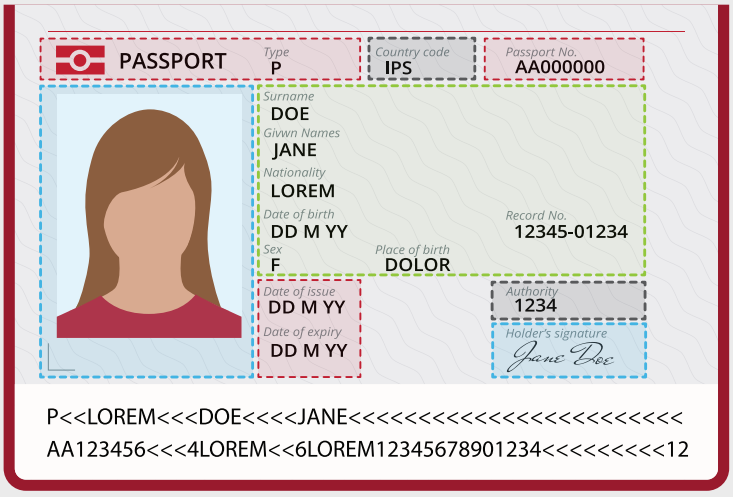


Figure 1 – Visual Inspection Zone of an ICAO passport with several categories of information.

Physical credentials in the form of a piece of paper have been with us for centuries. They are used for many purposes and in many contexts, including entering a country or building, being allowed to view classified information, enrolling in a university, applying for a job or receiving medical care. Typically, physical credentials are protected against change and forgery by various security measures, such as the subject's signature or portrait, difficult-to-reproduce printing techniques or watermarks.

Digital credentials are the virtual counterparts to physical credentials. Digital credentials exist in electronic forms and are protected using logical security measures such as cryptography. This type of credential first emerged when traditional issuers of physical credentials started issuing electronic versions. This began over 20 years ago with the issuance of bank cards and SIM cards, soon followed by healthcare cards, electronic passports and many more.

In many cases, a digital credential is combined with its physical counterpart in a single document. However, these credentials are increasingly being further digitized so they can be stored on mobile phones or tablets, in the same way payment data is with Apple Pay or Android Pay. The most recent development in this area is a standard to digitize the international driving license, i.e., ISO/IEC 18013-5 [1]. This standard specifies the requirements for the so-called mDL, but can also be used for other types of credentials.

A quite different approach to digital credentials originated from internet-based companies and organizations collaborating within the World Wide Web Consortium (W3C). This effort was completely independent of the developments described above. Rather than attempting to digitize existing physical credentials, people started thinking about ways to solve the problem of using and proving the legitimacy of any credentials in the virtual world. A key concept here is self-sovereign identity — the principle that the credential holder should have full control over their credential. In this context, the W3C started the specification of verifiable credentials. These credentials are not an evolution of existing physical credentials. Rather, they are an attempt to allow any person or entity to express a digital credential on the internet about any subject while also allowing the preservation of the credential's subject's privacy.

1.2 – This white paper

The pace of developments in the field of digital credentials has left many industry stakeholders puzzled, especially regarding the relative merits of the two types of digital credentials discussed in the previous section. On the one hand, there are verifiable credentials as specified by World Wide Web Consortium (W3C), and on the other, there are credentials based on ISO/IEC 18013-5, such as mobile driving licenses. UL has received questions about this topic several times. What are the characteristics of each solution? What are their respective possibilities and limitations? Are they competing or complementary? Can they be combined?

This white paper attempts to answer these questions by making an explicit comparison between these two technologies in Chapter 3, then explores the ways in which the technologies can be combined in Chapter 4. Chapter 2 gives an overview of the backgrounds, ecosystems and goals of both verifiable credentials and credentials based on ISO/IEC 18013-5.

2 – Overview of ISO/IEC 18013-5 and the VC data model

2.1 – ISO/IEC 18013-5

2.1.1 – Background

As explained in the Introduction of this white paper, a mDL is the latest development in the evolution from traditional physical credentials to electronic and digital representations of such credentials. This evolution has been ongoing for over two decades and includes electronic banking cards, healthcare cards, electronic passports and electronic driving licenses.

There are two major differences between these earlier credentials and the mDL. Firstly, the earlier credentials are all limited to one type of document. There is, for instance, no way to use the specifications for mobile banking cards to create a digital variety of healthcare cards. In contrast, ISO/IEC 18013-5 can be used to easily specify many types of credentials, although it primarily specifies the mDL. One only has to specify the attributes needed for a new credential while keeping all other aspects of the standard the same. Please refer to Section 3.4.1 for more information on how this can be achieved.

Secondly, most earlier electronic documents are in the form of an integrated circuit card. This means they use interfaces, communication protocols and data formats that are both specific to such cards and very limited in data throughput, message size and physical interface. This limits usefulness in situations where credentials are required to be validated remotely, such as across the internet. In contrast, the fact that an mDL lives on a mobile device allows for the use of more common, versatile communication protocols and data formats. It also allows for enhanced privacy features, such as user consent, data minimization and selective disclosure. All of these will be discussed in detail in Chapter 3.

2.1.2 – Ecosystem

The mDL is standardized in the International Standard ISO/IEC 18013-5 [1].

Figure 2 shows the main components and associated roles and interfaces in the mDL ecosystem, as presented in this standard.

