VitalChek®
A LexisNexis® Risk Solutions Company

LexisNexis®
RISK SOLUTIONS

STANDARDS WHITE PAPER

Digital Credentials and the Vital Record Ecosystem

Verifiable Credential Data Model specification published by the World Wide Web Consortium (W3C), and the ISO/IEC 18013-5 standard for mobile driving licenses

Table of Contents

INTRODUCTION

As the world becomes increasingly digitized, the need for secure and reliable digital identity document solutions has become paramount for solving trust issues. Verifiable credentials offer a promising framework to establish trust in digital interactions, enabling individuals to share and prove their credentials while maintaining privacy and security. Vital records security trust framework heavily relies on physical document attributes. The birth certificate, for example, is the first identity document with claims or assertions made about a subject such as name, date of birth, place of birth, etc. When an entitled holder of that document provides it to a verifying entity, that entity can verify its authenticity via raised seals, watermarks, signatures related to the issuing authority, and the fact that the certified document is printed on properly stored uniquely identifiable security paper. The verifier therefore does not have to directly communicate with the issuing authority because the certificate can be proofed because of the artifacts of the actual certificate. But there are security vulnerabilities in this trust framework. Paper certificates can be stolen, counterfeit, or altered. Security features may vary between issuing authorities, and there may be limited training for fraud detection. In some cases, the document is authentic, but it is the holder that is an impostor. Verifiable credential standards are important in ensuring interoperability, privacy, and security.

This white paper discusses two predominant standards that attempt to address the needs of the vital records ecosystem; the Verifiable Credential Data Model specification published by the World Wide Web Consortium (W3C), and the ISO/IEC 18013-5 standard for mobile driving licenses. The credentials described in each document seemingly 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. By understanding and adopting standards, the vital records ecosystem can unlock the potential of verifiable credentials and usher in a new era of trusted digital interactions.

Digital Credentials

Digital credentials are much more than a digital copy of a physical document; they are the virtual counterparts to physical credentials. This type of credential first emerged when traditional issuers of physical credentials started issuing electronic versions. This began over twenty years ago with the issuance of bank cards and SIM cards. In some cases, a digital credential is combined with its physical counterpart in a single document via an embedded QR code. 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 used with Apple Pay or Android Pay. These digital-first credentials provide identity assurance and allow for presentation remotely in a secure digital channel.

A credential is provided to the holder by an issuer. An entity can be an issuer by asserting claims about one or more subjects, digitally signing the credential, and transmitting the verifiable credential to a holder. The credential is then wholly controlled by the holder and held in a digital wallet controlled by private keys. A verifier — sometimes called a "relying party" — will accept that the holder does, in fact, possess the abilities or experiences asserted in the credential, if 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, but not always, 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.

When a credential is digitally signed and can cryptographically prove its authorship, it is called a verifiable credential. Verifiable credentials are tamper-proof, cryptographically secure, and can be easily shared between different parties.

