NIST SPECIAL PUBLICATION 1800-42

Digital Identities — Mobile Driver's License (mDL)

Enabling Secure and Interoperable Online Use

Yee-Yin Choong
William Fisher
Ryan Galluzzo
National Institute of Standards and Technology

Jason Ajmo
Christopher Brown
Sudhi Umarji*
The MITRE Corporation

Ellen Nadeau
Coralline

Heather Flanagan
Spherical Cow Consulting

November 2026

SECOND PUBLIC DRAFT

This publication is available free of charge from
https://www.nccoe.nist.gov/projects/digital-identities-mdl

*Former employee: all work for this publication was done while at employer.



DISCLAIMER

Certain commercial entities, equipment, products, or materials may be identified by name or company logo or other insignia in order to acknowledge their participation in this collaboration or to describe an experimental procedure or concept adequately. Such identification is not intended to imply special status or relationship with NIST or recommendation or endorsement by NIST or NCCoE; neither is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

HOW TO CITE THIS NIST TECHNICAL SERIES PUBLICATION

Chong Y, Fisher W, Galluzzo R, Ajmo J, Brown C, Umarji S, Nadeau E, Flanigan H (2026) Digital Identities — Mobile Driver's License (mDL): Enabling Secure and Interoperable Online Use. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Series SP 1800-42.

NIST TECHNICAL SERIES POLICIES

Copyright, Use, and Licensing Statements
NIST Technical Series Publication Identifier Syntax

AUTHOR ORCID IDS

Yee-Yin Choong: 0000-0002-3889-6047
William Fisher: 0009-0004-7569-5668
Ryan Galluzzo: 0000-0003-0304-4239
Sudhi Umarji: 0000-0001-6842-8167
Ellen Nadeau: 0009-0000-1748-7749
Christopher Brown: 0009-0000-7829-1918
Heather Flanagan: 0000-0002-2647-2220
Jason Ajmo: 0009-0007-4046-6146

FEEDBACK

Comments on this publication may be submitted to: mdl-nccoe@nist.gov.

Comments can also be submitted on the deliverables published on our resource hub.

Public comment period: November 17th 2026, through December 20th 2026

All comments are subject to release under the Freedom of Information Act.

National Cybersecurity Center of Excellence
National Institute of Standards and Technology
100 Bureau Drive
Mailstop 2002
Gaithersburg, MD 20899

Email: nccoe@nist.gov

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity issues. This public-private partnership enables the creation of practical cybersecurity solutions for specific industries, as well as for broad, cross-sector technology challenges. Through consortia under Cooperative Research and Development Agreements (CRADAs), including technology partners—from Fortune 50 market leaders to smaller companies specializing in information technology security—the NCCoE applies standards and best practices to develop modular, adaptable example cybersecurity solutions using commercially available technology. The NCCoE documents these example solutions in the NIST Special Publication 1800 series, which maps capabilities to the NIST Cybersecurity Framework and details the steps needed for another entity to re-create the example solution. The NCCoE was established in 2012 by NIST in partnership with the State of Maryland and Montgomery County, Maryland.

To learn more about the NCCoE, visit https://www.nccoe.nist.gov/. To learn more about NIST, visit https://www.nist.gov.

NIST CYBERSECURITY PRACTICE GUIDES

NIST Cybersecurity Practice Guides (Special Publication 1800 series) target specific cybersecurity challenges in the public and private sectors. They are practical, user-friendly guides that facilitate the adoption of standards-based approaches to cybersecurity. They show members of the information security community how to implement example solutions that help them align with relevant standards and best practices, and provide users with the materials lists, configuration files, and other information they need to implement a similar approach.

The documents in this series describe example implementations of cybersecurity practices that businesses and other organizations may voluntarily adopt. These documents do not describe regulations or mandatory practices, nor do they carry statutory authority.

ABSTRACT

Mobile Driver's Licenses, and Verifiable Digital Credentials more broadly, represent an emerging technology with the capability to enhance the methods used to prove identity both in-person and online. Many sectors stand to benefit from this emerging technology seeking to enhance the security, privacy, usability, and reliability of online identity services. This practice guide provides foundational information and considerations for any organizations adopting Verifiable Digital Credentials. It serves as the base document for the NIST SP 1800-42 series, which captures insights generated through engagement with a robust cohort of industry collaborators and the lessons learned by developing functional online mDL demonstrations for various use cases.

KEYWORDS

authentication; credentials; identity; mobile driver's license (mDL); verifiable digital credentials.

ACKNOWLEDGMENTS

The project team is grateful to all the collaborators who donated their time and expertise to make this project a reality. See our project resource hub for a complete list of collaborators who participated in this project.

DOCUMENT CONVENTIONS

The terms “shall” and “shall not” indicate requirements to be followed strictly to conform to the publication and from which no deviation is permitted. The terms “should” and “should not” indicate that among several possibilities, one is recommended as particularly suitable without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required, or that (in the negative form) a certain possibility or course of action is discouraged but not prohibited. The terms “may” and “need not” indicate a course of action permissible within the limits of the publication. The terms “can” and “cannot” indicate a possibility and capability, whether material, physical, or causal.

CALL FOR PATENT CLAIMS

This public review includes a call for information on essential patent claims (claims whose use would be required for compliance with the guidance or requirements in this Information Technology Laboratory (ITL) draft publication). Such guidance and/or requirements may be directly stated in this ITL Publication or by reference to another publication. This call also includes disclosure, where known, of the existence of pending U.S. or foreign patent applications relating to this ITL draft publication and of any relevant unexpired U.S. or foreign patents.

ITL may require from the patent holder, or a party authorized to make assurances on its behalf, in written or electronic form, either:

a) assurance in the form of a general disclaimer to the effect that such party does not hold and does not currently intend holding any essential patent claim(s); or

b) assurance that a license to such essential patent claim(s) will be made available to applicants desiring to utilize the license for the purpose of complying with the guidance or requirements in this ITL draft publication either:

1. under reasonable terms and conditions that are demonstrably free of any unfair discrimination; or
2. without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination.

Such assurance shall indicate that the patent holder (or third party authorized to make assurances on its behalf) will include in any documents transferring ownership of patents subject to the assurance, provisions sufficient to ensure that the commitments in the assurance are binding on the transferee, and that the transferee will similarly include appropriate provisions in the event of future transfers with the goal of binding each successor-in-interest.

The assurance shall also indicate that it is intended to be binding on successors-in-interest regardless of whether such provisions are included in the relevant transfer documents.
Such statements should be addressed to: mdl-nccoe@nist.gov.

Contents

1 Introduction to the Guide 7
1.1 Scope 7
1.2 Audience 7
1.3 How to Use This Guide 8
2 Project Overview 9
2.1 Project Motivation 9
2.2 Current Challenges with Online Identity Proofing 9
2.3 Benefits of mDLs 10
3 A Brief Introduction to VDCs and MDLs 11
3.1 An Overview of VDCs 11
3.1.1 The VDC Trust Model 12
3.2 An Overview of mDLs 12
3.3 Other Components in the VDC Ecosystem 13
3.4 Standards in the VDC Ecosystem 14
3.4.1 Standards Maturity 14
4 NCCoE mDL Use Cases 15
5 Threat Model 16
5.1 mDL Security Capabilities 16
5.2 mDL Threats and Mitigations 17
5.2.1 Quantum Computing 26
5.2.2 Credential Revocation, Validity and Freshness 26
6 Privacy Considerations 28
6.1 Privacy Overview 29
6.2 Privacy in the mDL Architecture 30
7 Usability Considerations & Evaluation Summary 33
7.1 User Experience and Usability 33
7.2 Usability Best Practices 34
7.2.1 Preserve the positive characteristics of mDL-based verification 35
7.2.2 Improve QRC scanning reliability and predictability 35
7.2.3 Standardize terminology across presentment flows and attribute displays 35

159 7.2.4 Ensure consistent and predictable user-interface behaviors 35
160 7.2.5 Provide explanatory text and visual cues to support user understanding 35
161 7.2.6 Consider factors and potential barriers to adoption 36
162 7.2.7 Evaluate and plan for additional, user-driven use cases 36
163 **Appendix A References 37**
164 **Appendix B List of Available Online Resources 39**
165 **Appendix C List of Symbols, Abbreviations, and Acronyms 40**

166 # List of Figures

167 Figure 1. Callout box 8
168 Figure 2. Verifiable digital credentials 11
169 Figure 3. Presenting verifiable digital credentials through a mobile application or a browser 13
170 Figure 4. Standards landscape (October 2026) 14
171 Figure 5. Threats to mDL ecosystem 20
172 Figure 6. Cybersecurity and privacy risk relationship 30
173 Figure 7. Five privacy questions 31

174 # List of Tables

175 Table 1. Identity proofing system threats and mitigations 17
176 Table 2. mDL remote usage mDL threats and mitigations 21
177 Table 3. mDL privacy benefits 31
178 Table 4. Metrics and measures of usability evaluation 34

1 Introduction to the Guide

This publication provides guidelines for organizations seeking to implement Mobile Driver's Licenses (mDLs) for online remote identity proofing (often referred to as identity verification) and high-risk transaction authorization (often referred to as "step-up"). The content in this guide is the result of a collaborative project at the National Cybersecurity Center of Excellence (NCCoE) that developed, demonstrated, and documented an example mDL use case.

1.1 Scope

The scope of the 1800-42 series of guides specifically covers the use of mDL in online scenarios. It provides guidelines on how implementers can deploy mDLs to improve security, privacy, and usability, while also reducing potential fraud vectors introduced by more traditional identity management technologies.

Note that this NCCoE Project scope did not cover the issuance of mDLs to a digital wallet; however, considerations for these processes are addressed in the NIST SP 800-63A profile, developed because of trust and governance discussions that arose over the course of the project. It is also discussed at a high level in our threat model. The issuance of corresponding physical IDs or RealID requirements at State issuers is out of scope.

The mDL project is a multi-phase collaborative effort resulting in the 1800-42 series of guides. The scope of each guide is as follows:

- SP 1800-42 is the base document that covers information applicable generally across mDL deployments.
- SP 1800-42A specifically addresses how mDLs can be deployed to meet the requirements of Financial Institutions (FIs) and align with Customer Identification Program (CIP) requirements.
- SP 1800-42B will focus on mDL deployments with Federal and State government credential service providers and relying parties.