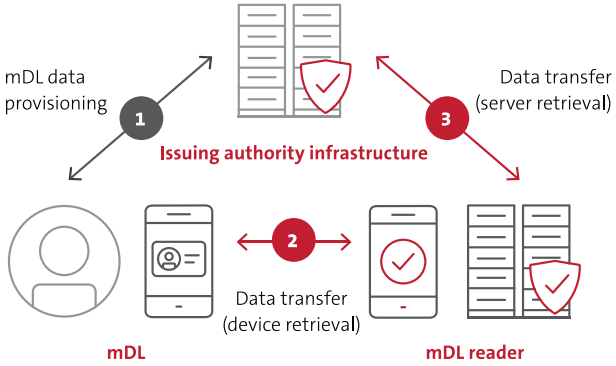


Figure 2 — mDL ecosystem components, roles and interfaces

Figure 2 shows the following:

- Interface 1 is the interface between the infrastructure of an issuer and an mDL provided by that issuer. The issuer can use this interface to provision and personalize an mDL on the holder's mobile device and to manage the mDL throughout its lifetime. This interface is out of the scope of ISO/IEC 18013-5 but is currently being worked on for the upcoming ISO/IEC 23220 series of standards.
- Interface 2 is the short-range interface between an mDL and an mDL reader. The mDL reader is operated by an mDL verifier. This interface is fully specified in ISO/IEC 18013-5 and must be implemented by an mDL as well as an mDL reader.
- Interface 3 is the remote interface between an mDL reader and the infrastructure of an mDL issuing authority. This interface is also fully specified in ISO/IEC 18013-5. However, implementation of this interface is optional for both the issuing authority and the mDL reader.

ISO/IEC 18013-5 standardizes two methods that a verifier can use to obtain a set of mDL data from an mDL. First, the mDL reader can obtain data from the mDL itself using interface 2. This is called device retrieval. Second, the mDL reader can use interface 3 to obtain mDL data from the mDL issuing authority infrastructure, provided the issuing authority supports this. This is called server retrieval. The current version of ISO/IEC 18013-5 only covers the so-called attended use cases in which the holder physically presents the mDL to an mDL reader managed by a verifier. It therefore does not allow for a remote verifier to directly interact with an mDL over the internet. However, such unattended use cases are under study for the next version of the standard.

2.1.3 – Goals

The main goals of ISO/IEC 18013-5 are interoperability, extensibility, security and privacy.[4]

Interoperability means that any mDL implementation conformant to ISO/IEC 18013-5 can communicate with any conformant mDL reader, and any conformant mDL reader can communicate with the infrastructure of a conformant issuing authority. To allow interoperability, the standard specifies which communication stacks shall be supported for both interface 2 and interface 3 in Figure 2 above. This includes data transmission methods, message structures and data encoding. These communication stacks use mature technologies for which widespread and mature support exists on many (mobile) platforms. For more information, refer to Section 3.5.1.

Several test events were held during the development of the standard to verify that different mDL and mDL reader implementations, created by different manufacturers, were in fact interoperable. The results of these tests were used to improve the correctness, completeness and clarity of the provisions in the standard. Finally, a test standard, ISO/IEC 18013-6, is also currently being drafted. This test standard can be used as a basis for conformance testing and certification programs.

Extensibility is achieved mainly at the level of the data model used in ISO/IEC 18013-5. All mDL data elements are defined within the so-called mDL namespace. However, the standard allows for anyone to define their own namespace and then to define their own data elements within that namespace. This means that, besides mDLs, all kinds of other digital credentials can also be based on ISO/IEC 18013-5. Please refer to Section 3.4.1 for more information on how this can be achieved.

Security is ensured via several security mechanisms. For device retrieval, the standard specifies three mandatory security mechanisms: session encryption, issuer data authentication and mdoc authentication. All of these mechanisms are fully specified, and Section 3.6.1 of this white paper explains them in more detail. These mechanisms aim to protect the confidentiality and authenticity of both the mDL and mDL data against a wide range of attacks, such as eavesdropping or alteration of communication, replay attacks, man-in-the-middle attacks and cloning of mDL data. An optional fourth mechanism, known as mdoc reader authentication, allows authentication of an mDL reader toward an mDL. For server retrieval, the standard specifies either the use

of OpenID Connect (OIDC), which has its own security mechanisms, or the use of Transport Layer Security (TLS) in combination with JSON Web Tokens and JSON Web Signatures (JWT and JWS, respectively).

Compared to other electronic credentials, the **privacy** of the mDL holder is, in many ways, better protected by an mDL implementation. This is because the mDL standard supports selective disclosure of data elements, informed user consent and data minimization. Section 3.7.1 describes these properties in more detail. Crucially, the mDL also enhances the holder's privacy when compared to other approaches to identification and authorization, such as federated authentication and single sign-in solutions, by allowing for use offline and without the need for involvement by an issuing authority. This is not possible for federated authentication solutions. Finally, ISO/IEC 18013-5 specifies measures to avoid the ability to either link transactions or track the holder.

2.2 – Verifiable credentials

2.2.1 – Background

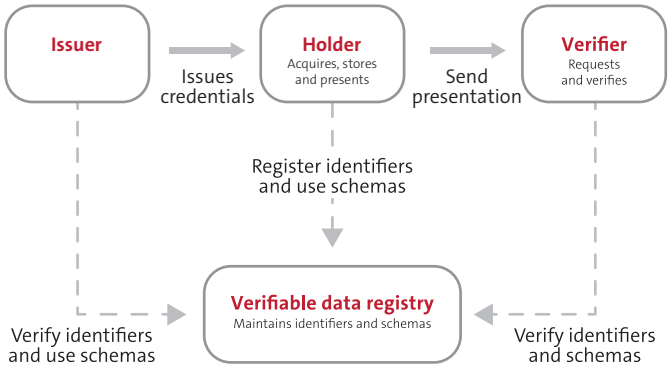
VCs originated from the W3C. The W3C perceived the need for credentials that could be used both online and in-person. These credentials would be issued by a trusted party to an individual or institution and then could be presented to a relying party who could easily and reliably verify the issuer of the credential and be confident the content had not been altered. The holder of an issued credential retains possession and complete control over who gets to see it and how it is shared. In general, once a credential is issued, the issuer is no longer required to be involved – any given verifiable interaction is permitted to happen confidentially between the holder of the credential and the relying party alone.