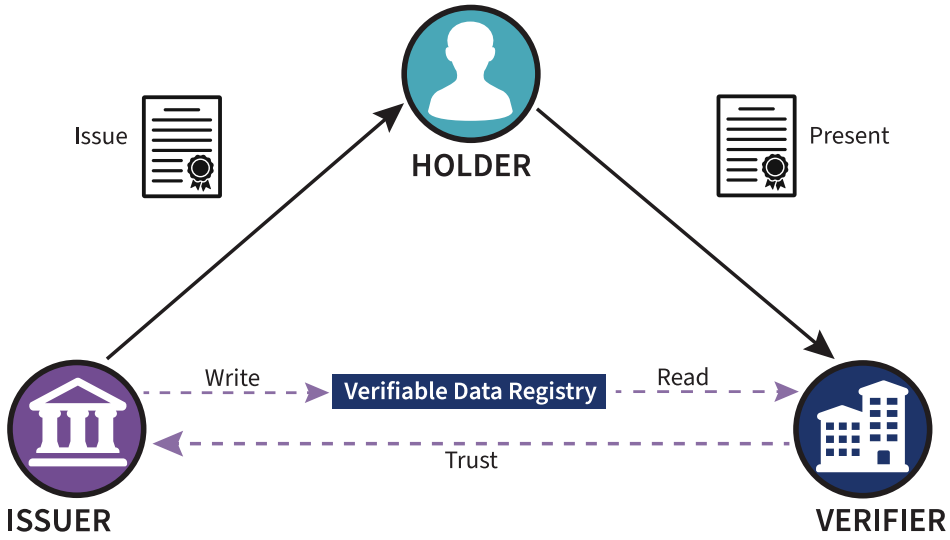
The Trust Triangle

To better understand digital credentials and the standards discussed in this white paper, it is helpful to have some understanding of the three components of a credential. The relatively new concept of digital identity has three essential pillars: the issuer, the holder, and the verifier.

An issuer is an entity that is authorized to issue a credential. Issuers are typically government organizations, healthcare centers, banks and financial institutions, schools, and universities. For example, in the ISO/IEC 18013-5 standard for mobile driving licenses, the Department of Motor Vehicles is the issuer that is authorized to issue a mobile driver's license credential that contains the license number of an individual. Within the vital records ecosystem this issuer could be the state or local health department.

The holder is an individual who receives the verifiable credentials they are entitled to and has complete control over them to present them to the verifiers. The holder may or may not be the subject, for example in vital records, a parent may hold their child's certificate.

A verifier is an entity that verifies a credential and ensures that it comes from a competent issuer, is tamper-evident, and is still relevant (not expired or revoked). A verifier takes the verifiable presentation from the holder to determine its authenticity. Verifiers are entities that require specific information about a holder for authentication, so services can be offered to the holder.



A trust system is the foundation for establishing trust between decentralized systems. These decentralized systems must trust that data sharing between themselves is authentic, it has not been altered or tampered with, and that the originator of the data follows certain trusted processes.

The trust triangle conceptually modeled by the issuer, holder, and the verifier represents the relationships between these entities and the trust that exists among them. It highlights the trust placed in the issuer by the verifier. The verifier relies on the issuer's trustworthiness by the proof within the credential to ensure the validity and accuracy of the information contained in the verifiable credential. The holder and the verifier trust the issuer to issue true credentials about the subject. The issuer may also rely on proof mechanisms for a level of assurance for the holder identity to accurately represent the attested to claims contained in the credential prior to issuance.

The use of cryptographic techniques, such as digital signatures, ensures the integrity and authenticity of the verifiable credentials. This helps establish trust among the entities involved, and enables the verifier to make informed decisions based on the information presented in the verifiable credential.

VERIFIABLE CREDENTIALS (W3C)

