NIST SPECIAL PUBLICATION 1800-42A

Digital Identities—Mobile Driver's License (mDL)

Accelerating Development and Adoption of Digital Identity for Financial Institutions

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

MARCH 2026

INITIAL PUBLIC DRAFT

NIST NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

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.

National Institute of Standards and Technology Special Publication 1800-42A, Natl. Inst. Stand. Technol. Spec. Publ. 1800-42A, 100 pages, (March 2026), CODEN: NSPUE2

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

You can improve this guide by contributing feedback. As an initial public draft, this document intends to gain critical feedback from stakeholders across government and industry on the implementation of mDL to support Customer Identification Programs and high assurance use cases more broadly. Comments are welcome on all aspects of this document and specifically encouraged on the following areas:

1. **Implementation and Adoption Challenges**. This document highlights challenges to the adoption of mDL technology learned through engagement with collaborators and stakeholders spanning technology providers, financial institutions, standards bodies and government agencies. However, additional insights on barriers to adoption can help focus the project and future phases of work and NIST's engagement with standards development organizations.
2. **Regulatory and Compliance Alignment**. This document offers insights into the ways in which mDL online presentation aligns with existing regulatory structures. Additional insights on other regulatory mappings, views on the degree to which alignment is achieved, and suggested clarifications are encouraged.
3. **Technology Transfer and Resources**. This document as well as supporting resources are intended to aid in implementation of the technology in real world environments. The project team is highly interested in additional resources and tools which may further aide in both technical implementation and broader adoption of the technology.

4. **Threats and Threat Model**. The threat model proposed here is intended to act as a starting point for members of the ecosystem to identify and prepare for how attacks may shift in an mDL environment. Input on approach, specific threats, and mitigations will be highly valuable in maturing this view and providing greater visibility into future risks.

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

Comments can also be submitted on the deliverables published on our supporting resources site.

Public comment period: March 18th 2026, through May 8th 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 we use to prove identity both in-person and online. Many sectors stand to benefit from this emerging technology, including financial institutions seeking to enhance the security, privacy, usability, and reliability of online identity services. This practice guide captures insights generated through engagement with a robust cohort of industry collaborators and the lessons learned by developing a functional online mDL demonstration to provide a practical roadmap to enable adoption and implementation of mDLs for online financial account management.

KEYWORDS

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

ACKNOWLEDGMENTS

We are grateful to all the collaborators who donated their time and expertise to make this project a reality. See Section 4.1 for complete list of collaborators who participated in this project. We would also like to acknowledge the following individuals for their time and effort working with the NCCoE team to build out our demonstration lab environment.

Name	Organization
Tim Roufa	AAMVA
Oliver Terbu	MATTR Limited
Tobias Looker	MATTR Limited
Avner Matan	MATTR Limited
Ralf Engbers	MATTR Limited
Muthuramakrishnan Viswanathan	Google
Jacob Healy	SpruceID
Libby Brown	SpruceID
Gail Hodges	OpenID Foundation
Ajay Gupta	California Department of Motor Vehicles
Jas Suri	Microsoft Corporation
Rohit Gulati	Microsoft Corporation
Juliana Cafik	Microsoft Corporation[1], OpenID Foundation
Joseph Irudayasamy	Maryland Department of Transportation
Negash Assefa	Maryland Department of Transportation
Bharat Deolekar	Maryland Department of Transportation[1]

[1] Former employee: all work for this publication was done while at employer.

Name	Organization
Stefan Schubert	JP Morgan Chase
Nicholas Hazelbaker	JP Morgan Chase
Stephanie Goldner	Capital One
George Fletcher	Capital One[1]

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

List of Figures

List of Tables

1 Executive Summary

- Identity proofing is the process of establishing that a person is who they claim to be. Online identity proofing is a critical security capability that relies on verifying identity evidence to protect individuals from identity theft and organizations from unauthorized access and fraud.

- Current online identity proofing processes, such as uploading an image of a driver's license or knowledge-based verification, are not optimized for online transactions and do not sufficiently mitigate against current threats, especially those posed by generative AI (e.g., deepfakes).

- Mobile driver's licenses (mDLs), and more broadly Verifiable Digital Credentials (VDCs), are an emerging technology that, when implemented using standards and best practices, can help mitigate current threats to identity proofing systems, while also offering potential benefits in user experience and privacy.