2.2.2 – Ecosystem

Verifiable credentials are standardized via a W3C recommendation known as the "Verifiable Credentials (VC) Data Model – Expressing verifiable information on the Web" [2]. They are further explained and enhanced in a number of other documents by the W3C, including [3] – [5].

Figure 3 shows the flow of roles and information used in the VC Data Model specification. Note that this figure is an example only, and verifiable credentials may be used in ecosystems with a different architecture.

Figure 3 – Flow of roles and information used in the VC Data Model



Apart from the roles of credential holder, credential issuer and credential verifier, Figure 3 also shows the Verifiable Data Registry (VDR). This system must be trusted by all other entities in the ecosystem. It may store identifiers, entity keys, revocation registries or issuer public keys. What is stored exactly depends on what is required to use and verify the credentials. The VDR may come in the form of a distributed ledger or blockchain.

2.2.3 – Goals

The goals of verifiable credentials, as mentioned in the VC Data Model [2], are that they must be cryptographically secure, privacy respecting, and machine-verifiable.

When it comes to **security**, each VC must contain proof that is cryptographically verifiable to ensure the authenticity of the VC. The VC Data Model specification does not, however, dictate any particular digital proof or signature format. The proof mechanism in a given implementation of the VC Data Model may range from digital signatures in a public key infrastructure (PKI) to zero-knowledge proofs (ZKPs) committed to a distributed ledger. Since the VC Data Model does not go into detail regarding proof mechanisms, protection against other security threats besides loss of authenticity are generally not covered. More information on this topic can be found in Section 3.6.

Regarding **privacy**:

- All entity identifiers used in verifiable credentials are required to be Uniform Resource Identifiers (URIs). These can be human-readable URLs, which may give hints regarding the entity's real-world identity. VCs can, however, also use so-called DIDs, which are a type of identifier that enables a verifiable, decentralized digital identity that is not human-readable. DIDs are specified in [5].
- The VC Data Model makes a distinction between verifiable credentials and verifiable presentations. A verifiable credential is a set of claims about the subject of the credential, all made by the same entity. Once a holder has received one or more VCs, they can combine several of them into a verifiable presentation. For example, if a driver is pulled over, they may present data from their driver's license as well as their vehicle registration to an officer as one verifiable presentation. In other words, a verifiable presentation is a collection of data consisting of one or more verifiable credentials. The verifiable presentation must be signed by the holder to allow the verifier to verify that all data belongs to the same holder.
- Some verifiable credentials support selective disclosure, meaning that the subject can present some claims contained in a given VC while keeping other claims secret. In order for this to be the case, the proof in the VC must typically be a ZKP. Please refer to Section 3.6.2 for more information about ZKPs.

Machine-verifiability means that a verifiable credential can be read, parsed and verified by a computer. This is what makes a verifiable credential a digital credential as opposed to a physical one.

Finally, the VC Data Model is not prescriptive in terms of how interoperability can be achieved for individual use cases or types of credentials. However, the VC Data Model does discuss some aspects of interoperability, such as semantic interoperability. But many other aspects necessary to achieve interoperability between systems are explicitly left open for implementers. As mentioned, this is true for the digital proof format used by a VC, but it also applies to requirements for VC serialization (see Section 3.4.2), and for the transmission technologies and the message structures that must be used by systems that are exchanging VCs (see Section 3.5.2). All of this means that different implementations of the VC Data Model will most likely not be interoperable in practice unless such implementations all comply with an additional standard or specification.

3 – Comparing ISO/IEC 18013-5 and the VC Data Model

3.1 – Introduction

This chapter compares verifiable credentials and credentials based on ISO/IEC 18013-5 regarding the following:

- **Scope –** Which aspects are specified in the standard and which are not?
- **Architecture –** Which components are distinguished in the ecosystem? How do these components interact?
- **Data model –** What data elements are specified in each of the standards? How should data elements be encoded? Does the standard allow others to define new data elements?
- **Communication protocols –** How can a digital credential be requested and released?
- **Security –** How do each of the standards ensure the digital credential's security? Which security mechanisms are specified? What is the trust model behind these mechanisms?
- **Privacy –** How does the digital credential ensure the holder's privacy? Which aspects of privacy are considered? What concrete measures are taken?

Each of these aspects is discussed in the sections below for both solutions. Please note that, for clarity, some of these sections contain separate subsections for ISO/IEC 18013-5 based credentials and verifiable credentials.

3.2. – Specified scope

When comparing verifiable credentials to credentials based on ISO/IEC 18013-5, one of the first things that come to mind is that the scope of what is specified in the VC Data Model [2] is much more limited than that of ISO/IEC 18013-5 [1]. The VC Data Model, as the name suggests, specifies a data model only. It does not mandate any data representation syntax, transmission technologies, data element definitions or request and response mechanisms or messages.

Obviously, this is a conscious choice. The VC Data Model tries to be as open as possible. As outlined in the specification, their approach is an "open-world assumption." This means any entity can say anything about any other entity. It also means that verifiable credentials may be used with a wide variety of technologies and in many different contexts. A drawback of this approach is that it seriously hampers the chance of two different VC implementations being interoperable without complying as well to an additional, use case-specific, specification.

Additionally, the VC Data Model intentionally leaves the specifics regarding authentication to the implementer. This means there can be no universal statement regarding the security posture or threat models to be applied to a VC implementation.

In contrast, ISO/IEC 18013-5 explicitly aims to achieve interoperability between all systems conforming to this standard. Therefore, the standard makes concrete choices for all the mentioned aspects.

3.3. – Architecture

When comparing the ecosystem used in ISO 18013-5 (Figure 2) to the ecosystem used for verifiable credentials (Figure 3), there are many similarities. Firstly, the holder plays a central role in both ecosystems. The issuer provides the credentials to the holder, who stores them on a device or repository under their control. After issuance, the holder is in complete control and is the only one who can determine to which verifier the credentials are released. The issuer is not able to release credentials directly to a verifier without the holder's knowledge and consent.