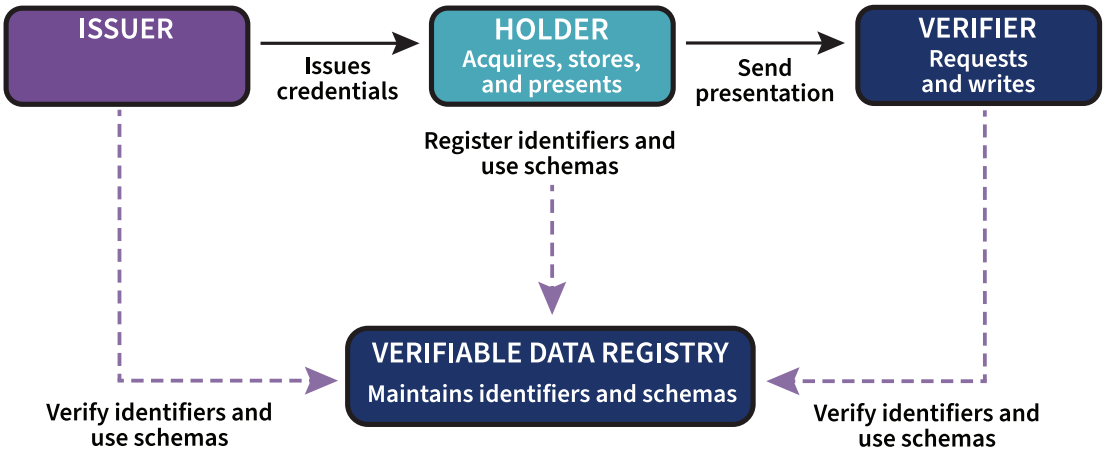
Background

The Verifiable Credential Data Model specification published by the World Wide Web Consortium (W3C) is a standard that aims to provide a secure and decentralized way to manage digital identity. The Verifiable Credential Data Model has been developed in collaboration with several industry partners, including Microsoft®, IBM®, and the Decentralized Identity Foundation. It is based on open standards and is designed to be interoperable with existing identity management systems, making it easy for organizations to adopt and integrate into their existing workflows.

Ecosystem

Apart from the roles of credential holder, credential issuer, and credential verifier, the Verifiable Credential Data Model also incorporates the Verifiable Data Registry (VDR) shown below. 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 depends on what is required to use and verify the credentials. The VDR may come in the form of a distributed ledger, blockchain, or trusted web domain.

Flow of roles and information in the VitalChek Data Model



Goals

The goals of verifiable credentials, as mentioned in the VC Data Model, 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 authenticity of the VC. The VC Data Model specification does not dictate any digital proof or signature format. The proof mechanism in each 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 is generally not covered.

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.

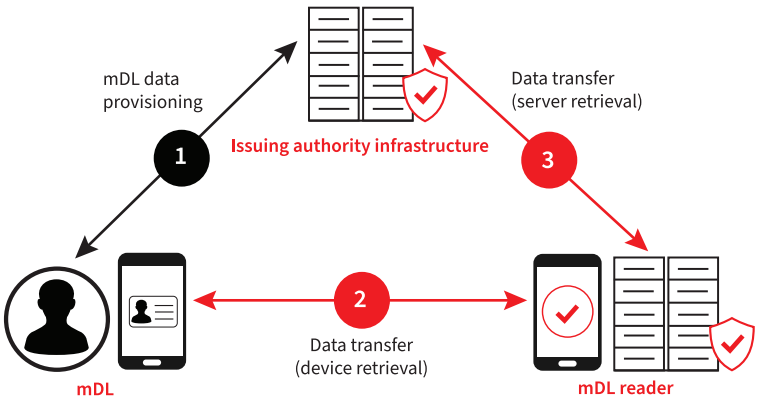
ISO/IEC 18013-5

Background

ISO/IEC 18013-5 technical standard outlines the requirements for mobile driving licenses (mDLs) and their related systems. The standard was developed by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) to provide a framework for the development and implementation of secure and interoperable mDLs.

Ecosystem

The mDL is standardized within the International Standard ISO/ IEC 18013-5. The main components and associated roles and interfaces in the mDL ecosystem, as presented in this standard are shown below.



The ISO/IEC 18013-5 standard specifies several technical requirements that must be met to ensure the secure and reliable operation of mDLs systems. Some of the key technical requirements include:

- **Cryptography:** The standard requires the use of cryptography to protect the confidentiality and integrity of the data stored in mDLs.
- **Biometric authentication:** The mDLs must be protected with biometric authentication, such as fingerprint or facial recognition, to ensure that only the authorized user can access it.
- **Secure data storage:** The standard requires that mDLs data be securely stored on the device, with appropriate measures in place to prevent unauthorized access.
- **Secure communication:** The standard requires that all communication between the mDLs and other systems be encrypted and authenticated to prevent interception or tampering.