- High assurance relying parties, such as Financial Institutions (FIs), represent high value targets for identity-related fraud and are considering the adoption of mDLs to support Know Your Customer (KYC) processes. To move forward, however, FIs need a better understanding of how this technology integrates with their current identity systems and business processes, as well as insights into how mDLs meet Customer Identification Program (CIP) compliance requirements and the identity proofing component of KYC.

- To help address these needs, the National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) created this practice guide as part of a portfolio of resources to help FIs implement mDL standards and best practices using commercially available technology and realize the security, privacy, usability, reliability, and compliance benefits that can result from an FI mDL deployment.

- FIs can use the tools and resources in this guide to assess the feasibility of integrating mDLs with their current technology and business processes while aligning to compliance requirements.

- To build this portfolio of resources, the NCCoE collaborated with technology providers, government agencies, standards bodies from across the mDL ecosystem, and the financial sector to build a laboratory environment that demonstrates a standards-based mDL architecture that integrates with financial institution identity systems and banking back ends.

- This architecture uses existing standards and commercial off the shelf technologies to demonstrate 1) the presentation of mDLs for online transactions as identity proofing evidence when a potential customer applies to open a financial account, 2) the provisioning and issuance of a phishing-resistant authenticator to applicants whose financial account is approved, and 3) the presentation of mDLs by financial institution customers as an additional security signal (often referred to as a step-up) when authorizing high-risk transactions.

- This practice guide is complemented by the resources that are published on the mDL project supporting resources website, to include a video demonstration of mDL implementation built in the NCCoE lab environment.

1.1 Key Findings

Throughout the project and collaborator engagement, the project team learned several critical lessons, including insights into the technology, the state of the ecosystem, and the strategic direction of VDC and mDL. These findings include:

1. **FIs Should Begin Assessing VDC and mDL Technology Adoption Early**. mDLs are currently in the hands of millions of Americans and have the potential to improve online Customer Identification Programs. While standards and ecosystem practices continue to mature (see takeaways below), the assessment of integrating mDL adoption in high-assurance and regulated industries is a multi-year effort. Institutions that begin market research, proofs of concept, and pilots now will be better positioned to onboard mDL verification and realize the technology's potential benefits. The portfolio of resources published under this project can assist FIs in initiating their mDL journey.
2. **VDCs and mDLs Can Improve Security, Privacy, Reliability, and Usability of Online CIP**. mDLs present an opportunity to improve upon current CIP practices by providing accurate, integrity-protected information delivered through phishing-resistant mechanisms, with selective disclosure, and support for more efficient customer onboarding. This project focused on the benefits of mDL integration for account opening and high-risk transaction authorizations and highlights how mDLs can advance security, privacy, reliability and usability of online identity proofing.
3. **The VDC and mDL Trust Ecosystem Still Has Work to Do.** Our FI collaborators see the value in this technology. However, the adoption of this technology hinges on the ecosystem understanding the needs and concerns of high-assurance and regulated sectors. Notably, shifting FIs to a new trust model will require a more consistent issuance process across states and territories, standardized holder verification techniques, enhancements to credential protocols to support access requirements, and trust establishment in the wallet as a key component of transactions.
4. **The Standards Ecosystem Needs to Focus on Stabilization and Consolidation.** Standards Development Organizations (SDOs) have laid the essential technical foundation for the mDL ecosystem. However, as the market shifts from pilot to commercial deployment, the focus must turn to finalizing critical standards and consolidating specifications to ensure scalability. This is particularly urgent for presentation protocols, where fragmentation currently complicates implementations for verifiers and Relying Parties (RPs). The ecosystem must prioritize aligning core specifications with RP requirements and progress towards operational stability.

2 Introduction to the Guide

This publication provides guidelines for organizations seeking to implement 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 NCCoE that developed, demonstrated, and documented an example mDL use case for Financial Institutions (FIs) such as banks. The NCCoE and its collaborators have used commercially available technology in lab environments to build a functional, interoperable, standards-based mDL implementation ("build"). While this guide contains information useful to any organization seeking to accept the online presentation of mDLs, the focus of the recommendations, considerations and resources in this document are to support financial institutions in accepting mDLs for online identity proofing and meeting CIP requirements.

2.1 Scope

The scope of this guide 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 supporting Customer Identity Program implementation and reducing potential fraud vectors introduced by more traditional identity management technologies. It provides guidelines on the online presentation of mDL in support of identity proofing and high-risk transaction verification. User authentication is addressed through the deployment of Passkeys (i.e., WebAuthN/FIDO2 credentials [1][2]).