Moreover, when an mDL holder and a verifier use device retrieval to exchange credentials, neither the issuing authority nor any other party has any visibility into when or where the mDL holder uses the mDL. The same is true for a verifiable credential.

It should be noted that ISO/IEC 18013-5 differs considerably from the VC Data Model in that it also allows server retrieval.[5] If server retrieval is used, credentials are sent directly from the issuer to the verifier and, therefore, the issuer knows when and by whom the mDL is being used. However, a verifier that wants to retrieve mDL data in this way must start by interacting with the mDL to obtain a token using an mDL reader. It should not be possible for a verifier to retrieve data from an mDL issuing authority without first communicating with the mDL.[6] The standard also outlines that the issuing authority must ask for the holder's consent before releasing any data elements to the verifier.

The second difference is the location in which a digital credential is stored. The VC Data Model explicitly states that holders must be able to store verifiable credentials in any location. In contrast, a credential complying with ISO/IEC 18013-5 is always stored either on the mobile device to which it was originally issued by the issuing authority or on a server managed by — or on behalf of — the issuing authority.[7] This somewhat diminishes the level of control a holder has over their credentials. On the other hand, it significantly reduces the risk of the credentials being reused by adversaries.

Finally, a third difference between the two ecosystems is the fact that the VC ecosystem in Figure 3 shows a VDR that connects to issuers, holders and verifiers. Depending on the implementation, a verifier may need to use this VDR during each transaction. The mDL ecosystem in Figure 2 does not show or require such a system. However, in practice, a system with a similar functionality is also possible — even likely — within an mDL ecosystem. This optional system is called a Verified Issuer Certificate Authority List (VICAL) in the ISO/IEC 18013-5 standard. If present, its function is to distribute Issuing Authority CA (IACA) root certificates to verifiers in a trustworthy manner. See Section 3.6.1.2 for more information.[8] A verifier that uses a VICAL will only need to contact it periodically to check whether any new IACA root certificates have been issued or revoked.[9] The VICAL does not need to be available during each individual transaction.

3.4 – Data model

3.4.1 – ISO/IEC 18013-5

First and foremost, ISO/IEC 18013-5 specifies the mobile driving license (mDL). The attributes — called mDL data elements — defined in this standard are only those that may be needed for an ISO-compliant driving license. These data elements must be encoded in Concise Binary Object Representation (CBOR) or JavaScript Object Notation (JSON)[10], depending on whether an mDL reader retrieves the data from an mDL or from the mDL issuing authority. All data elements have an identifier. The value of a data element can be any valid CBOR or JSON data item, including a map or array.

However, the data model in this standard is set up in such a way that other mobile credentials besides mDL can be created by simply defining a different namespace and defining new data elements within that namespace while complying with all other provisions in the standard.[11] All mDL data elements are defined within a namespace with value "org.iso.18013.5.1." To avoid name collisions, the standard suggests using the reverse domain extension approach for namespace values, as shown in the mDL namespace value above. Once a separate namespace and data elements have been defined, these data elements can be requested and communicated using the interoperability provisions specified in the standard without any adaptations.

Apart from namespaces, ISO/IEC 18013-5 also uses the concept of document types, which use a similar naming convention. The value of the document type for mDLs is "org.iso.18013.5.1.mDL." As with namespaces, anyone can specify other document types. At the moment, different groups are already considering document types such as mobile vehicle registration cards and COVID-19 vaccination passports. The document type is indicated in every request or response message. An ISO/IEC 18013-5-based credential may contain multiple documents, each with a different document type.[12]

A document of a given type may contain data elements from several different namespaces. This allows an issuer, for example, of mobile driving licenses, to include some data elements in their mDL that are defined and used only domestically, not internationally.

This approach allows other credentials besides driving licenses, including those listed in Chapter 1, to be based directly on ISO/IEC 18013-5. The only requirement for this is that the data model of the credential must be expressed in CBOR or JSON.[13]

3.4.2 – Verifiable credentials

Verifiable credentials are not specified for a specific type of credential, such as a driving license or bank card. Therefore, the VC Data Model does not contain a list of attributes that must be supported by a VC, except a few generic ones such as issuer or credentialSubject. VC Data Model schemas (and hence credential templates) can be created by anyone, not just a permissioned authority. In the process they are cryptographically bound to their creator so it is transparent to all parties who may use such a schema. Each implementation should define its own attributes. However, all attribute identifiers used in a verifiable credential are required to be URIs. Because URIs are typically globally unique, anyone can define new attributes for a VC by defining a URI for these attributes. The attributes can be identified by their full identifier, i.e., URI, but alternatively, the issuer can include a so-called context in the VC, which is itself a URI. The context allows for the use of the attributes' more user-friendly identifiers.

The VC Data Model does not mandate any concrete encoding of verifiable credentials. It contains examples using JSON and JavaScript Object Notation for Linked Data (JSON-LD), but other data representation syntaxes may also be used, including Extensible Markup Language (XML), YAML Ain't Markup Language (YAML) or CBOR. Different implementations may therefore use different representations of the same attributes. It is reasonable to expect that this will be an impediment to interoperability across varying implementations, without complying as well to an additional, use case-specific, specification.

3.5 – Communication protocols

3.5.1 – ISO/IEC 18013-5

As previously mentioned, the ISO/IEC 18013-5 standard fully specifies the interfaces between an mDL and an mDL reader (interface 2, Figure 2) and between an mDL reader and an mDL issuing authority infrastructure (interface 3). Section 2.1.2 introduced the concepts of device retrieval and server retrieval. Using device retrieval, an mDL reader requests and receives data from the mDL using interface 2. Using server retrieval, the reader uses interface 3 to obtain the data from the mDL issuing authority.