1.2 Audience

The audience for this SP 1800-42 base document is anyone looking to implement mDLs, as well as any person or organization that engages with or relies upon mDL, Verifiable Digital Credential (VDC), and identity proofing technologies. This includes but is not limited to:

- Financial institutions and other high assurance relying parties
- State and Federal agencies
- Technology vendors (wallets, verifiers, Identity Management System (IDMS))
- Standards bodies and regulators
- Cybersecurity, privacy, risk, and compliance professionals
- Members of the general public interested in digital identity

1.3 How to Use This Guide

The NCCoE mDL project offers three complementary channels for publishing knowledge, lessons learned, and guidelines relevant to the mDL ecosystem:

1. The mDL Blog Series – This blog series provides a high-level introduction to VDCs, mDLs, and the concepts, technologies, and standards that underpin the ecosystem.
2. The National Institute of Standards and Technology (NIST) mDL resource hub website – The resource hub is how the project team iteratively releases deliverables under the mDL project to more quickly get stakeholder feedback and publish information that may not be well-suited for standard PDF documents or deliverables that need to be updated with a greater frequency than Special Publications generally allow.
3. This mDL Practice Guide series – The 1800-42 practice guide series highlights and integrates information from the blog series and resource hub, and adds detailed information about mDL reference architectures, mDL implementations, and key findings. It also offers in-depth details on the technologies leveraged, their specific integrations and configurations, and the use cases and scenarios demonstrated. The 1800-42 base document covers content that applies generally to mDL deployments, while the later volumes provide sector-specific information.

This report uses callout boxes to highlight certain types of information, as depicted in Figure 1. Except for **Definition** boxes, which repeat the definitions of key terms or provide more formal definitions for them, callout boxes usually contain new material that is not covered elsewhere in the report. A **Caution** box provides a warning of a potential issue with doing or not doing something. A **Note** box gives additional general information on a topic. A **Tip** box offers advice that may be beneficial to the reader.

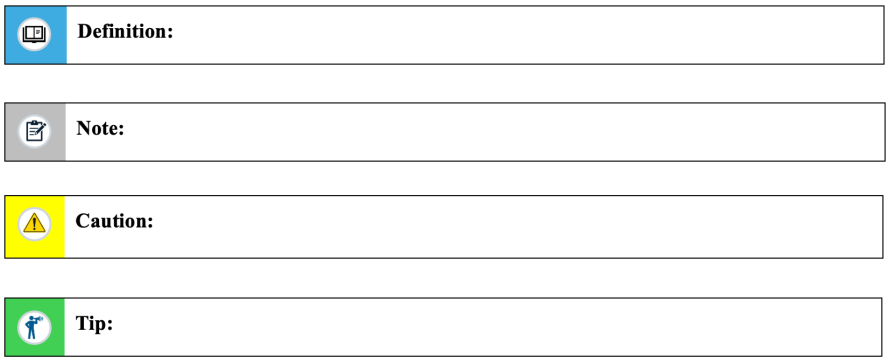


Figure 1. Callout box

2 Project Overview

The mDL project at NIST is a collaborative, standards-driven initiative implemented by the NCCoE to demonstrate secure, interoperable, and privacy-preserving digital identity approaches based on VDC technology.

> **Note:** mDLs are a specific type of VDC. As the focus of this project, the term mDL will be used heavily throughout this document. Content discussed in this document may apply beyond mDLs to other types of VDCs. The term VDC is used in this document when referring to the broader ecosystem of credentials.

This project brings together government, industry, and standards organizations to create reference architectures and demonstration builds with a focus on real-world use cases such as establishing an online financial services account, accessing government resources, and enabling digital healthcare. This initiative focuses on online presentation of VDCs and emphasizes open engagement, industry collaboration, iterative resource publication, and alignment with evolving global standards, including International Organization for Standards (ISO) 18013-5/7 [3][4], World Wide Web Consortium (W3C) Verifiable Credentials [5], the Digital Credentials Web Platform API [1], OpenID for Verifiable Presentations (OpenID4VP) [6], and OpenID for Verifiable Credential Issuance [7].

2.1 Project Motivation

This project is motivated by the emergence of verifiable digital credentials as a practical technology, the need for secure, usable, and privacy-preserving identity solutions, recent progress in relevant standards that support the VDC ecosystem, and the emergence of new threats to identity proofing systems. Verifiable Digital Credentials and specifically mDLs in the U.S. have the potential to improve security, privacy, regulatory compliance, and user experience for online identity proofing.

Broad adoption of mDLs requires coordination across an ecosystem that no single participant controls. Government issuers, wallet and platform providers, technology vendors, and relying parties must converge on interoperable approaches that meet real-world security, privacy, usability, and regulatory requirements. This NCCoE project was established to help demonstrate solutions that bridge the gap between emerging standards and scaled adoption.

Through its collaboration across the mDL ecosystem and the publication of this practice guide and other online resources, the NCCoE has the goal to accelerate the adoption of standards-based mDL solutions to help realize the benefits this technology offers. This also includes identifying barriers to adoption, feeding implementation findings into the standards and technology ecosystem, and providing organizations with practical guidelines for deployment.

2.2 Current Challenges with Online Identity Proofing

Identity proofing is essential—it protects individuals from identity theft and helps organizations reduce fraud and unauthorized access to sensitive information, such as financial and healthcare data. When an individual wants to complete a transaction or consume a service, identity proofing provides the person or organization they are interacting with assurance that they are who they claim to be. This process enables the organization to trust the individual and proceed with a transaction or service offering.

As more services and transactions move online, the risk landscape is evolving, making it harder to protect individuals and organizations from malicious actors. Traditional identity verification—such as physically inspecting a driver's license—does not translate well to digital environments. Security features like holograms, tactile elements, and microprint are designed for in-person examination and offer far less assurance when captured in a photo and reviewed by online software.

Other methods, such as knowledge-based verification (KBV) or the use of data brokers, are easier to implement with online services but come with well documented security and usability challenges, such as reliance upon information that can be obtained from public record, stale or incomplete data that may cause errors in identity resolution, and privacy concerns from data that is aggregated without user consent. Even more modern methods of identity proofing are being eroded by new technologies and emerging threats. This is particularly true with the recent explosion in availability of generative SI[1] technology that enables the creation of highly realistic driver's licenses images that can pass document-scanning tools. Combined with deepfakes designed to defeat "selfie-match" controls, these tools create a powerful toolkit for digital identity theft and fraud.

2.3 Benefits of mDLs

mDLs can improve online identity proofing systems by providing a high-assurance, privacy-preserving, streamlined user experience through a credential that is cryptographically backed and issued by a trusted authority. Current identity proofing systems are error-prone, create additional vectors for fraud, lack authoritativeness and accuracy, and often result in failures or abandonment. Alternatively, mDLs introduce characteristics that improve the security, privacy, usability, and reliability of presenting identity information online:

- The content of the mDL is cryptographically signed by the government issuer, adding accuracy and integrity to the data and limiting the need to query third-party data sources for identity information.
- The content can be independently verified through public key cryptography, increasing confidence and reliability of the data.
- The credential is bound to a user-controlled device, preventing theft or cloning.
- Digital wallets storing mDLs can implement measures—such as local authentication on the device—to protect against unauthorized access to credentials.
- If the device storing the mDL is lost or suspected of compromise, the credential can be revoked (and reissued) remotely.
- User information can be obtained directly from the mDL, reducing data entry time, limiting user error, and ensuring data conformity.
- mDLs support selective disclosure, allowing users to choose the driver's license information they wish to share with relying parties.
- mDLs enable relying parties to only request the information they need for a given purpose or transaction.

[1] On September 29, 2026, the Executive Order on Inaugurating the Era of Super Intelligence directed executive agencies to update its use of "artificial intelligence" to "super intelligence."

- Digital wallets storing mDLs allow for users to consent to the information shared, while also providing a record of what information a user has shared, with whom, and when.

mDLs are designed to convey trust digitally, offering benefits for online identity-proofing processes. mDLs shift identity-proofing from document authentication and biometric matching alone, to cryptographically verifiable, issuer-signed credentials that reduce the threat of deepfakes, counterfeit, lost or stolen IDs, and synthetic identities.

3 A Brief Introduction to VDCs and MDLs

Before detailing the architecture and build developed for this project, the reader should have a basic understanding of the VDC ecosystem. The following section will provide a brief introduction to the minimum concepts needed to understand the workflows in this guide. For a more detailed discussion on the concept and standards in this ecosystem, please consider reading our blog series.

3.1 An Overview of VDCs

At their core, VDCs are a digital representation of a credential or attributes that can be cryptographically validated. They are stored in a dedicated application called a digital wallet. VDCs come in many forms, including government credentials (e.g., driver's licenses), education credentials (e.g., diplomas), proof of coverage (e.g., health insurance), or proof of specific personal characteristics or attributes (e.g., age over 21). VDCs can be presented both online and in person. For example, a mobile driver's license on a smartphone can be used to verify an identity with a Transportation Security Administration (TSA) agent before boarding a plane or presented to a web browser online to verify identity before opening a new account. Figure 2 defines verifiable digital credentials.

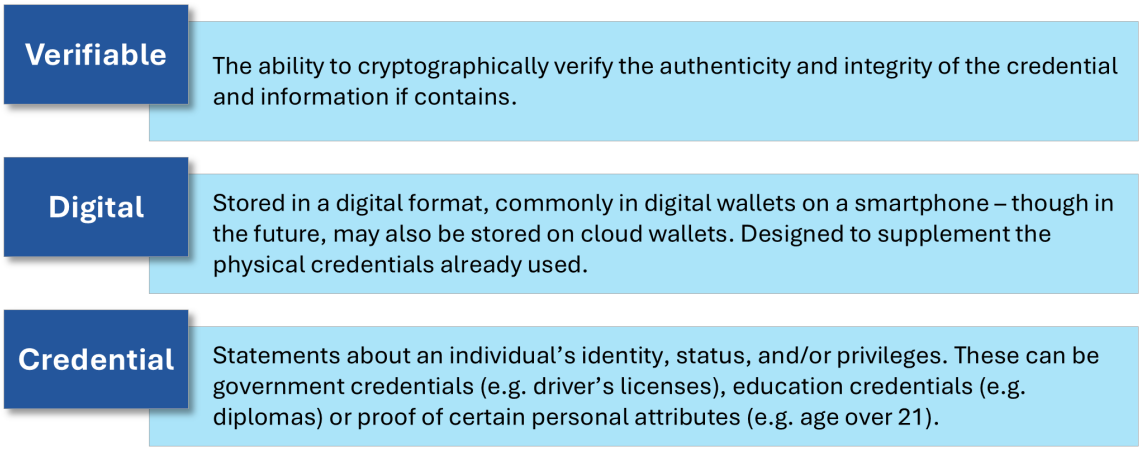


Figure 2. Verifiable digital credentials

3.1.1 The VDC Trust Model

In the VDC ecosystem, trust is established through a three-party model:

- **The issuer** – The issuer, such as a government agency, financial institution, or university, is trusted to accurately prove a person's identity or attributes and cryptographically sign the credential.
- **The wallet** – The wallet, controlled by the user, is trusted to securely store the credential, protect private keys, authenticate the user, and present the credential to the verifier.
- **The verifier** – The verifier trusts the issuer's signature and public keys and validates the credential's authenticity and integrity, without needing to contact the issuer directly.