Note that this build 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 as a result 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, and this document describes only the first phase, which focuses on an FI use case. The next use case will address the use of mDLs in a government or public sector use case.

2.2 Audience

The audience for this guide is anyone looking to implement mDLs, as well as any person or organization that engages with or relies upon mDL, 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, IDMS)
- Standards bodies and regulators
- Cybersecurity, Privacy, risk, and compliance professionals
- General Members of the public interested in digital identity

2.3 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 – Our blog series provides a high-level introduction to VDCs, mDLs, and the concepts, technologies, and standards that underpin the ecosystem.
2. The NIST mDL Supporting Resources website – Our supporting resources site is how we iteratively release 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 – This 1800-42 practice guide highlights and integrates information from our blog series and our supporting resources site, and adds detailed information about our mDL reference architecture, 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.

This report uses callout boxes to highlight certain types of information, as depicted in Figure 1. With the exception of **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.

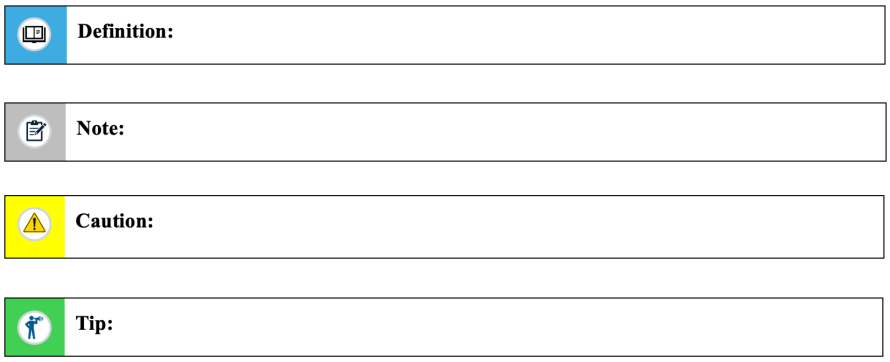


Figure 1. Callout Box

3 Project Overview

The Mobile Driver's License (mDL) project at the National Institute of Standards and Technology (NIST) is a collaborative, standards-driven initiative implemented by the National Cybersecurity Center of Excellence (NCCoE) to demonstrate secure, interoperable, and privacy-preserving digital identity approaches based on Verifiable Digital Credential (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 ISO 18013-5/7 [3][4], W3C Verifiable Credentials [5], the Digital Credentials Web Platform API [1], OpenID for Verifiable Presentations [6], and OpenID for Verifiable Credential Issuance [7].

This document is the result of our first use case—deploying mDLs at financial institutions to support identity proofing and Customer Identification Program (CIP) requirements [8].

> **Note:** This project specifically explores how financial institutions could accept mDLs to collect only necessary user attributes required by CIP. This effort does not address broader KYC requirements such as transaction monitoring, fraud and sanctions checks, enhanced customer due diligence or reporting requirements.

3.1 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.

Through its collaboration across the mDL ecosystem and the publication of this practice guide and other online resources, the NCCoE hopes to accelerate the adoption of standards-based mDL solutions to help realize the benefits this technology offers.

3.2 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 AI 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.

3.3 Financial Institutions and High Assurance Use Cases

Financial institutions, who have direct access to money and sensitive personal information, are subject to emerging cyber threats. Attackers seeking to drain bank accounts, open fraudulent lines of credit, launder money or steal PII, may target financial institution identity proofing systems. These threats directly impact bottom lines: The Financial Crimes Enforcement Network (FINCEN) linked $212 Billion dollars [9] to identity related suspicious activity in 2021, a figure that reached as much as $394 billion by 2023 [10]. Furthermore, inadequate digital identity systems cost institutions an estimated 3.1% of annual revenue [11].

The industry also operates under regulations, such as the CIP Rule, which requires institutions to maintain a "reasonable belief" in a customer's identity. This combination of high-risk and regulatory oversight makes the financial sector a "high assurance" use case. Consequently, the NCCoE chose the financial sector for its initial mDL project for two reasons:

- **High-Impact:** To accelerate mDL adoption in a sector where risk mitigation has the greatest economic impact.
- **Scalability:** Solving for the most stringent requirements gives confidence that the solution can translate to other sectors with equal or lower assurance needs.

Ultimately, by addressing the rigorous demands of the financial sector, the NCCoE hopes to establish a blueprint for mDLs that can be scaled across all sectors of the economy.