Regardless of whether device retrieval or server retrieval is used, all transactions start with a device engagement phase between the mDL reader and the mDL. According to the standard, the technologies that can be used for device engagement are quick response (QR) codes or near field communication (NFC). Both are short-range and most likely require cooperation[14] from the mDL holder to be successful. This arrangement therefore reduces the risk of the verifier obtaining mDL data without the holder's knowledge and consent.

During device engagement, the mDL communicates to the mDL reader a limited amount of data necessary for setting up the communication interface for the subsequent data retrieval phase. The mDL indicates which transmission technologies it supports for device retrieval. One or more of Wi-Fi Aware, Bluetooth® Low Energy (BLE) or NFC can be used. This is an increase from the technologies which can be used in the device engagement phase, recognizing both the security layer provided by that phase as well as the increased data payload required of the retrieval phase.

An mDL must support at least BLE and NFC, and a reader must support both transmission technologies. Furthermore, the mDL indicates if its issuer supports server retrieval. If so, the mDL includes a URL and a server retrieval token in the device engagement structure. The URL identifies either a server-side Web API endpoint or an OpenID Connect (OIDC) end point.[15] The server retrieval token is specific to an issuing authority and is not standardized in ISO/IEC 18013-5. However, the standard specifies that the token identifies the mDL and recommends the use of short-lived, one-time-use tokens.

For both device retrieval and server retrieval, the ISO/IEC 18013-5 standard specifies the structure of the requests and responses exchanged between all components in the ecosystem. In a single request, an mDL reader can request multiple documents, each with different document types. For each document, it can request data elements from multiple namespaces. It should be noted that the mDL reader must explicitly include the identifier of each data

element it wants to receive in the request. The mDL and/or its holder can decide for each of the requested data elements whether or not to release it. This is described in more detail in Section 3.7.1.

3.5.2 – Verifiable credentials

The VC Data Model does not specify anything regarding communication protocols needed for the exchange of verifiable credentials. This may be related to a business requirement stated in the specification, namely that holders must be able to store verifiable credentials in any location. If nothing is assumed regarding the storage location, it is difficult to specify anything regarding these aspects.

3.6 – Security aspects

3.6.1. ISO/IEC 18013-5

3.6.1.1. Security measures

For server retrieval, ISO/IEC 18013-5 specifies that Transport Layer Security (TLS) and JSON Web Signatures (JWS) must be used to protect the confidentiality and authenticity of the data.

For device retrieval, ISO/IEC 18013-5 specifies the following three mandatory security mechanisms:

- Session encryption ensures that all requests and responses between an mDL and an mDL reader are encrypted and authenticated. This is done using two ephemeral Advanced Encryption Standard (AES) keys that are agreed upon using a Diffie–Hellman key agreement algorithm. Both the reader and the mDL use an ephemeral key pair for key agreement. The mDL sends its public key to the reader during device engagement (see Section 3.5.1). Together with its own private key, the mDL reader uses the public key to derive the session keys and uses these keys to protect the first — and perhaps only — data request message. The reader then sends its public key to the mDL during the device retrieval phase, together with the first request message. After receiving this message, the mDL uses the reader public key with its own private key to derive the same session keys. The mDL continues by decrypting the request message, creating a suitable response, protecting it using the session keys and sending it to the mDL reader.
- Issuer data authentication allows the verifier to validate that the mDL data elements — or other attributes if the credential is not an mDL — actually originate from the relevant issuing authority. To achieve this, the issuer generates a digital signature over the so-called mobile security object (MSO). The MSO is a data structure that contains a hash value for each data element in the document, regardless of whether that data element is actually included in the response from the mDL to the mDL reader.
- To perform issuer data authentication, the verifier essentially performs two steps.
  1. Verify that for each data element returned, there is a corresponding hash included in the MSO and the hash value matches.
  2. Verify that the signature over the MSO is correct. To do this, the verifier needs a Document Signer (DS) certificate included in the metadata of the MSO. The authenticity of the DS certificate can be verified using an IACA root certificate, which the verifier can obtain from the issuing authority, either directly or via a VICAL provider, as discussed in Section 3.6.1.2 below.
- mdoc authentication prevents cloning attacks. Cloning means that an adversary reads the mDL data, including the MSO, from a genuine mDL and then tries to reuse that data using another device or system. To implement mdoc authentication, the mDL uses a static key pair. The private key of this pair is stored on the mobile device on which the mDL resides and cannot easily be retrieved or cloned.[16] The public key belonging to this private key is included in the MSO and is therefore signed by the issuing authority. To perform mdoc authentication, the mDL uses its static private key in combination with the ephemeral reader public key in a key agreement protocol to derive an AES key. Then, the mDL uses the resulting key to create a message authentication code (MAC) over an authentication data structure. The reader uses the public key in the MSO, which is authenticated by the issuing authority — in combination with its own ephemeral private key — to arrive at the same AES key and verify the MAC.[17]

3.6.1.2 – Trust model

The trust model in ISO/IEC 18013-5 uses a PKI with multiple independent roots. Every issuing authority has their own root key pairs and corresponding root certificates, called Issuing Authority Certificate Authority (IACA) certificates. It uses these root key pairs to sign DS certificates, Transport Layer Security (TLS) server certificates and JSON Web Signature (JWS) signer certificates. To verify signatures created using these certificates, verifiers must possess and trust the corresponding IACA root certificate.

There is no single root certificate authority that signs all the IACA root certificates. Instead, the informative Annex C in ISO/IEC 18013-5 suggests that IACA root certificates will be communicated by the issuing authorities to the verifiers using one or more so-called Verified Issuer Certificate Authority Lists (VICALs), each managed by a VICAL provider. A VICAL is simply a list of certificates signed by the VICAL provider. The key difference between the VICAL provider and a central root certificate authority is that the VICAL provider is not authorized to revoke IACA certificates. Moreover, a breach of security of the VICAL

provider systems would not necessitate the revocation of any certificate on the VICAL.