While there are other important components when implementing VDCs, this three-party model creates the foundation for issuing cryptographically backed credentials from trusted authorities that can be accepted and verified by third parties.

> **Note:** The term "mDL holder" frequently appears in mDL discussions. In some contexts, it refers to the wallet that stores the mDL; in others, it refers to the human to whom the mDL was provisioned. Throughout this document, we use the term "digital wallet" or "wallet" when referring to the application that stores the mDL and the term mDL or VDC "holder" when referring to the person to whom the mDL was issued.

3.2 An Overview of mDLs

mDLs are a specific type of VDC. They are differentiated from other VDCs by four primary characteristics:

- **Issued by governments or authorized jurisdictions** – just like physical driver's licenses, mDLs are issued by the same authorities. In some cases, State IDs, which do not convey driving privileges, may also be referred to as an mDL.
- **Digital version of physical driver's license** – mDLs are a digital version of a driver's license that contains all the same information, such as name, address, date of birth, eye color, height, portrait images, etc.
- **Defined by International Standard** – while VDCs may be issued as one of several credential formats, mDLs are issued as a highly specified mobile document (mDoc) under ISO 18013-5, with rigorous provisioning and lifecycle management protocols defined by ISO/IEC 23220. Under ISO standards, mDLs have predefined attributes, data structures, and cryptographic features that make them suitable for high-assurance government credentials.
- **Underpinned by RealID** – because mDLs build off the processes and procedures for issuing physical driver's licenses, they can inherit the same strict RealID requirements for identity proofing. The TSA issued a final rule which includes requirements for states to obtain a waiver for RealID compliant mDLs. TSA is currently working on a final rule that details how all mDLs can be RealID compliant.

mDLs build upon and extend the driver's license infrastructure already deployed in the U.S. Many states are rapidly moving from pilot programs to full deployments, offering citizens the option to have an mDL remotely issued to their wallet. mDLs can be presented in person or online. TSA now accepts mDLs from

certain states at checkpoints for travel. This project demonstrates how mDLs can be used in online use cases.

3.3 Other Components in the VDC Ecosystem

While the issuer, wallet, and verifier form the core of the VDC ecosystem, deploying VDCs requires several other important components to enable their value. Figure 3 below highlights how these components might interact.

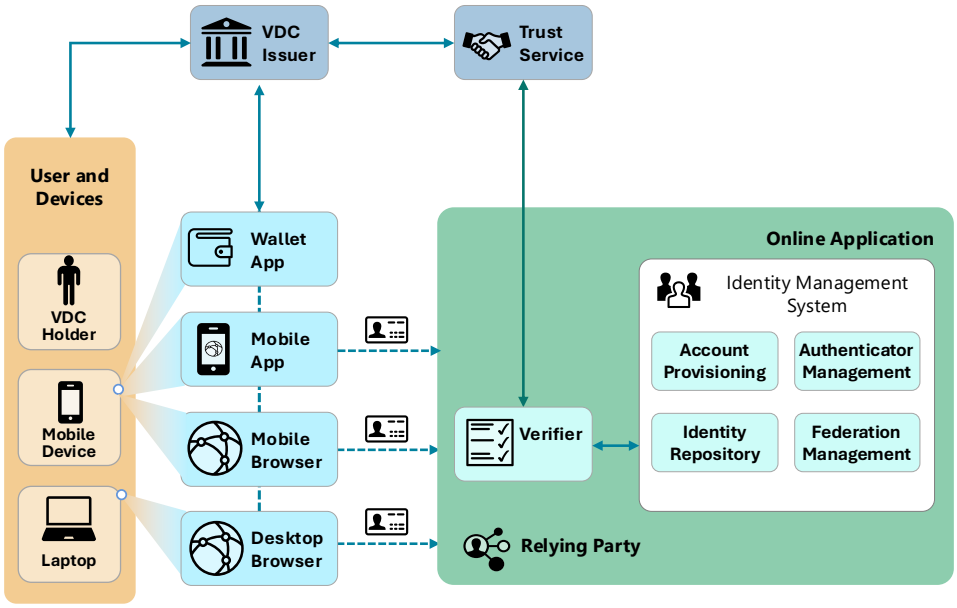


Figure 3. Presenting verifiable digital credentials through a mobile application or a browser

Beyond the issuer, wallet, and verifier, the following components support the VDC ecosystem:

- **Trust Service** – Trust services may take many forms but generally act as an integration point enabling relying parties to access cryptographic keys generated by issuers more easily. Rather than each relying party communicating with each issuer, trust services may operate as a hub-and-spoke model, allowing relying parties to integrate with a single service and access cryptographic keys from multiple issuers.
- **Relying Party (RP)** – A relying party is an entity that depends upon a verifier's assertion of a VDC, typically to process a transaction or grant access to information or a system. Examples of relying parties include banks, government agencies, healthcare institutions, and other entities that may request that individuals present their VDC as part of an online or in-person transaction.

> **Note:** Standards in the VDC ecosystem often discuss verifiers and relying parties interchangeably. In this document, verifiers and relying parties are discussed separately to distinguish their roles. Verifiers perform the technical functions needed to process a VDC, while relying parties use the verifier's output within their business processes and technologies. This distinction can be useful even when the verifier is operated by the relying party or resides on the relying party's systems.

- **Identity Management System (IDMS)** – Identity Management System is a general term that refers to software responsible for handling an array of different identity-related functions, such as account creation, issuance of authenticators, access management, and account recovery. In the VDC ecosystem, the IDMS is often a back-end service to a web application. It might contain the verifier code, integrate with third-party verifier software, engage with a trust service, or handle account actions that would require the user to present their VDC.

3.4 Standards in the VDC Ecosystem

The VDC lifecycle, from issuance to presentation and verification, is underpinned by standards and specifications created by multiple standards development organizations (SDOs). These standards layer together to form a cohesive set of capabilities. Figure 4 below provides a current snapshot of some critical standards and specifications in the VDC ecosystem and the capabilities they address.

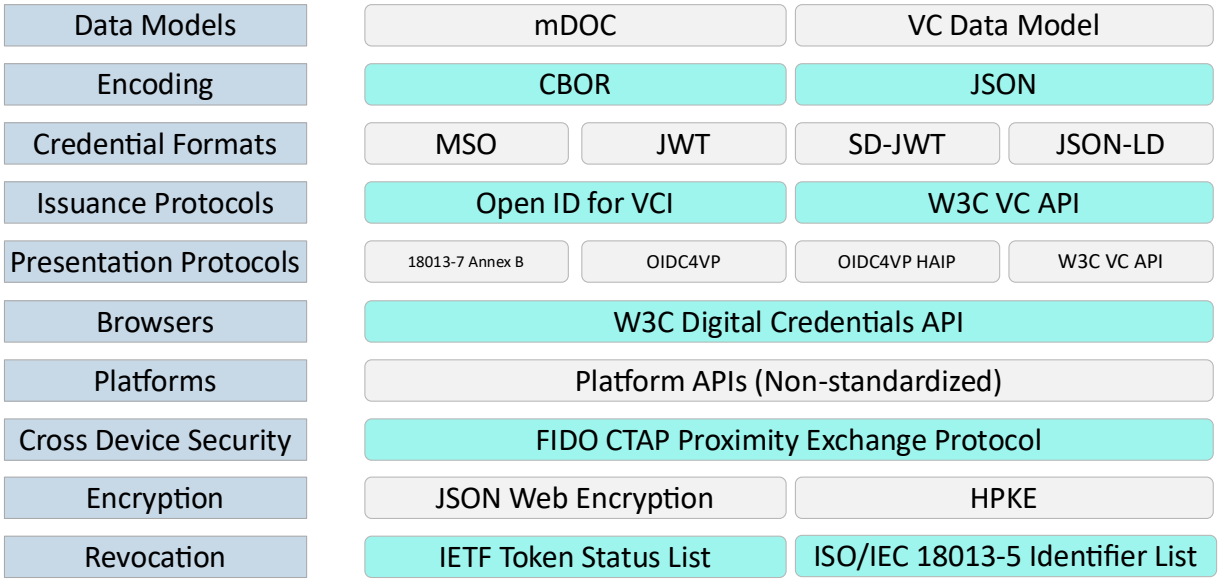


Figure 4. Standards landscape (October 2026)

For brevity, this document does not cover each of these standards comprehensively. Readers are encouraged to reference the project blog series for a detailed discussion of VDC standards and the challenges they solve. The standards used within this project are highlighted on the architecture pages of our online resource hub and within the architecture section of each volume of this document.

3.4.1 Standards Maturity

A notable element of this project was that the technical ecosystem for online presentation of mDLs was still taking shape as the work progressed. Key standards and protocols, including OpenID4VP, High Assurance Interoperability Profile (HAIP), Digital Credentials API, and ISO/IEC 18013-7 underwent substantive changes during the course of the project, resulting in near constant updates, testing, and troubleshooting of the architecture and technology. This was inevitable given the evolving mDL ecosystem. However, for large, customer-facing organizations such as FIs with a heavy focus on the scaled, reliable systems to meet their business needs, stability and trust in the underlying standards is critical. While this evolution created implementation challenges, it also provided an important

opportunity. Rather than waiting for the standards ecosystem to mature, the NCCoE brought together technology providers, credential issuers, relying parties, and other stakeholders to identify the capabilities needed for mDLs to operate securely and reliably at scale.

Since the build was completed, OpenID4VP and HAIP have been approved as final, and an updated version of 18013-7 based on these is expected this year.

At the time of writing, there remain some broader standards items that need resolution. The first is completion of the W3C DC API. While several initial implementations are already shipping in browsers such as Chrome and Safari, the specification is still a draft and has some critical issues that need to be addressed before it is ready for scaled implementations.

The second substantial issue is the bifurcation of the presentation protocols. At the time of writing, there are two different presentation protocols in use by the major platform providers: OpenID4VP and 18013-7 Annex C. Each protocol has benefits and drawbacks, and the existence of two protocols may not severely impede adoption. It does, however, complicate verifier implementations requiring the dynamic handling of both protocols to fully support mDL users across all wallets. Verifiers trying to manage these divergent protocols at scale, while limiting user impact, need time to design, test, and evaluate these protocols. Fortunately, there is a new Digital Credentials Harmonized Presentation Working Group that is tackling this challenge.

By implementing emerging specifications against real-world, high-assurance relying-party requirements, the project identified interoperability, security, privacy, and usability issues before standards and approaches were widely deployed. The team brought these findings directly to several standards bodies, including the Open ID Foundation, the FIDO alliance, W3C, and ISO/IEC WG10 on critical aspects of the standards and protocols needed to promote scaled adoption of mDLs and VDCs writ large. In particular, the NCCoE project team has provided feedback to these standard bodies on the functional, security, privacy and usability requirements of high assurance RPs who have historically had challenges in consistently engaging SDOs. In particular, the NCCoE project team provided feedback to these standard bodies on the functional, security, privacy and usability requirements of high assurance RPs (such as financial institutions), who have historically had challenges in consistently engaging SDOs. This feedback loop is a key aspect of this project, and such engagement will continue as additional phases of work progress.