3.4 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[2] 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 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 the time spent on data entry and 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.
- 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.

For financial institutions, mDLs are another tool in the toolbox that can meet or exceed current identity proofing systems. In a recent white paper, the American Banking Association, Better Identity Coalition, and Financial Sector Services Coordinating Council call out mDLs as a key mitigation to AI-powered attacks against identity systems stating that "Government-issued verifiable credentials, such as mDLs, can play a crucial role in reducing the risk of deepfake attacks. If available, they can be used to cryptographically assert an identity," [12]. Additionally, The Secretary of Treasury also offered support for mDLs saying that "[t]hese types of verifiable credentials represent innovative means for financial institutions […] to conduct customer identification and verification while minimizing the amount of sensitive data collected," and that, "Treasury will issue guidance to financial institutions on how they can utilize verifiable digital credentials consistent with their existing customer identification programs," [13].

[2] Review Appendix D for a detailed comparative analysis composed of security, privacy, and usability considerations.

3.5 Financial Institution Adoption Challenges

As mDLs and VDCs gain traction, financial institutions stand to benefit significantly. Yet, the path to adoption is hindered by a persistent market maturity challenge: the classic “chicken-and-egg” dilemma.

Consumers are unlikely to adopt mDLs unless they are accepted in high-value, everyday use cases. Meanwhile, financial institutions are hesitant to invest in mDL integration without widespread consumer demand or adoption. This deadlock stalls the emergence of scalable, high-assurance digital identity solutions in the financial sector, despite their clear long-term value.

What limits current mDL adoption isn't the technology itself, it’s the maturity of the surrounding ecosystem. This includes a complete set of mature standards, clear governance, and interoperable tools that make it easy to verify mDLs across diverse workflows, whether at the branch, online, or through mobile apps.

Constructing this ecosystem requires deep coordination between the financial services sector, government issuers, and technology providers. Just as the industry coalesced around common protocols to scale previous digital innovations, stakeholders must now align to reduce the integration burden and provide the necessary foundation for mDLs to operate as a scalable, high-assurance identity proofing solution.

4 A Collaborative Approach

The ability to provide meaningful value towards the adoption of standards-based mDL deployments requires collaboration across the mDL ecosystem. With this in mind, the NCCoE project team formed a collaborative research and development agreement (CRADA) consortium that included technology providers, standards bodies, government agencies, state issuers, and financial institutions. The NCCoE engaged these stakeholders in an iterative process to inform the project demonstration and direction.

Engagement with our financial institution partners helped us understand their concerns (discussed in section 7.1), compliance regimes, privacy expectations, internal systems, and business processes that might impact integration of an mDLs. Engagement with standards bodies informed the profiles and best practices in our implementation and enabled the NCCoE to serve as a feedback loop, providing implementation experience to advance the state of the standards. Our state partners and the American Association of Motor Vehicle Administrators (AAMVA) provided crucial context from the issuer's perspective, including wallet support decision-making process, trust frameworks, and accessibility/user experience concerns. Technology providers in the mDL ecosystem, such as digital wallets, verifiers, and identity management systems, provided subject matter expertise on current state of mDL components and how to design an architecture that would meet the needs of financial institutions.

The output of these discussions and working sessions resulted in the artifacts and resources on our NIST pages site, as well as this practice guide.

4.1 Project Collaborators

The NIST project team would like to acknowledge the CRADA consortium that helped us realize the mDL project. The technology collaborators who participated in this project submitted their capabilities in response to a Federal Register notice. Respondents with relevant capabilities, products, or subject matter expertise were invited to sign a CRADA with NIST, allowing them to participate in a consortium to build this example solution. We worked with:

Table 1. Project Collaborators

Organization(s) / Project Collaborator(s)	
1Password	MATTR Limited
American Association of Motor Vehicle Administrators (AAMVA)	Microsoft Corporation
California Department of Motor Vehicles	Navy Federal Credit Union
Capital One	New York State Department of Motor Vehicle

Organization(s) / Project Collaborator(s)	
Department of Homeland Security (DHS), Science and Technology Directorate	Ohio Bureau of Motor Vehicles
Georgia Department of Driver Services	Open Identity Foundation (OIDF)
Google	PNC Bank
Idemia	Raymond James
iLabs	SpruceID
JP Morgan Chase	Synchrony
Kentucky Transportation Cabinet	US Bank
Maryland Department of Transportation	Wells Fargo
	Yubico

510

5 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 our blog series.