The standard suggests, but does not mandate, that a VICAL provider only accept the IACA root certificates from issuing authorities that comply with the VICAL provider requirements, e.g., regarding the way the issuing authority ensures the security of the corresponding private keys. The standard contains an informative policy that can be used as the basis for a VICAL provider's security policy.

3.6.2 – Verifiable credentials

3.6.2.1 – Security measures

As noted previously in this white paper, the VC Data Model requires each verifiable credential to contain proof that is cryptographically verifiable. This proof is used to ensure the VC's authenticity. The VC Data Model does not, however, mandate any particular format or type of digital proof or signature. The proof mechanism in a given implementation of the VC Data Model may range from digital signatures in a PKI to zero-knowledge proofs (ZKPs) committed to a distributed ledger. The VC extension registry[18] contains a list of proof mechanisms currently in development. At the time of this writing, the list includes two possibilities — an RSA-based signature or an Ed25519-based signature.

Since the specification does not go into detail regarding proof mechanisms, protection against other security threats is generally not guaranteed, unless an implementation complies as well with an additional, use case-specific specification. There is a list of security considerations, potential issues and countermeasures, but these are non-normative.

3.6.2.2 – Trust model

The trust model detailed in the VC Data Model does not imply a PKI. The specification instead states that a verifier either directly trusts or does not trust an issuer. It actually contains a generic warning about potential security weaknesses introduced by the use of a PKI system.

Another requirement of the trust model is that all entities must trust the verifiable data registry to be tamper-evident and to be a correct record of what data is controlled by which entities. Similar to ISO/IEC 18013-5, regarding VICAL providers, the VC Data Model does not discuss the conditions under which trust in a verifiable data registry is warranted.

3.7 – Privacy aspects

3.7.1 – ISO/IEC 18013-5

An mDL complying with ISO/IEC 18013-5 protects the holder's privacy in a number of ways.

- The holder is able to manage and verify to which verifier any data elements are to be released.
- The mDL is able to selectively release individual data elements that are contained in the same document. This means that it can disclose certain data elements but not others. As explained in Section 3.6.1.1, this is based on the presence of a hash over each data element that exists on the mDL in the mobile security object.[19]
- The user can also give or withhold consent for the release of each individual data element. The mechanism for obtaining user consent is not specified in ISO/IEC 18013-5. However, to promote informed consent, the standard requires that, for every requested data element, the mDL verifier must indicate whether or not they intend to retain that data for longer than strictly necessary for transaction processing.
- The mDL data model contains a few data elements explicitly designed for data minimization. The best example is the age_over_NN data element, which only reveals whether or not the holder is above a certain age. If an issuer includes multiple of these data elements in an mDL, it allows a verifier to determine whether or not the age of the mDL holder matches their business criteria, e.g. over 18 and under 65 years old, without the need to request the holder's actual birth date.[20]
- The mDL can be used fully offline without the need for involvement by the issuing authority and even without their knowledge.[21]
- The standard avoids — or contains recommendations to avoid — the use of static identifiers on all levels of the communication stack to prevent the ability of transactions to be linked. Likewise, to prevent tracking of the mDL holder, the standard implements — or recommends implementing — ephemeral session keys, OpenID Connect pairwise identifiers and key rotation. To mitigate the chance that the signature over the MSO or the public mdoc authentication key becomes a static identifier, a single document on the mDL may be provisioned with multiple MSOs, each containing a different mdoc authentication public key and using different salts for a given mDL data element. At the time of transaction, the mDL can randomly pick one of these MSOs to be returned to the mDL reader.

3.7.2 – Verifiable credentials

When comparing the mDL's privacy characteristics in the previous section to those of a verifiable credential, we see the following:

- As with the mDL, the holder is in control of the VC and determines to which verifier a credential may be released.
- For selective release of data elements, the situation is more complicated. A VC may be able to selectively release individual attributes contained in the VC. This is possible if the proof mechanism of the VC is a ZKP. The VC Data Model mentions Camenisch-Lysyanskaya signatures as an example. The theory of ZKPs is well understood. However, they are standardized to a much lesser degree than standard digital signatures. Support for ZKPs in cryptographic libraries is still scattered. In fact, as mentioned, the only proof mechanisms being standardized in the context of verifiable credentials are based on RSA and EdDSA, both of which are not ZKPs.
- Like ISO/IEC 18013-5, the VC Data Model assumes that a mechanism for user consent is in place, but how this should be implemented is not specified.
- Data minimization is an important topic in the VC Data Model, just as it is for ISO/IEC 18013-5. The possibility of issuing specific data-minimized credentials such as ageOverNN is mentioned several times.[22]
- A verifiable credential can be used offline, provided the verifier is in possession of a copy of the VDR or a subset of it. Since that registry is, in many cases, a distributed ledger and the verifier does not need to add anything to it when verifying a VC, this may be technically possible.
- Finally, the VC Data Model also warns against the use of static identifiers.

4 – Combining ISO/IEC 18013-5 and the VC Data Model

4.1 – Introduction

Chapter 3 of this white paper focused on the similarities and differences between credentials based on the VC Data Model and those based on ISO/IEC 18013-5. From this discussion, it is clear the VC Data Model does not specify all aspects necessary to ensure that two different verifiable credential implementations are interoperable. In particular, no common communication protocols, data encodings or security mechanisms are specified. ISO/IEC 18013-5, on the other hand, does specify all of these aspects.

The question is, therefore, whether it is possible to combine a verifiable credential with a credential based on ISO/IEC 18013-5, such that the essential properties of the VC are retained but interoperability is also ensured. In fact, this would mean that ISO/IEC 18013-5 can be a important road to a standards-based implementation of VCs. This is a frequently asked question that will be addressed in this chapter.

Currently, we see at least four ways in which ISO/IEC 18013-5 and the VC Data Model may be combined.