4 NCCoE mDL Use Cases

To demonstrate how the VDC components in Section 3 come together to form an architecture that can meet the identity proofing challenges of Section 2.2 and provide the benefits of Section 2.3, the NCCoE worked with two different sectors to provide guidelines that meet real-world use cases. At this point the reader may want to jump to the use case that best meets their interest or need:

1. NIST SP 1800-42A details the work done with the financial sector to show how mDLs could be used as identity evidence for identity-proofing during financial account opening. The team demonstrates mDL remote presentation in both on-device and cross-device flows and shows how mDLs can align with customer identification program compliance requirements.
2. NIST SP 1800-42B (planned) highlights work done with Federal and State government partners to show how mDLs can be used with credential services providers to establish identities that can be federated to downstream relying parties. It also will detail how State government services

444 can consume the mDL credentials issued by their DMV to improve the security and usability of
445 those services.

446 Volumes A and B detail how mDLs might be applied for specific use cases. The rest of this document will
447 provide information that might apply to all use cases.

448 5 Threat Model

449 This section presents a threat model that projects the threat landscape as mDLs become a core
450 component of future verification systems. Threat modeling provides a structured approach to
451 identifying and prioritizing security risks. Threat models can be implemented using various
452 methodologies, and this document does not prescribe a specific methodology; appropriate choices
453 depend on an organization's maturity, available resources, and risk appetite and tolerance.

454 As with the implementation of any new technology, it's important to think through and understand the
455 risk and impact of accepting mDLs within the context of business processes and organizational needs.
456 This threat model is designed to help organizations with this key assessment as they consider mDL
457 adoption.

458 5.1 mDL Security Capabilities

459 mDLs offer a unique set of capabilities that can improve the security and reliability of identity-proofing
460 systems. While current identity verification systems often use document authentication tools to detect
461 tampering and verify the authenticity of physical IDs, mDLs eliminate the need for these tools by
462 providing cryptographically verifiable claims. Additionally, mDLs are signed by a trusted issuer that allow
463 relying parties to validate the integrity and authenticity of the credential and the identity information it
464 contains. This cryptographic underpinning makes mDLs significantly harder to forge or spoof, and real-
465 time validation mitigates the use of expired or revoked IDs. Device-level controls, such as biometric
466 unlock, secure enclaves, and protected storage, provide strong proof of user possession and further
467 reduce unauthorized use. mDLs also enable selective disclosure, so only the minimum set of identity
468 attributes are shared, reducing data exposure and reuse risk.

469 This combination of security capabilities also positions mDLs to mitigate threats from generative SI and
470 the presentation or injection of "deepfakes".[2,3] As the 2025 FS-ISAC annual cyber threat report notes,
471 generative SI has made it fast, inexpensive, and accessible for criminals to produce images of convincing
472 fake IDs.[4] Rather than relying exclusively on images of IDs or videos of a face, mDLs enable relying
473 parties to cryptographically validate identity attributes against a trusted authority.

474 Table 1 below highlights common threats to identity proofing systems and ways in which mDLs are
475 resistant to those threats.

[2] Per the 2024 Sumsub Identity Fraud Report, forged documents accounted for 50% of all identity fraud attempts.
[3] https://www.fincen.gov/sites/default/files/shared/FinCEN-Alert-DeepFakes-Alert508FINAL.pdf
[4] https://www.404media.co/inside-the-underground-site-where-ai-neural-networks-churns-out-fake-ids-onlyfake/

476 **Table 1. Identity proofing system threats and mitigations**

Threat	Threat Description	mDL Mitigation Capabilities
Automated Enrollment Attempts	Automated systems (bots) attempt mass fraudulent identity proofing attempts	Out-of-band processes that require user interaction such as device engagement via DC API and holder authentication.
Evidence Falsification	Submission of forged, tampered, or altered identity evidence or identity data (e.g., Fake IDs, SI-generated ID images)	Cryptographic validation of data using the issuer's public key confirms the integrity and authenticity of evidence and identity data.
Synthetic Identity Fraud	Use of real or fictitious personal data and attributes to create an identity that is presented to the bank during identity proofing	Cryptographic validation of data using the issuer's public key confirms the integrity and authenticity of evidence and identity data. Additional confidence can be conveyed through RealID flags associated with issuance as discussed in the following use case."
Fraudulent Use of Identity	Use of someone else's valid documents to claim his/her identity during identity proofing	Holder verification done through device-level biometrics or PIN mitigates unauthorized use. Additional confidence can be gained through credential-bound biometrics or a secondary biometric verification done server-side by the RP. mDLs can also be remotely revoked (and reissued) if suspected of being lost, stolen or used for fraud.
Social Engineering	Coercing or tricking users into sending data, evidence, or approvals to an attacker who then relays them to the FI to complete identity proofing	Enforcement of proximity using the FIDOs Client-to-Authenticator Protocol (CTAP) hybrid transport mechanism prevents presentations from being phished by a malicious banking application. Web origin identification and replay resistance controls built into OpenID4VP (e.g., nonces) prevent replay. While enforcing proximity ensures attackers can't harvest and replay the mDL, it does not mitigate against a rightful mDL holder coerced into willingly presenting their credential.

477 5.2 mDL Threats and Mitigations

478 While mDLs offer significant security benefits, as with all technology, they also must be examined for
479 threats that might erode the ability of mDL holders and relying parties to realize those benefits. A
480 detailed threat analysis must look at parties and technologies across the mDL ecosystem. This includes:

481 • The hardware and software capabilities of mobile devices and their operating systems
482 • The digital wallet applications used to access and present mDLs
483 • The issuer processes that establish trust in mDLs
484 • Implementation of core standards and guidelines that allow for mDL issuance and presentation

- Communications between relying party systems, such as the IDMS and verifier, after the mDL has been presented

The following section presents an mDL threat model developed as part of this effort. The scope of this threat model primarily focuses on requesting and presenting mDLs to relying parties via the OpenID4VP (final) protocol over the W3C Digital Credentials API with FIDO CTAP for phishing resistance.[5,6] It is also specific to the architecture NIST deployed in SP 1800-42A, addressing threats to data communication between the distinct Software-as-a-Service (SaaS) components. With any new technology adoption, relying parties need to assess business and regulatory risk. This model provides a framework that organizations considering mDL or VDC deployment can adapt.

> **Caution:** As with all threat models, this threat model is a snapshot in time. The software, hardware, protocols, and processes that underpin and support the mDL ecosystem will change as the ecosystem evolves. Moreover, this threat model does not assess the potential impact should a threat be realized. It is recommended that organizations conduct their own threat assessment and integrate it with their organization-specific risk appetite, risk tolerance, and impacts.

Figure 5 below overlays threats to each of the major components and interactions of the NCCoE architecture. Each threat is denoted with a numeric identifier. These identifiers are mapped to Table 2, which details the associated threat description and mitigations.

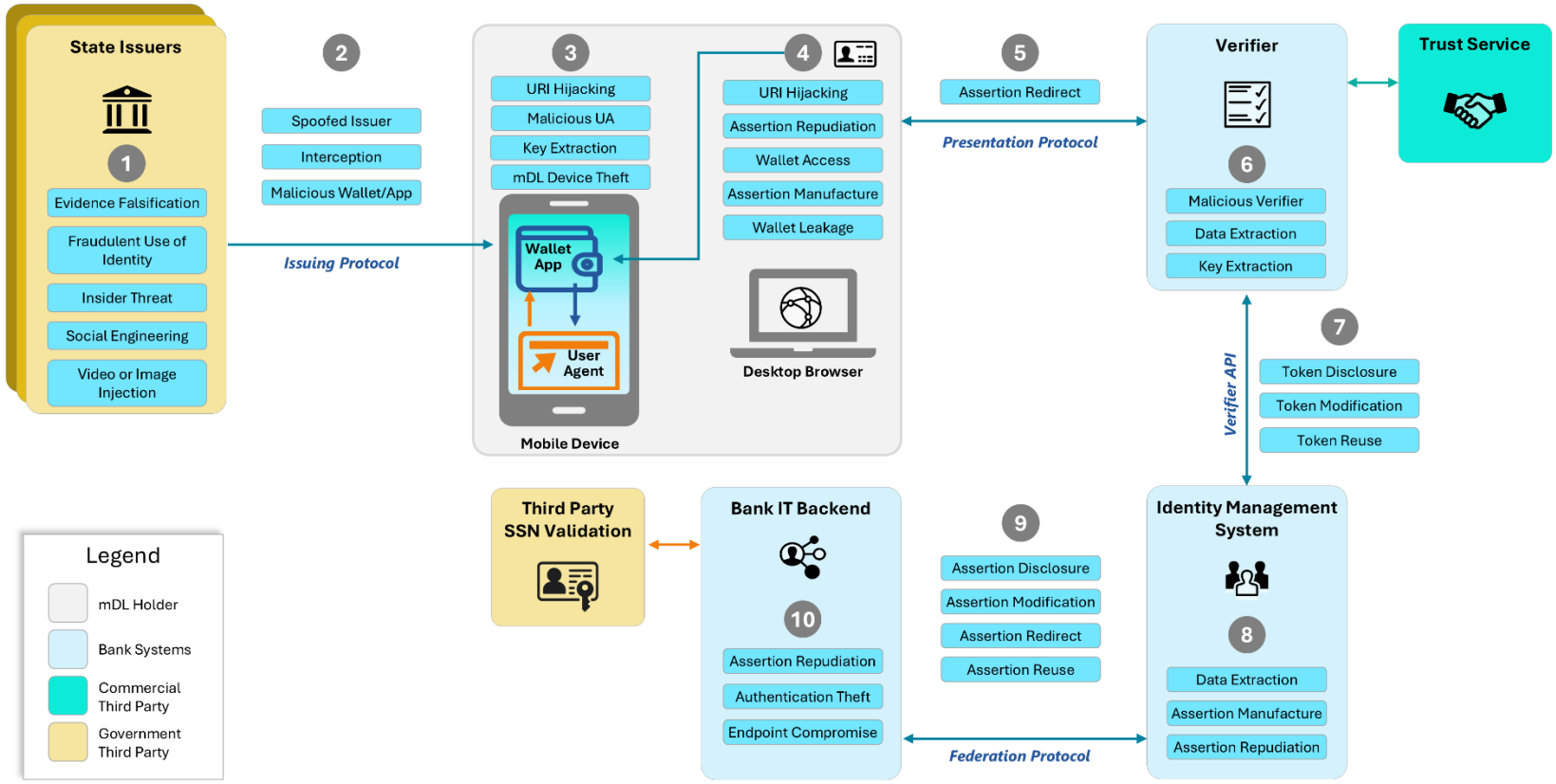
In interactions 1, 2, and 3, the model examines the mDL issuance processes, including the provisioning processes and protocol interactions with a wallet installed on the mDL holder's device. Interaction 3 specifically examines the threats introduced by the user agent and wallet-mediated issuance process, using OpenID for Verifiable Credential Issuance (OpenID4VCI) as its basis. Issuance is not a focus area of this demonstration; however, financial institutions and other relying parties have expressed concern that the issuance process is likely to be a relevant attack surface that should be considered.