5.1 An Overview of VDCs

At their core, VDCs are a digital representation of a credential or attribute(s) 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 TSA agent before boarding a plane or presented to a web browser online to verify identity before opening a new account.

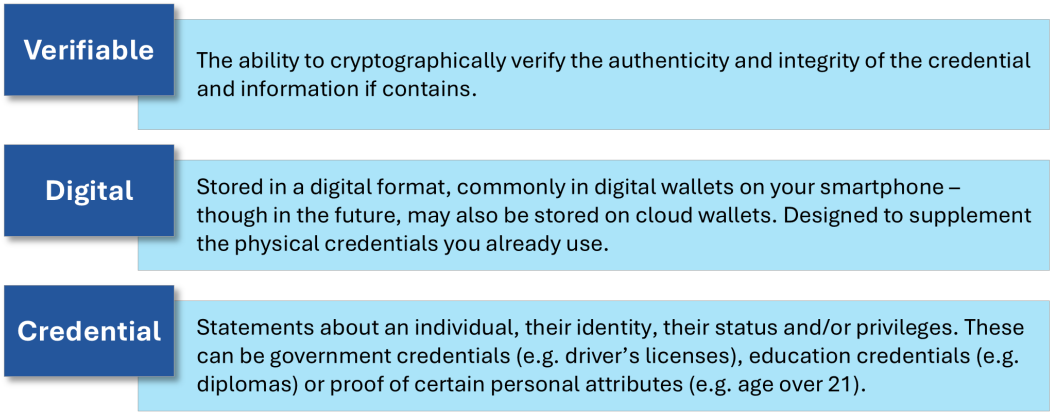


Figure 2. Verifiable Digital Credentials

5.1.1 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 (See section 5.3), 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 talking about the application storing the mDL and use the term mDL or VDC "holder" when referring to the person the mDL was issued to.

5.2 An Overview of mDLs

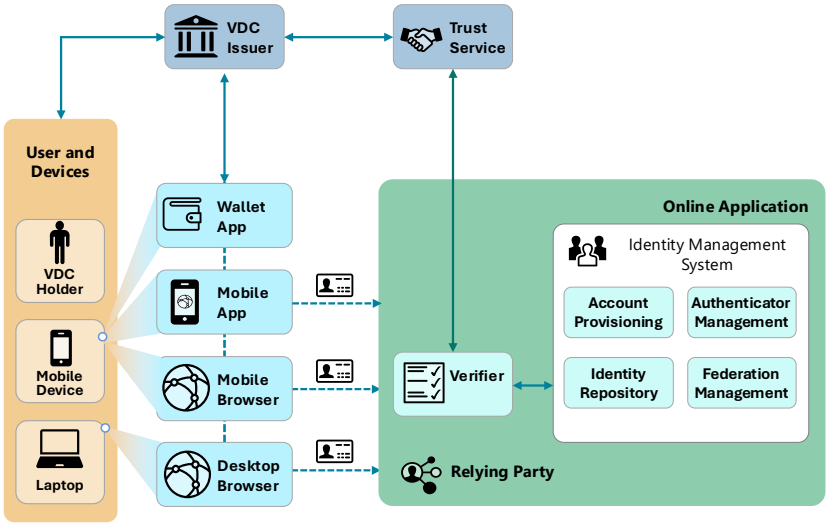
mDLs are a specific type of VDC. They are differentiated from other VDCs by three primary characteristics:

- **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 your 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.

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. The Transportation Security Administration (TSA) now accepts mDLs from certain states at checkpoints for travel. This project demonstrates how mDLs can be used in online use cases.

5.3 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 that enable their value. Figure 3 below highlights how these components might interact.



Users may present VDCs online to relying parties through a mobile application or through a browser

Figure 3. Presenting Verifiable Digital Credentials

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

- **Trust Service** – Trust services may take many forms, but in general act as an integration point that enables 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 replying 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 talk about verifiers and relying parties interchangeably. In this document, they are discussed separately to highlight the distinction between the technical functions that verifiers provide when processing a VDC and the relying party's business processes and technologies that rely on the verifier's output. This distinction can be useful, even if, in practice, the verifier may be run or reside 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.

6 Architecture & Build

This section defines the architecture and reference design developed in collaboration with our consortium. It highlights our approach to developing the architecture, including decisions and assumptions made, as well as the components, standards, and best practices used.