Goals

The main goals of ISO/IEC 18013-5 are interoperability, extensibility, security, and privacy. 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. ISO/IEC 18013-5 includes provisions for the privacy of mDL holders by requiring that personal data is protected and that the mDL holder's consent is obtained before any data is shared. The standard also includes provisions for the accessibility of mDLs by requiring that they are compatible with assistive technologies and that they are available in multiple languages.

CONCLUSION AND FUTURE WORK

When comparing W3C verifiable credentials to credentials based on ISO/IEC 18013-5, there are gaps in each and existing differences between them in data model, credential format, signature scheme, issuing protocol, presentation exchange, and trust model. The first thing to note is that the VC Data Model is simply a data model specification. The VC Data Model tries to be as open as possible. As outlined in the specification, this approach is an "open-world assumption." This 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 specification and a suite of other complementary open standards like OIDF and DIF. 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. No common communication protocols, data encodings, or security mechanisms are specified. 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.

ISO/IEC 18013-5 can be used as a basis for another type of digital credential besides the mobile driving license. This can be accomplished by defining a new document

type and/or a new name space for data elements of the new credentials. Although this is the case the standard itself has an individual scope of concern around a mobile driver's license where there is one holder, and the holder is the same as the subject of the credential. Within the vital records ecosystem, we know there can be more than one subject of a credential as in the case of marriage and divorce. In addition, the holder may be different than the subject of a credential as in the case of a parent holding their child's credential. The W3C credential data model specifications address these use cases, allowing for more than one credential subject and different subject-holder relationships, making it more extensible to the different types of vital record credentials.

To develop a standard that meets the needs of the vital records ecosystem today, we support efforts for the next generation of the two standards to align for the best implementation. The W3C VCs Working Group and the ISO/IEC JTC 1/SC 17 Working Groups (WG 4 &10) have a critical role in working towards this alignment. Community projects are already in place to ensure that W3C verifiable credentials are a viable alternative for implementers of the ISO 18013-5 standard, and are compatible with the outputs of the ISO working groups. ISO/IEC JTC 1/SC 17 Cards and security devices for personal identification standard has enabled working towards aligning ISO-compliant mobile driving licenses with the work of the Verifiable Credentials Working group. Alignment of the two standards will give the VC and mDL wallet vendors a level set, while urging wallet vendors to support both standards. Alignment does not mean convergence to one set of standards, as there will not be a "one size fits all" standard to digital credentialing within the market, and we already see that when defining use cases for the vital records ecosystem. Instead, what is being suggested is for the two standards to interact/inter-operate with each other while each is providing unique market value. This should now be a necessary effort given the market initiative toward digital vital records. In an open letter to the two standards communities from the Identity Woman in Business, a threat to not working together is highlighted as, "the market is being captured by implementers creating their proprietary solutions that cannot evolve to align with standards and will fail to achieve anything long-term. The lack of settled standards and the lack of clarity of how different standards align increase the risk that proprietary solutions are adopted as they are seen to be an easier decision: worsening everyone's future prospects except the proprietary providers'."

This threat can be averted sooner with continued efforts to work together alongside continuous development efforts. Widespread standard adoption will provide verifiable credentials that have the potential to revolutionize vital records and empower individuals to take control of their digital identities.

REFERENCES

Reference	Author	Date
1. W3C Recommendation: Verifiable Credentials Data Model – Expressing verifiable information on the Web	W3C	November 2019
2. ISO/IEC 18013-5: Personal identification – ISO-compliant driving license – Part 5: Mobile driving license (mDL) application	ISO/IEC	September 2021
3. W3C Working Group Note: Verifiable Credentials Use Cases	W3C	September 2019
4. W3C Working Group Note: Implementation guidance for Verifiable Credentials	W3C	September 2019
5. W3C Working Draft: Decentralized Identifiers (DIDs) - Core architecture, data model, and representations	W3C	March 2021
6. Where can the W3C VCs meet the ISO 18013-5 mdl	Identity Woman in Business	December 4, 2022