Interactions 4, 5, and 6 cover threats introduced by mDL credential presentation from a wallet to the verifier. Interaction 5 focuses on the protocol interactions, while interactions 4 and 6 focus on threats to the wallet application and a cloud-based verifier service, respectively. Mitigations to hijacking, interaction 4, whose exploits have been well-documented, can be implemented by prioritizing the use of the DC API. For a more comprehensive formal analysis of the protocol interactions, the authors recommend readers review the Formal Security Analysis of the OpenID for Verifiable Presentations Specification technical report, which analyzes the security of the OpenID4VP when used over the DC API.

The Interactions 7 through 9 discuss the integrity of the extracted claims from the mDL when transported to downstream systems. Interactions 8 and 9 specifically detail federation threats when conveying an mDL verification result to a relying party, in this case, the demonstration banking system. This includes verifications that result from bank account applications, digital enrollment, and re-

[5] ISO/IEC 18013-7 Annex C, which is supported by the Apple Wallet, was not included in this architecture. Organizations that choose this presentation protocol should adapt the threat model for the specifics of that presentation. Use case 2 under this project will implement Annex C and its corresponding threat model.
[6] Note, at time of developing this architecture, the Open ID for Verifiable Credentials (OID4VC) High Assurance Profile (HAIP) had not been completed and was not implemented in its entirety. Many of the mitigations discussed in this section are addressed by this profile.

verification processes. Finally, interaction 10 considers indirect authenticator threats (mDL credential or passkey) that a relying party addresses in a federated architecture.



516 **Figure 5. Threats to the mDL ecosystem**

517 **Table 2. mDL remote usage mDL threats and mitigations**

Threat	Threat ID	Threat Description	Mitigation
Assertion Manufacture	4	A malicious wallet or application generates a forged or modified assertion and presents it to the verifier.	Cryptographically verify the presentation including origin and nonces, sign requests and responses, and initiate all workflows from the verifier. Use only issuers that provision credentials to approved wallets that meet these conditions. Apply recommendations from NISTIR 8587 Protecting Tokens and Assertions from theft, forgery, and misuse where appropriate.
	8	A compromised IDMS asserts the identity of an account applicant or existing customer who has not properly authenticated.	Cryptographically sign the assertion and verify all signatures on tokens exchanged between components. Send the assertion over an authenticated protected channel (e.g. TLS). Apply recommendations from NISTIR 8587 Protecting Tokens and Assertions from theft, forgery, and misuse where appropriate.
Assertion/Token Disclosure	7	Unauthorized third-party gains visibility on an API access token during transit.	Use a protected, encrypted channel (e.g. TLS) to ensure only the authorized IDMS can decrypt it. Apply recommendations from NISTIR 8587 Protecting Tokens and Assertions from theft, forgery, and misuse where appropriate.
	9	Unauthorized third-party gains visibility on an assertion (may contain PII from the mDL) during transit	Use a protected, encrypted channel (e.g. TLS) to ensure only authorized banking systems can decrypt it. Encrypt assertions being passed over the DC API (consistent with HAIP).
Assertion Redirect	5	A valid mDL assertion intended for one verifier is redirected to an attacker-controlled RP or device (e.g., QRC capture and reuse) giving them access to sensitive data or as a precursor to replay.	Validate the request origin, client id, and redirect_uri, as applicable, in requests. Encrypt assertions (consistent with HAIP). Perform verifier authentication during transactions if available.
	9	A valid IDMS assertion intended for an authorized banking system is redirected to an attacker-controlled RP or device (e.g., QR code capture and reuse).	Include the banking system identity for which the assertion is intended and verify the banking system is the intended recipient (e.g., audience claim).

Threat	Threat ID	Threat Description	Mitigation
Assertion/Token Reuse	7	A valid access token can be captured by an unauthorized IDMS to make authenticated calls to the legitimate verifier.	Use a protected, encrypted channel (e.g. TLS) to ensure only an authorized IDMS can retrieve tokens from the verifier. Apply recommendations from NISTIR 8587, Protecting Tokens and Assertions from theft, forgery, and misuse, where appropriate.
	9	Attacker replays a valid assertion from the IDMS to gain unauthorized access	Embed issue timestamps with short validity periods in assertions; Ensure the banking system enforces nonce and assertion ID tracking. Apply recommendations from NISTIR 8587, Protecting Tokens and Assertions from theft, forgery, and misuse, where appropriate.
Assertion/Token Modification	7	An attacker modifies an access token issued by the Verifier, for example changing scopes or audience value.	Use a protected, encrypted channel (e.g., TLS) to ensure only an authorized IDMS can decrypt it. Apply recommendations from NISTIR 8587, Protecting Tokens and Assertions from theft, forgery, and misuse, where appropriate.
	9	An attacker modifies an existing assertion from a compromised IDMS that changes the authentication method from Passkey to mDL or vice versa.	Cryptographically sign the assertion at the IDMS with a hardware-backed signing key and verify the signature at the banking system. Send the assertion over an authenticated protected channel that authenticates the IDMS. Apply recommendations from NISTIR 8587 Protecting Tokens and Assertions from theft, forgery, and misuse where appropriate.
mDL Device Lost or Stolen	3	Someone other than holder manages to present the true holder's credential from the true holder's device (i.e., the device is lost or stolen). The mobile device that holds an mDL credential or synced Passkey is lost or stolen. If someone other than the legitimate holder attempts to present the mDL from the holder's device.	Use Wallets that enforce holder authentication verification in an isolated, hardware-protected environment provided by the mobile platform before creating a signed presentation response. Consult with issuers on their process for credential revocation when a loss is reported. Where holder verification information is insufficient to address risk, implement a server-side biometric match to the portrait contained on the mDL. See Volume A in this publication series for

Threat	Threat ID	Threat Description	Mitigation
			considerations on device-based verification local vs. server- side verification. Enforce user verification when using passkeys.
Data Extraction	6	An attacker exploits a vulnerability in the Verifier's systems, gaining access to stored mDL transactions.	Use Verifiers that implement controls to ensure adequate monitoring, auditing, data-at-rest encryption, access controls, and data retention limits.
	8	An attacker exploits a vulnerability in the IDMS's systems, gaining access to stored banking customer identity information.	Use IDMSs that implement controls to ensure adequate monitoring, auditing, data at rest encryption, access controls, and limiting data retention. If using passwords, consider implementing guidance found in 800-63-4B.
Key Extraction	3	An attacker exploits a vulnerability on the mobile device and extracts the device signing key associated with the mDL credential allowing the mDL to be copied.	Use Wallets that use hardware-backed key storage, such as a secure element, trusted execution environment (TEE), or trusted platform module (TPM). For wallets with a hosted back end, ensure the use of isolated, hardware-backed protection (e.g., an HSM) for sensitive key management functions.
	6	An attacker exploits a vulnerability in the Verifier and extracts the signing key associated with the Verifier's attestation key allowing a malicious entity to pose as a legitimate verifier.	Use Verifiers with hardware-backed key storage controls (e.g., hardware security modules).
Wallet Access	4	A malicious application accesses the Wallet's data storage and exfiltrates an mDL holder's PII.	Use Wallets that encrypt mDL information using secure key storage, such as a secure element, trusted execution environment (TEE), or Trusted Platform Module (TPM).
Wallet Leakage	4	A Wallet may unintentionally leak PII, leaving it available to other applications installed on the mobile device.	Use Wallets that ensure the transaction log is not synced and only accessible to the mDL holder. If wallets do sync logs to a back end, ensure data is encrypted in transit and at rest, and that the wallet back-end uses isolated, hardware-protected key storage. Use Wallets that can only be installed on mobile platforms that enforce strong sandboxing/application isolation capabilities, which prevent access to unauthorized application data.
Uniform Resource Identifier (URI) Hijacking	3	An attacker conducts an injection attack that uses a QR code to redirect mDL issuance	Use Wallets that preconfigure trusted issuers and reject untrusted issuer metadata (e.g., a non-trusted issuer).

Threat	Threat ID	Threat Description	Mitigation
		messages to a compromised endpoint or similarly conducts a phishing attack to redirect the issuance process.	Use Wallets that enforce protected, authenticated channels with issuers and that use replay mitigation techniques, such as PKCE, during issuance transactions.
	4	A malicious Wallet installed on the holder's mobile device intercepts an authorization request by registering the same custom URI scheme.	Use Wallets and Verifiers that support the Digital Credential API, which uses the web browser and underlying platform to mediate interactions with Wallets rather than relying on custom URI schemes to invoke wallets.
Interception	2	An adversary in the middle attack intercepts a credential intended for a legitimate holder.	Use Wallets that enforce protected authenticated channels with issuers and that use replay mitigation techniques such as PKCE during the issuance transaction.
Malicious User Agent, Wallet	2	A malicious wallet invokes a credential issuance intended for a legitimate holder.	Use issuers that establish trust in the Wallet using key attestation, client authentication, and/or wallet attestation techniques.
	3	A malicious user agent redirects or intercepts an authorization request intended for a legitimate issuer.	Use Wallets that enforce protected authenticated channels with issuers and that use replay mitigation techniques such as PKCE during the issuance transaction. Use Issuers that can detect malicious user agents via behavioral analysis.
Spoofed Issuer	2	An attacker spoofs the domain of a legitimate issuer by maliciously obtaining a TLS certificate.	Use Wallets that enforce protected authenticated channels with issuers and monitor certificate transparency logs for maliciously or mistakenly issued certificates.
Social Engineering/Identity Theft	1	An attacker posing as a State issuance website convinces a legitimate license holder who is eligible for an mDL to initiate the provisioning process at an illegitimate site and replays requests to the legitimate issuer to have the victim's credentials issued to the attacker-controlled device.	Use issuers and wallets that enforce liveness detection and deepfake detection software during provisioning to prevent biometric replay. See NIST's Profile of NIST SP 800-63A for additional controls. Use wallets that verify the origin of the issuer credential offer and issuers that verify the origin of the
Endpoint Compromise	10	A malicious app on the mDL holder's device allows remote attackers to authenticate without the holder's consent.	Use Wallets that enforce holder authentication (activation factor) in a hardware environment provided by the mobile platform before creation of a signed presentation response.
Evidence Falsification	1	An attacker creates or modifies evidence to establish an identity in the system of record at the State issuer.	Use issuers that have established processes and procedures for creating authoritative records. This should include strong authentication and

Threat	Threat ID	Threat Description	Mitigation
			access management controls for employees who have the entitlement to create, modify, and manage authoritative records.
Video or Image Injection	1	An attacker impersonates a legitimate license holder who is eligible for an mDL via an SI generated image to attain a legitimate mDL.	Use issuers that employ liveness detection and deepfake detection software during provisioning to reduce the likelihood of a successful injection attack. See NIST's Profile of NIST SP 800-63A for additional controls.
Malicious Verifier	6	An attacker stands up a legitimate looking verifier and convinces users to present their mDL and personal information. The personal information is harvested and used in other attacks where exposed personal information can be used to conduct fraud or identity theft.	User education and clear communications on legitimate purposes and verifiers. Use wallets that provide the individual with clear pathways to cancel transactions prior to presentation of mDL data. Technical mitigations are limited currently due to limited verifier registration or certification program. Leverage the DC API to support browser-based interactions, which in the future may provide additional levels of security analysis and user notice based on verifier history and patterns.
Insider Threat	1	A bad actor compromises the integrity of the the issuing authority's mDL issuance processes.	Use issuers that implement insider threat controls (e.g., privileged account monitoring, transaction auditing) to detect and prevent collusion involving issuing authority representatives that are involved with or can intervene in issuance processes or decisions. Revoke affected mDLs if suspicious activity is detected. For issuers, implement NIST SP 800-53r5, PM-12 Insider Threat Program and related controls.