- First, an ISO/IEC 18013-5 implementation may also be seen as an implementation of the VC Data Model. That is, it is possible to design a credential that complies with both ISO/IEC 18013-5 and the VC Data Model.
- Second, a mobile device that contains an ISO/IEC 18013-5 based credential may simultaneously be used to store an existing verifiable credential. The two types of credential live side by side in the same wallet, but do not (have to) share data retrieval mechanisms or security mechanisms.
- Third, an existing verifiable credential may be implemented as a data element in an ISO/IEC 18013-5 based document. In this case, the VC uses the data retrieval mechanisms specified in ISO/IEC 18013-5. It also uses the security mechanisms of that standard, possibly in addition to its own security proof.
- Finally, an existing verifiable credential may also be implemented as a separate ISO/IEC 18013-5-based document. This would mean that only the data element definitions of the VC are kept and the proof mechanism is replaced by the security mechanisms of ISO/IEC 18013-5.

Each of these options is discussed in further detail in the sections below.

4.2 – ISO/IEC 18013-5 as an Implementation of the VC data model

If a new digital credential is created, it can be specified in such a way that it complies with both ISO/IEC 18013-5 and the VC Data Model. This is possible because the VC Data Model is open enough to accommodate ISO/IEC 18013-5 based credentials. However, the following must be considered:

- As defined in ISO/IEC 18013-5, a new namespace will probably have to be created for the attributes of the new credential, as discussed in Section 3.4.1.
- The cryptographic proof that will be used in this solution is the Mobile Security Object (MSO) — see Section 3.6.1. Although such a solution is not explicitly recognized as a possibility in the VC Data Model, it is not ruled out either.[23] In fact, the VC Data Model states that new proof mechanisms are expected to be standardized over time.

- The above means that there will not be a proof property in the VC. This is similar to the situation described in paragraph 6.3.1 of the VC Data Model in which the proof takes the form of a JSON Web Token with a JSON Web Signature. Section 4.7 of the VC Data Model describes this as an external proof.
- As described in Section 3.3, the Verifiable Data Registry (VDR) mentioned in the VC Data Model would probably take the form of a Verified Issuer Certificate Authority List (VICAL), as specified in ISO/IEC 18013-5. However, such a VICAL would fit in the VC Data Model.
- The new credential will be encoded in CBOR or JSON, depending on whether device retrieval or server retrieval is used. The VC Data Model does not mention CBOR as an example of encoding for verifiable credentials. Again, however, there is nothing in the Data Model that precludes this.
- The attributes of the new credential must comply with the relevant VC Data Model requirements. For example, an "issuer" property that is a URI must be present. The "credentialSubject" property must be present and may have to contain (an array of) URIs as well, depending on the way the VC will be used.
- Finally, in this setup, the new credential will always be located either in the mobile device the issuer has issued it to or on an issuing authority server. This is because mdoc authentication — which is mandatory according to ISO/IEC 18013-5 — prevents cloning of the credential.

4.3 – Storing ISO/IEC 18013-5 based credentials and VCs side by side

To combine an existing ISO/IEC 18013-5 based credential with a verifiable credential, it may be possible to extend the functionality of an existing mDL application in such a way that it can store VCs and present them to a verifier as a QR code or via NFC.

In this way, the mDL application functions as a repository for the VC. Some functions of the mDL application would then be reused for the VC, in particular the QR and/or NFC functionality it already uses for device engagement — see Section 3.5.1 — and possibly also its secure data storage. However, there would be no further integration between the mDL functionality and the VC functionality. In particular, the VC can still use a proof mechanism of its own and does not need to use the security mechanisms of ISO/IEC 18013-5. After reading the VC from the mobile device, the verifier would process the VC as specified for the particular VC implementation. For that reason, this option seems particularly suited for combining an already existing verifiable credential with an mDL or other ISO/IEC 18013-5 based credential.

4.4 – Implementing a VC as an ISO/IEC 18013-5 data element

A way to integrate an existing verifiable credential more deeply with an existing ISO/IEC 18013-5 based document is to store the VC as an additional data element in the document. The VC itself would not be changed in any way. The new data element would have to be specified in a namespace, either as an addition to an existing namespace or in a dedicated one.
Storing a verifiable credential in a document ensures that the VC can profit from the communication protocols and security mechanisms specified in ISO/IEC 18013-5. If the verifiable credential already exists, it will have its own proof mechanism. Since ensuring authenticity is also one of the goals of issuer data authentication, there will be some redundancy between the mechanisms. However, this does not need to be considered a disadvantage, as redundant security mechanisms are not uncommon and may, in fact, contribute to in-depth defense measures.

4.5 – Implementing a VC as an ISO/IEC 18013-5 document

Finally, a VC can also be stored as a separate ISO/IEC 18013-5 based document. In this case, it is necessary to specify a dedicated document type value for the VC. Within that document, the VC will not be stored as-is. Instead, the individual attributes in the VC are stored as data elements. As before, a dedicated namespace must be specified for these data elements.

This approach looks a lot like the one described in Section 4.2. In particular, if the VC already exists, it will probably contain a proof property.[24] This property must, however, not be stored as a data element in the new VC document, as its function will be performed by that document's MSO.

4.6 – Conclusion and future work

The previous section discussed how verifiable credential and ISO/IEC 18013-5 based credential may be combined. There are different methods by which this may be achieved, and each of these ways has distinct advantages and drawbacks. Still, at the time of writing, neither ISO/IEC 18013-5 nor the VC Data Model explicitly discuss how this may be achieved.

Discussions on this topic are currently ongoing within ISO/IEC JTC1/SC17, the same committee responsible for the creation of ISO/IEC 18013-5. It is expected that the outcome of these discussions will be standardized in the forthcoming ISO/IEC 23220 standard series.

It would be beneficial if the W3C would similarly develop views on or mechanisms for combining a verifiable credential with ISO/IEC 18013-5. One avenue to do so would be to formally specify a mobile security object according to ISO/IEC 18013-5 as a proof mechanism for verifiable credentials.