6.1 Defining an mDL User Journey at a Financial Institution

Before the NCCoE could build an mDL architecture, our team needed to understand the desired end state for the online presentation of an mDL at a financial institution. Through discussion with our financial institution partners and consortium members, a consensus was reached to demonstrate the following capabilities:

1. **Account Application** – Illustrate a journey from the perspective of an "applicant" who applies for a new bank account using an mDL as evidence to verify their identity in alignment with CIP requirements.
2. **Digital Enrollment** – After account approval, show a "customer" setting up online account access, using an mDL to confirm that the user accessing the account is the same user who applied for the account, and subsequently issuing the user a Passkey (or other phishing-resistant authenticator) for future authentication.
3. **High Risk Transaction Authorization** – Demonstrate a customer attempting to make a high-risk transaction who is put through mDL re-verification flow to confirm they are in possession and control of the mDL linked to their account, and provide the financial institution with an additional security signal before authorizing the transaction.

This user journey set the goalpost for our final demonstration and informed the architectural decision later to include a fictitious "NCCoE Bank" as our financial institution. It's worth noting that these capabilities can and will vary in operational implementations based on the needs of the FI and the technologies available to them.

6.2 Architecture Decisions & Assumptions

This section describes key decisions and assumptions made in collaboration with our consortium members to support our build architecture. Readers should note that while our decision path resulted in this architecture, it is only one potential implementation. Organizations in other sectors or regulatory environments may confront different decision points that shape their final architecture.

6.2.1 Centralized IDMS and Verifier

In initial discussions with our technology, SDO, and financial institution partners, there was consensus that for the financial industry to adopt strong identity proofing and authentication—to include mDL verification—they needed a plug-and-play solution that can scale across all interactions between the financial institution and the customer, referred to as consumer touchpoints. To enable this, we implemented a standards-based, centralized, scalable IDMS and verifier.

Centralized Verifier

While it is conceivable that large Financial Service providers may choose to implement multiple verifiers (typically for resilience or to potentially deal with different presentation protocols) a single central verifier integrated with the IDMS offered a pattern that limited integration complexity while supporting scaled integration across enterprise-wide services.

Centralized Identity Management System (IDMS)

Although individual applications may provide limited identity services, the build team elected to leverage a dedicated enterprise Identity Management System (IDMS) to serve as the bank's central orchestration layer. In this architecture, the IDMS coordinates the entire account opening process initiated by the mDL holder, supporting a compliant and seamless workflow. This includes managing critical regulatory steps such as capturing appropriate notice and consent, while aggregating mDL data with additional verification details (i.e., Taxpayer Identification Numbers) required to align with CIP mandates. This design empowers financial institutions to customize the orchestration logic, controlling exactly which attributes are validated in transit and which persist within the FI's backend systems to align with risk and business objectives.

By centralizing mDL verification and authentication within the IDMS, the bank requires only a single integration point, allowing all customer touchpoints to programmatically leverage this capability at scale. This replicates an enterprise service model that maximizes value across the FI's entire portfolio, consistent with industry input from our collaborators.

Integrating the verifier into this orchestration layer also allows banks to extend their existing policies, governance frameworks, logging, and auditing mechanisms to mDL data. Attributes derived from the mDL are processed consistently with other identity data subject to the same consent, attribute release, risk evaluation, and audit requirements already enforced by the IDMS. This approach prevents the creation of parallel identity silos, minimizes integration complexity, supports asynchronous mDL presentation to account activation processes and ensures that mDL adoption fits naturally into a bank's broader Customer Identity and Access Management (CIAM) strategy.

6.2.2 Use of Software as a Service (SaaS) products

As with most modern technology deployments, there are multiple patterns and architectures that can be used to achieve desired outcomes, depending on the implementing organization's risk appetite and preferences. Notably, organizations have a plethora of options available to them on where and how to deploy software. For this project, we prioritized SaaS products for several key components—notably our verifier and our IDMS. This was done for several reasons:

- Using SaaS allowed the project to rapidly integrate multiple disparate services with minimal resources. As NIST is not an operational entity and the outcome was not intended to be a long-term operational service, this approach allowed us to deliver maximum value with minimal cost and resources.
- SaaS also enabled us to make use of the expertise offered by our SaaS partners to deploy and maintain their software. IDMS and verifiers are complex software that often require substantial experience to operate effectively and troubleshoot when issues arise. This is particularly true with respect to the MATTR verifier, which is implementing standards and protocols that evolved

as the project progressed. This gave us the greatest chance for success, given we were "building the plane while flying it."