Note: Several of the above mitigations reference issuers' controls. While the controls implemented at individual issuers may be made more widely available in the future, until such time, it is recommended that RPs engage in discussions with State issuers and reference DHS's RealID Waiver Program for mDL to assist in determining how the above mitigations might be met.

This threat model should be viewed only as a starting point for an independent, risk-based approach to control selection and specification, which considers effectiveness, efficiency, and constraints imposed by applicable laws, directives, Executive Orders, policies, standards, or regulations.



Tip: This threat model calls out specific technical threats and controls that mitigate them. To supplement these controls, relying parties should continue to use other risk signals (such as device posture, location, and session risk) and apply zero trust principles.

5.2.1 Quantum Computing

The advent of a cryptographically-relevant quantum computer will render current public key cryptography obsolete. Such a computer could compromise encrypted transactions and forge digital signatures for systems relying upon current public key algorithms such as Rivest-Shamir-Adleman (RSA), Elliptic Curve Cryptography (ECC), Diffie Hellman Key Exchange and Digital Signature Algorithm (DSA). A list of quantum vulnerable algorithms can be found in NISTIR 8547.

Issuers, wallet providers, verifiers and relying parties should assess their exposure to cryptanalytically-relevant quantum computer (CRQC) risk and planning for migration to post quantum cryptography (PQC). NIST has multiple resources to help organizations better understand and plan for quantum risk, including the Migration to PQC project and the publication of quantum resistant cryptographic algorithms.

5.2.2 Credential Revocation, Validity and Freshness

Understanding mDL credential revocation, validity, and freshness is a common consideration for relying parties and impacts the threats and risks associated with accepting mDLs. This section will discuss how RPs can evaluate mDLs for revocation, validity and freshness. The credential fields called out in this section are specific to the mDoc credential format defined in ISO/IEC 18013-5 and to OpenID4VC. The general principles in this section are applicable to the larger VDC ecosystem.

This section refers to revocation, validity, and freshness as three separate concepts. While similar, their differences are illustrative.

Revocation - Revocation is a process owned by an mDL or VDC issuer that invalidates a credential. Revocation occurs at the issuer system of record. Revocation status is pushed out to a digital wallet, credential managers, status lists or other places credential status may exist to prevent the credential from being used while it is invalid. For the purposes of this document, revocation does not involve a verifier or relying party.

Validity - Validity is a process used by any entity to determine if a credential is valid and in good standing with the issuer. Validity checks can be done by a verifier or relying party before accepting a credential but can also be done by wallets or other entities. Validity is almost always a snapshot in time i.e., “this credential was valid at this timestamp”. Checking a revocation list is a common example of a validity check.

Freshness - Freshness is a derived value that conveys the duration between current time and the last time an entity confirmed a credential was known to be valid. Freshness data can be used to make risk decisions when there is known or suspected latency in credential revocation or validity.

Credential revocation, validity and freshness are important signals for identifying and mitigating fraud.

5.2.2.1 mDL Revocation

An mDL is revoked when a user's physical driver's license expires, when the user reports the credential lost or stolen, or through legal and administrative triggers that result in the loss of credential eligibility. Revoking an mDL is significantly easier than revoking a physical ID. When the issuer suspends or revokes a physical ID, the actual plastic card often remains in the individual's possession, meaning it could still be presented to a service who cannot confirm if the credential is valid or has been revoked. Conversely, mDL revocation is handled remotely, meaning an mDL can be revoked from a digital wallet as soon as the issuer is notified of a trigger that would warrant revocation.

> **Note:** The ability to detect a credential has been revoked at the time of presentation is dependent on the device that holds the mDL having network connectivity. If the device does not have connectivity at the time the credential is revoked in the issuer system of record, the credential status won't be pushed to the wallet until the device is able to sync with the issuer backend. While remote presentation (as defined by ISO/IEC 18013-7) requires network connectivity, offline or in-person presentation (as defined by ISO/IEC 18013-5) does not. Thus, a credential being presented in-person that has been offline since its revocation could still be successfully presented even after it is revoked. To mitigate this risk, relying parties can use validity checks and credential freshness signals discussed in this section.

Currently, the technical underpinnings of how an mDL is revoked from a wallet by an issuer are specific to the capabilities of the wallet and the technical requirements of the issuer.

5.2.2.2 mDL Validity Checks

Because mDLs build upon existing infrastructure for issuing and managing physical IDs, an mDL's legal validity period can never exceed that of its physical counterpart. However, the technical validity of the mDL, specifically the validity of its Mobile Security Object (MSO), does not need to mirror the multi-year expiration of a physical card. In fact, for security purposes, it is highly desirable to issue MSOs with significantly shorter validity periods, such as weeks or months. This limits the potential attack window if a device is compromised or lost, and it forces the device to regularly sync with the issuing authority's backend. This approach is practical because the mDL's MSO can be refreshed or revoked quickly and remotely, without the need for the mDL holder to visit a physical facility.

> **Definition: Mobile Security Object** - a cryptographically signed data structure defined in ISO/IEC 18013-5 and created by the issuing authority during mDL issuance. It contains identity and credential attributes that can be cryptographically verified by a verifier or relying party.

As specified in ISO/IEC 18013-5, the validity period of an MSO can be found in the *validUntil* field of the credential. Additionally, ISO/IEC 18013-5 allows for relying parties to check the validity of an mDL using a privacy-preserving status list. The draft IETF Token Status List specification defines a mechanism where an issuer provides a status list token on an accessible endpoint. This endpoint can be queried by the relying party during mDL presentation and provides the RP with information about the status of a credential, including its validity. Each status list contains status information about many different tokens or credentials. Thus, when the RP queries the endpoint to pull down the list, the issuer does not know the specific credential for which the RP is requesting a status update. This feature is referred to as a "herd privacy" protection. Section 12 of the Token Status List specification details privacy considerations

and implementation recommendations. The privacy properties of this method can be further enhanced by using the protocols-defined approaches for third party hosting of status lists—that do not have access to identifying information for users—to create further separation between the issuer and the verifier.

> ⚠ **Caution:** Any architecture that requires a verifier to connect back to the issuer each time an mDL or VDC is presented has potential privacy implications and could allow the issuer to track the use of a credential holder. The Token Status List specification mentioned earlier requires specific privacy preserving controls to mitigate this risk–implementing these correctly is essential to achieving appropriate privacy outcomes if issuers and verifiers choose to use this specification for validity checks. Issuers, verifiers, and relying parties should conduct a privacy risk assessment when implementing protocols that allow for credential validity checks.

5.2.2.3 mDL Freshness

The "freshness" of an mDL generally refers to the time and frequency with which an issuer updates the MSO or to the time that has elapsed since the credential was confirmed to be valid. Credential freshness can be used as a security signal by relying parties when determining if a credential should be accepted and/or if additional security controls need to be triggered to accept the credential. Freshness can be derived from multiple values and sources:

Freshness of locally cached certificates - A common privacy-preserving option for verifying an mDL is for a verifier to cache a known valid list of mDL public certificates that are signed by an issuer or trust service. This model is often referred to as a Verified Issuer Certificate Authority List (VICAL). The VICAL is a cryptographically signed, centralized registry of authorized Issuing Authority Certificate Authorities (IACAs), that act as the trust anchor for mDLs verification. Relying parties can periodically pull down and cache the VICAL, allowing an mDL to be cryptographically verified without the need to reach back to the issuer to “phone home”. ISO/IEC 18013-5 calls for VICALs to include the *date* and *nextUpdate* fields which detail the time when the latest VICAL was issued and when the next VICAL update will occur. Because each VICAL update contains the latest set of valid public keys needed to verify an mDL, relying parties can use these fields as an element of credential freshness.

Freshness values in the credential and presentation protocol - Each time an issuer issues or updates an mDL, the *validFrom* field in the MSO is updated to reflect the timestamp of the moment the credential is valid and active. Relying parties can also leverage the *expectedUpdate* field in the MSO which indicates when the issuer expects to push a credential refresh. Additionally, relying parties might use “presentation freshness” through the *Issued At (iat)* claim required by the OpenID4VC HAIP 1.0. This claim is a timestamp of when the wallet generated and signed a specific presentation.

6 Privacy Considerations

Mobile driver’s licenses can help reduce privacy risks that arise during identity verification and account enrollment. However, as with any new technology, it may also introduce new or different risks for users compared to existing or previous practices. Understanding and balancing these benefits and risks is critical to deploying a system that supports an organization's privacy objectives. This section gives a

primer on the importance of privacy protections when using mDL for online services, the relationship between privacy and cybersecurity risk, and how NIST approaches privacy risk assessment.

6.1 Privacy Overview

Consumers spend a significant portion of their lives online. The way organizations manage data throughout their life cycle, known as data processing, can result in privacy issues for individuals, which in turn can impact the organization. Privacy risks can evolve in response to changes in technology and associated data processing. Recognizing the evolving impact of technology on individual privacy, governments around the world are working to address their concerns through new or updated laws and regulations. However, changes in law and regulation may not keep pace with technological advancements, and even when they do, they often maintain an inherent flexibility that cannot anticipate every risk. Organizations need to develop strong privacy risk management capabilities as a result.