References

Reference and title	Author	Version	Date
1. ISO/IEC 18013-5: Personal identification – ISO-compliant driving license – Part 5: Mobile driving license (mDL) application	ISO/IEC	First edition	September 2021
2. W3C Recommendation: Verifiable Credentials Data Model – Expressing verifiable information on the Web	W3C	1.0	19 November 2019
3. W3C Working Group Note: Verifiable Credentials Use Cases	W3C	-	24 September 2019
4. W3C Working Group Note: Implementation guidance for Verifiable Credentials	W3C	-	24 September 2019
5. W3C Working Draft: Decentralized Identifiers (DIDs) - Core architecture, data model, and representations	W3C	1.0 (Draft)	02 March 2021
6. RFC 8949 Concise Binary Object Representation (CBOR)	IETF	-	December 2020
7. RFC 8259 The JavaScript Object Notation (JSON) Data Interchange Format	IETF	-	December 2017

Endnotes

1. UL wrote a number of blog posts to introduce the mobile driving license (mDL) as well as the ISO/IEC 18013-5 standard. These blog posts also discuss several other aspects of the standard to considered when implementing it, such as interoperability and security issues. See https://www.ul.com/insights/dangerous-conditions-ahead-navigating-security-issues-mobile-identity, for more details.

2. Precisely speaking, the subject of a credential is the person or entity that has the attributes asserted in the credential. The holder of the credential is the person or entity that legitimately manages the credential and presents it to a verifier. The holder and the subject of a credential are often, but not always, the same. A simple counterexample is a parent holding and presenting an identification document for their child when boarding a plane.

3. In the case of a passport, the surname and given names are viewed as attributes, since the subject can use their passport to prove their name. In other credentials, a name is typically present to bind the subject of the credential to the holder (i.e., the person presenting the credential). For example, a pre-paid train ticket might only be valid if the holder can show an identity document bearing the same name as the name on the ticket. In such credentials, the subject's name is not an attribute that the issuer is asserting.

4. See, for example, the discussions in Annexes C and E of the standard.

5. If such a mechanism also exists for verifiable credentials, it is, in any case, out of the VC Data Model's scope.

6. Strictly speaking, this depends on the way the issuing authority specifies and uses the token that is needed for server retrieval, see Section 3.5.1. The standard does not mandate anything on these aspects, but does give some guidelines to prevent misuse.

7. Note that anyone, including the mDL holder, can read the credentials from an mDL and store them alongside the Mobile Security Object (MSO, see Section 3.6.1) in any location they want to. The MSO is the cryptographic proof that the credentials are authentic. However, it will not be possible to present these stored credentials to an ISO/IEC 18013-5 conformant mDL reader, because mdoc authentication will fail, as explained in Section 3.6.1.

8. If there is no VICAL, IACA root certificates will need to be communicated from an issuer to a verifier on a peer-to-peer basis.

9. Even if the VICAL serves a large number of mDL issuing authorities, the verifier only needs to do this check infrequently because an IACA root certificate will be valid for at least a few years. Doing so once per day will be more than enough.

10. CBOR is specified in RFC 8949, [6]. JSON is specified in RFC 8259, [7].

11. The standard uses different terminology to distinguish between provisions that apply to any mobile credential, referred to as "mdoc", and provisions that apply only to mobile driving licenses proper, or mDL. To avoid confusion, this white paper will continue to use mDL.

12. Note that ISO/IEC 18013-5 is careful not to define the internal structure of an mDL. The mDL is the entirety of the mobile device hardware (including possibly secure data storage), the OS, possibly a dedicated application and personalization data. The latter may include multiple documents, each containing multiple data elements.

13. Note that in case of legacy encoding of data elements, it is always possible to encapsulate the complete encoding in a CBOR or JSON (byte) string.

14. Such as presenting the display of the mobile device to the verifier or bringing the device within 10 cm of the mDL reader to interact with an NFC field.

15. Technically, it is possible to indicate two URLs and tokens, one for Web API and one for OIDC.

16. How difficult it is in practice to retrieve a private key from a mobile device depends on the strength of the security measures implemented on that device. This white paper does not attempt a discussion of this aspect.

17. The standard actually also specifies another mechanism for mdoc authentication in which the mDL uses the private key to create a signature over the authentication data structure. The mDL reader then verifies the signature using the public key in the MSO. An issuing authority is free to choose either mechanism. The standard indicates that the MAC-based method is preferred.

18. https://w3c-ccg.github.io/vc-extension-registry/

19. It should be noted that in fact this mechanism also protects mDL verifiers, by allowing them to request only those data elements that they need for their business purposes. This means that they will never end up with unnecessary information (which may be PII) on the mDL holder, even in case the mDL holder is not paying attention to the data that is being released.

20. ISO/IEC 18013-5 actually forbids a reader from requesting more than two age_over_NN elements in a single transaction because there is never a business need for doing so. This prevents unnecessary precise determination of the holder's age by the mDL verifier.

21. The only exception to this may be revocation checking of Document Signer and/or IACA root certificates if this is done online. However, this can be mitigated by using a local Certificate Revocation List (CRL) that is regularly updated.

22. Additionally, the VC Implementation Guidelines [4] observe that some ZKP-based proof mechanisms would allow a holder to derive an ageOverNN credential at transaction time from a date-of-birth credential, without the issuer's involvement and without the need to release the date of birth. However, the specification does not explain which ZKP-based mechanisms would allow this or how this could be done in practice.

23. The VC Implementation Guidelines [4] mention the use of hashed values as a solution for selective disclosure, but states that "no standard way [to model these] is currently defined." This is untrue. Apart from being standardized in ISO/IEC 18013-5, essentially the same mechanism has long been specified in ICAO Doc 9303 - Machine Readable Travel Documents, which covers the electronic passport. Moreover, many other signature formats use indirect signatures with hashes as well, often allowing partial validation explicitly. Examples include the XML signature and the JAR signing format.

24. If the proof is external, e.g. JWT style, it does not have such a proof property.

UL.com

0721