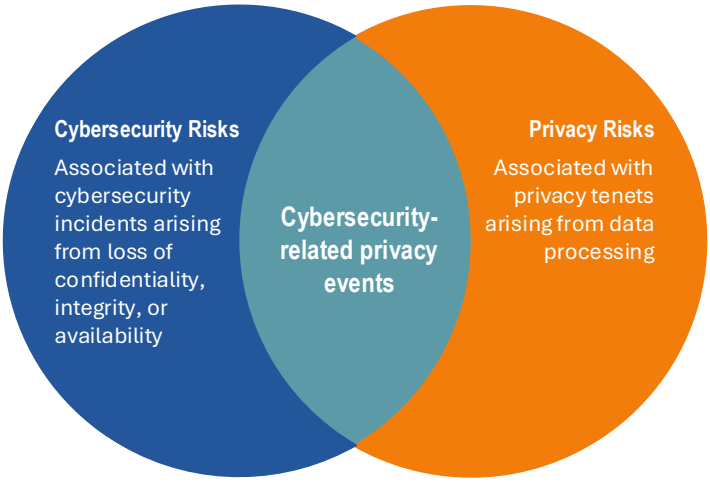
Recognizing this evolution of privacy, NIST has published content to help organizations assess and manage privacy risks, including the following:

- **Overall framework for a privacy program:** Following an open and transparent development process, NIST published the *NIST Privacy Framework* to help organizations better identify and manage their privacy risks, build trust with customers and partners, and meet their compliance obligations. Its Core provides privacy outcomes that organizations may wish to achieve as part of a privacy risk management program.
- **Tool for assessing privacy risk:** NIST provides a set of worksheets to help organizations analyze, assess, and prioritize privacy risks to determine how to respond and select appropriate solutions—called the *NIST Privacy Risk Assessment Methodology (PRAM)*.
- **Controls to manage identified risks:** *NIST Special Publication 800-53, revision 5*, *Security and Privacy Controls for Information Systems and Organizations*, offers a comprehensive set of controls that organizations can use to manage privacy risks.

These frameworks and tools also outline privacy engineering objectives that can help organizations prioritize their privacy risk management activities. These objectives are:

- **Predictability:** Enabling reliable assumptions by individuals, owners, and operators about data and how a system processes it.
- **Manageability:** Providing the capability for granular administration of data, including collection, alteration, deletion, and selective disclosure.
- **Disassociability:** Enabling the processing of data or events without association to individuals or devices beyond the operational requirements of the system.

It is important for individuals and organizations to understand the relationship between cybersecurity and privacy. As noted in the *NIST Privacy Framework*, having a general understanding of the different origins of cybersecurity and privacy risks is important for determining the most effective solutions to address the risks. Figure 6 illustrates this relationship, showing that some privacy risks stem from cybersecurity risks, while others are unrelated to cybersecurity risks.



650 **Figure 6. Cybersecurity and privacy risk relationship**

651 Though a cybersecurity incident may lead to privacy problems for individuals, it is important to note that
652 privacy risks can arise without a cybersecurity incident. For example, an organization might process data
653 in ways that violate an individual's privacy without the confidentiality, integrity, or availability of that
654 data having been compromised. This type of issue can occur under a variety of scenarios, such as when:
655 1) data is stored for extended periods, beyond the need for which the information was initially collected,
656 or 2) data is aggregated to track users' habits in a way that they would not expect.

657 Privacy risks arise from privacy events: the occurrence or potential occurrence of problematic data
658 actions.

> **Definition: Problematic Data Actions -** data actions that may have an adverse effect on individuals.

659 Problematic data actions might arise by data processing simply for mission or business purposes. Privacy
660 risk is the likelihood that individuals will experience problems resulting from data processing, and the
661 impact should these problems occur. As reflected in the overlap of Figure 6, analyzing these risks in
662 parallel with cybersecurity risks can help organizations understand the full consequences of data
663 processing within their system. Section 6.2 describes scenarios in which privacy problems may arise and
664 potential mitigations for those problems.

665 Review additional privacy guidelines and resources at NIST's privacy homepage.

666 6.2 Privacy in the mDL Architecture

667 Managing privacy risk is essential to protecting individuals and organizations and a key consideration for
668 deciding to accept mDLs. Emerging identity verification technology should seek to improve the current
669 state of privacy and provide users with greater protection. Mobile Driver's Licenses (mDL) and other
670 Verifiable Digital Credentials provide opportunities to improve not only security, but also privacy.
671 Through the selective disclosure of attributes, improved user control of credentials, the reduction of

672 calls to third party services to validate user data, and the potential for future use of zero-knowledge
673 proofs, mDLs can pave the way for a more privacy-preserving ecosystem.

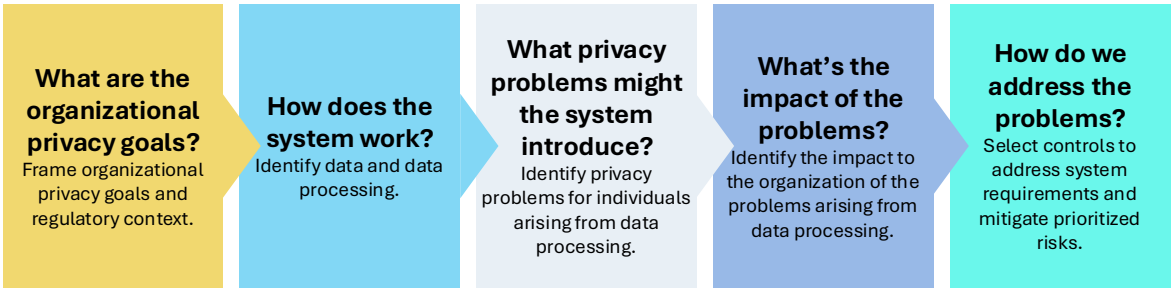
674 mDLs present privacy benefits for both in-person and online identity verification flows that are not
675 possible with traditional physical IDs. Table 3 illustrates a few of the benefits mDLs may introduce.

676 **Table 3. mDL privacy benefits**

Privacy Benefits	Description
User Control and Selective Disclosure	The mDL holder discloses only a subset of attributes needed to complete a transaction or engage a service — a level of granular data control which is unique to the mobile Driver's License.
Notice and Transparency	Customers are provided with easy-to-understand customer interfaces to enable informed decision-making about sharing their personal information.
Data Integrity & Accuracy	Customer data is presented, stored, and transmitted in a way that incorporates strong security. Enabling confidentiality, integrity, and availability of data facilitates controls that double as privacy protections for customer data, such as access control, encryption, and retention/deletion.
Local Biometric Verification	Customers can make use of local biometric capabilities, removing the need for centralized server-side biometric comparison and limiting the amount of biometric data regularly transmitted to support account onboarding.

677 Another benefit of mDLs is the ability to enable future-looking, privacy-preserving technologies; for
678 example, mDLs can support zero-knowledge proofs and other cryptographic techniques for uses such as
679 age verification. As with many technologies, the ability to realize the privacy benefits of mDLs greatly
680 depends on the design and technical implementation decisions. When implementing mDL technology,
681 relying parties should conduct a privacy risk assessment to identify, assess, prioritize, and manage
682 privacy risks tailored to their specific organization, implementation architecture, and business processes.
683 NIST's Privacy Risk Assessment Methodology (PRAM) provides an approach that can be applied to
684 manage risk consistently across the organization and technology implementations.

685 The PRAM helps organizations tackle five major questions. These questions are listed in Figure 7:



686 **Figure 7. Five privacy questions**

687 As part of the financial sector use case, the NCCoE applied the PRAM to assess the privacy risk of using
688 an mDL to establish a financial account through online remote identity proofing. The NCCoE developed

representative responses of how a Financial Institution may complete this assessment. The assessment can be found on the project resource hub.

Given the impact privacy problems can have on individuals and ultimately on financial institutions, it is crucial to complete a thorough privacy assessment. This enables relying parties to identify, within a given environment, the problems that could arise for individuals, assess the likelihood and impact of those problems, and implement controls for risk management. With a thoughtful approach such as this, the privacy benefits of mDLs can be realized while minimizing the risk to individuals and organizations.

7 Usability Considerations & Evaluation Summary

7.1 User Experience and Usability

mDLs offer several capabilities that can improve identity verification and reduce fraud, but to realize these benefits, it's essential to consider user experience. Relying parties collaborating on this project made it clear that any user friction added to the identity proofing process could lead to application or service abandonment and lower customer conversion rates. There are various usability techniques including but not limited to: A/B testing, card sorting, cognitive walkthroughs, contextual inquiry, expert review, focus group, heuristic evaluation, usability testing, user interviews, and user surveys. These different techniques can be applied at various stages of a product's lifecycle. Under use case 1, the NCCoE conducted usability testing of mDLs integrated with a fictitious banking application to identify usability issues, understand user behavior, and gather feedback on the application's functionality and overall UX.



Tip: Previous research indicates that as few as five participants can identify around 80% of usability problems, while 10 to 15 participants can identify 95–97%. Usability evaluations do not need to be resource intensive. Conducting them early in the development life cycle can be a cost-effective way to avoid expensive rework after deployment. For this project's usability evaluation, the team recruited 12 NIST staff, none of whom were involved in the NCCoE mDL project.

Usability evaluation, also known as user testing, involves systematic observation under controlled conditions to determine how easy or difficult it is for people to use something for its intended purpose. A typical usability evaluation consists of recruiting participants who match the target user population and asking them to perform a series of tasks using the product or system being tested. The tasks are designed to be representative of real-world scenarios and are often accompanied by pre- and post-task questionnaires to gather additional feedback. During the evaluation, observers (or moderators) watch and take notes on the participants' interactions, paying attention to any difficulties or frustrations they encounter. Other test instruments, such as data logging tools, may also be used to collect performance data, including metrics such as task completion rates, time on task, and error rates. The essential elements of a usability evaluation include a clear understanding of the target user population, a well-defined set of tasks and scenarios, and a systematic approach to data collection and analysis. By conducting usability evaluations rigorously and in a controlled manner, it is possible to identify usability issues, understand user behavior, and gather feedback that can inform design improvements. Usability evaluation should be conducted by trained usability professionals, who will be referred to as the Test Moderator (shortened as *Moderator*) in the remainder of this document.



Definition: Usability – As defined in ISO 9241-11, "the extent to which a system, product, or service enables specified users to achieve specified goals with *effectiveness*, *efficiency*, and *satisfaction* in a specified context of use." [17]

723 This evaluation employed a range of metrics and measures to assess the usability of the build, as listed
724 in Table 4.

725 **Table 4. Metrics and measures of usability evaluation**

Usability Metrics	Measures	Description	Data Source
Effectiveness	Task completion	Whether or not the user completes the task intended	*Moderator*
	Errors	User events that do not cause an expected outcome (not including technical issues encountered)	*Moderator*
	Assist	Occurrence(s) when the user needs help to complete the task intended	*Moderator*
Efficiency	Time on Sub-Task	Time spent performing a sub-task	Video recordings *Moderator*
	Time on Task	Time spent performing a task	Video recordings *Moderator*
Effectiveness Efficiency	Verbal	User's verbal interactions with *Test Admin* during the session	Video recordings *Moderator*
	Nonverbal	User's nonverbal information (such as facial expressions, body language) observed by *Test Admin* during the session	Video recordings *Moderator*
Satisfaction	Pre-session	Questionnaire answered by the user before using the system to understand user's background information	Pre-session questionnaire
	Post-task	Questions include: • Ease of Use • Task and Content Specific Questions • Perception of Outcomes/Interactions	Post-task questionnaire *Moderator*
User Experience	Verbal	User feedback during the think-aloud session and debriefing with the *Moderator*	Video recordings *Moderator*

726 ## 7.2 Usability Best Practices

727 This section provides a summary of best practices identified through the project's usability evaluation.
728 These practices reflect patterns observed across participant performance, satisfaction, and feedback.
729 Information describing the study design, participant demographics, tasks, and data-collection
730 methodology is available on the project website.

7.2.1 Preserve the positive characteristics of mDL-based verification

The evaluation demonstrated that users consistently perceived mDL verification as fast, straightforward, and more secure than traditional document-upload approaches. These characteristics contributed substantially to successful task completion and user satisfaction. Implementers should ensure that mDL workflows maintain low friction; present clear, minimal consent steps; and operate reliably across devices. Preserving these characteristics helps reinforce user trust in digital credentials and supports broader adoption.

7.2.2 Improve QRC scanning reliability and predictability

Participants encountered difficulties when QRCs expired before they could complete actions on the mobile device. In several instances, expiration resulted in displaying a new QRC that differed in appearance and content, causing confusion about whether the original task had restarted. To minimize user disruption, implementers should adopt measures such as extending QRC validity periods, maintaining consistent QRC formatting during presentation, and providing clear guidance regarding expected timing. These improvements support predictable user flows and reduce the likelihood of task abandonment or error.

7.2.3 Standardize terminology across presentment flows and attribute displays

Differences in terminology across wallet implementations created unnecessary cognitive burden for users. Phrases used to describe similar actions (e.g., unlocking the device or authorizing data release) varied significantly, leading participants to guess the intended meaning in some cases. Additionally, certain attribute labels within mDL data were unclear or not aligned with common user understanding. Implementers should employ consistent terminology across all steps of the verification process and use plain language for attribute labels and consent prompts. Standardization enhances comprehensibility, reduces ambiguity, and supports more intuitive decision-making by users.

7.2.4 Ensure consistent and predictable user-interface behaviors

Participants noted that user-interface elements did not always behave consistently. For example, some fields automatically advanced after data entry, while others required users to select a “Continue” button. Inconsistent behaviors made it difficult for users to anticipate what would occur after each action. Implementers should adopt consistent patterns for page progression, provide clear and timely system feedback, and ensure that completion actions (e.g., “Finish,” “Submit,” or “Exit”) accurately represent the state of the transaction. Predictable, uniform interactions reduce user confusion and improve overall usability.

7.2.5 Provide explanatory text and visual cues to support user understanding

The evaluation indicated that users benefited from supplemental explanations when interacting with unfamiliar concepts, such as digital credential presentment or authentication method selection (e.g., Passkeys). Users expressed uncertainty about the purpose of certain steps and the distinctions between available authentication options. Implementers should incorporate concise explanatory text specific to the action requested, visual aids, and contextual guidance to help users understand the purpose and

768 expected outcomes of each action. Supporting information should avoid technical jargon and align with
769 users' mental models. This practice enhances clarity and supports informed decision-making.

770 7.2.6 Consider factors and potential barriers to adoption

771 Participants identified several factors that may impact mDL adoption across different populations. These
772 include concerns about privacy, data security, trust in the requesting party, and comfort with mobile
773 devices. Some users, particularly those with limited technical experience, may also experience physical
774 or cognitive challenges when scanning QRCs or completing multi-step mobile flows. Implementers
775 should consider alternative interaction methods, provide clear privacy and security explanations, and
776 support accessibility needs.

777 7.2.7 Evaluate and plan for additional, user-driven use cases

778 Participants identified several potential future use cases for mDLs, including remote identity verification
779 for online banking, travel, school enrollment, and applications for government services. Users also
780 identified scenarios where physical IDs may remain preferable, particularly when interacting with
781 officials who may need temporary control of an identification document. Implementers should consider
782 these perspectives when designing or deploying mDL solutions, ensuring that systems support contexts
783 most aligned with user expectations and trust. Incorporating user-identified use cases can strengthen
784 system relevance and encourage sustained adoption.

Appendix A References

[1] World Wide Web Consortium (2021). Web Authentication: An API for accessing Public Key Credentials Level 2. Available at https://www.w3.org/TR/webauthn-2/

[2] FIDO Alliance (2025). Client to Authenticator Protocol (CTAP). Available at https://fidoalliance.org/specs/fido-v2.2-ps-20250714/fido-client-to-authenticator-protocol-v2.2-ps-20250714.pdf

[3] International Organization for Standardization (2021). Personal identification — ISO-compliant driving licence Part 5: Mobile driving licence (mDL) application. Available at https://www.iso.org/standard/69084.html

[4] International Organization for Standardization (2021). Personal identification — ISO-compliant driving licence Part 7: Mobile driving licence (mDL) add-on functions. Available at https://www.iso.org/standard/91154.html

[5] World Wide Web Consortium (2025). Verifiable Credentials Data Model v2.0 W3C Recommendation. Available at https://www.w3.org/TR/vc-data-model-2.0/

[6] OpenID Foundation (2025). OpenID for Verifiable Presentations 1.0. https://openid.net/specs/openid-4-verifiable-presentations-1_0.html

[7] OpenID Foundation (2025). OpenID for Verifiable Credential Issuance 1.0. https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html

[8] Customer identification program requirements for banks (2026) 31 CFR 1020.220. https://www.ecfr.gov/current/title-31/subtitle-B/chapter-X/part-1020/subpart-B/section-1020.220

[9] Financial Crimes Enforcement Network (2024). FinCEN Issues Analysis of Identity-Related Suspicious Activity. Available at https://www.fincen.gov/news/news-releases/fincen-issues-analysis-identity-related-suspicious-activity

[10] Text - H.R.7270 - 119th Congress (2025-2026): Stop Identity Fraud and Identity Theft Act of 2026." Congress.gov, Library of Congress, 27 January 2026, https://www.congress.gov/bill/119th-congress/house-bill/7270/text

[11] PYMNTS Intelligence (accessed 2026). The $95B Wake-Up Call: 'Good Enough' Digital Identity Is Costing Firms Growth. Available at https://www.pymnts.com/cybersecurity/2025/the-95b-wake-up-call-good-enough-digital-identity-is-costing-firms-growth/

[12] Financial Services Sector Coordinating Council (2026). Mitigating AI-Powered Attacks Against Identity and Authentication. Available at https://fsscc.org/wp-content/uploads/2026/02/AI-IA-Workstream-Mitigations.pdf

[13] The Department of the Treasury (2026). Report to Congress from the Secretary of the Treasury on Innovative Technologies to Counter Illicit Finance Involving Digital Assets. https://home.treasury.gov/system/files/246/GENIUS-Act-Illicit-Finance-Innovation-Congressional-Report-March-2026.pdf

[14] MATTR Global (accessed 2026). MATTR Verifier Web SDK - v2.1.0. Available at https://api-reference-sdk.mattr.global/verifier-sdk-web/latest/index.html#md:generate-challenge

[15] Bank Secrecy Act (2012) 31 CFR 1020.100. https://www.ecfr.gov/current/title-31/subtitle-B/chapter-X/part-1020?toc=1

[16] Federal Financial Institutions Examination Council (accessed 2026). Appendix P: BSA Record Retention Requirements. https://bsaaml.ffiec.gov/manual/Appendices/17
[17] ISO 9241-11:2018 Ergonomics of human-system interaction — Part 11: Usability: Definitions and concepts, https://www.iso.org/standard/63500.html

Appendix B List of Available Online Resources

This appendix provides a comprehensive list of resources related to this project that are available on the NIST resource hub.

Resource Name	Location
Project Blog Series	https://pages.nist.gov/nccoe-mdl-project-static-website/blogs.html
Project Event Recordings	https://pages.nist.gov/nccoe-mdl-project-static-website/events.html
Building Assurance in the mDL Ecosystem	https://pages.nist.gov/nccoe-mdl-project-static-website/use-case-1/building-mdl-assurance/index.html
NIST SP 800-63A Profile for mDL Issuance	https://pages.nist.gov/nccoe-mdl-project-static-website/use-case-1/building-mdl-assurance/nist_800-63a.html
Privacy Risk Assessment Methodology	https://pages.nist.gov/nccoe-mdl-project-static-website/use-case-1/pram.html
Usability Assessment	https://pages.nist.gov/nccoe-mdl-project-static-website/use-case-1/usability-results.html

Appendix C List of Symbols, Abbreviations, and Acronyms

API
Application Programming Interface

BSA
Bank Secrecy Act

CBOR
Concise Binary Object Representation

CFR
Code of Federal Regulations

CIP
Customer Identification Program

CRADA
Cooperative Research and Development Agreement

CRQC
Cryptanalytically-relevant quantum computer

CTAP
Client-to-Authenticator Protocol

DC API
Digital Credentials Web Platform API

DHS
Department of Homeland Security

DMV
Department of Motor Vehicles

FI
Financial Institution

FIDO
Fast Identity Online

FS-ISAC
Financial Services - Information Sharing and Analysis Center

HAIP
High Assurance Interoperability Profile

HPKE
Hybrid Public Key Encryption

HSM
Hardware Security Module

HTTPS
Hypertext Transfer Protocol Secure

IACA
Issuing Authority Certificate Authorities

IDMS
Identity Management System

IR
Interagency Report or Internal Report

ISO
International Organization for Standardization

JSON
JavaScript Object Notation

JWT
JSON Web Token

KYC
Know Your Customer

KBV
Knowledge-Based Verification

mDL
Mobile Driver's License

mDoc
Mobile Document

OIDC
OpenID Connect

OIDF
OpenID Foundation

OpenID4VCI
OpenID for Verifiable Credential Issuance

OpenID4VP
OpenID for Verifiable Presentations

PII
Personally Identifiable Information

PKCE
Proof Key for Code Exchange

POC
Point of Contact

PQC
Post quantum cryptography

PRAM
NIST Privacy Risk Assessment Methodology

QRC
Quick Response Code

REST
Representational State Transfer

RP
Relying Party

SaaS
Software as a Service

SI
Super Intelligence

SP
Special Publication

SSO
Single Sign-On

TLS
Transport Layer Security

TLS
Transport Layer Security

TPM
Trusted Platform Module

TSA
Transportation Security Administration

VC/VDC
Verifiable Digital Credential