While SaaS services offer substantial benefits, they also have drawbacks. SaaS products hosted in different environments do introduce new threats by allowing attackers additional pathways into the mDL verification process. For example, communications crossing boundaries between the Verifier, IDMS, and Core Banking Service could be intercepted, forged, or replayed and used to compromise aspects of the mDL trust model. While many of these can be mitigated through common, standards-based controls, the threat of exposure is increased, and some organizations may choose alternative architectural patterns.

As mDL become operational, several viable deployment alternatives exist. Most notably the deployment of verifier, IDMS, and core banking systems in a common, Financial Services controlled infrastructure. This could be on-premises, Infrastructure-as-a-Service (IaaS), private cloud, or similar. Direct control over the infrastructure provides FIs with greater confidence and visibility into the controls and protections applied to the mDL verification functions and the data involved in the process. Additionally, such an architecture can be deployed with fewer exposures as data does not need to be communicated over the internet to components residing in different trust domains, infrastructure, or networks. During the project this was indicated as the increasingly preferred deployment pattern among FIs with the resources to deploy, operate, maintain, and troubleshoot the respective software components.

> ⚠ **Caution:** Cloud based services, such as SaaS verifiers bring many benefits but also carry risk. Organizations seeking to make use of cloud service providers should have a detailed understanding of how the cloud services are architected and carefully evaluate risk to ensure that the service fits their risk profiles and that appropriate protections are deployed by the service provider.

6.2.3 User Experience Expectations

Financial institutions devote significant resources to UX development to promote customer retention and satisfaction. Any "friction" introduced could result in outcomes such as potential customer abandonment during the account application process. Thus, our build sought to enable a seamless experience across the account application and identity proofing process. This meant providing a consistent experience and reducing confusion as the user interacted with and between the banking website and the IDMS. This also meant limiting the number of clicks, manual input fields and pop ups to only those needed to guide the user through the process and provide necessary information such as user consent. Additionally, efforts were taken to implement consistent branding, color schemes, and optimizations where possible for mobile and desktop web browsers.

6.2.4 Use of Digital Credentials API and Avoiding Custom URI Schemes

From the start of this project, the build team wanted to prioritize using the W3C Digital Credentials API (DC API). Before the existence of the DC API, application developers were left with the task of managing the wallet and credential selection mechanism between the device and the verifier. This often resulted in wallets on mobile devices being invoked by a custom Uniform Resource Identifier (URI) scheme—a mechanism that allows applications to register a unique URI prefix with the operating system. This pattern creates a problematic user experience where little information is presented to the user before the wallet is invoked. It can also result in credentials that are non-responsive to verifier requirements

being invoked and are unable to support the wallet selection if credentials are present in multiple wallets. Further, once a wallet is selected, there is a context switch that makes it difficult for users to return to the original website if the user is accessing the website from the same device as the wallet.

The DC API offers UX improvements over the custom URIs by showing the user which application is making the wallet request and displaying a consistent view of the queried credentials and attributes being requested from the credential. This enables the user to make an informed decision and proceed with presenting their mDL with increased context.

The DC API further enhances VDC request and presentation by providing more robust security than custom URI. In the custom URI flows, the QR code for wallet invocation is presented by the verifier and not through the browser. By using the DC API and integrating with platform APIs this technique allows the presentation method to make use of FIDO's Client to Authenticator Protocol [2]. This protocol enforces proximity by establishing a secure connection between the primary device (e.g., the laptop) and the device hosting the VDC. This feature ensures that the device with the credential is in close proximity to the device requesting the presentation, preventing phishing attacks in which a bad actor initiates a presentation on their own device and relays the QR code via a malicious website visited by the legitimate credential holder.

In summary, because of the security and user experience benefits of the DC API, we expect that it will become a W3C recommendation and be widely adopted across the web browser ecosystem. Refer to section 8.2.7 for more discussion on this topic.

6.2.5 Representative Core Banking Capabilities

Due to the complex and sensitive nature of banking systems, it was not feasible for any of our financial institution collaborators to provide a demonstration banking system that could integrate with our architecture. Therefore, in the early stages of this project, the consortium reached a consensus that building a representative bank would better support the project's goals and timelines. The core technical team then surveyed several open-source projects that could provide "core-banking" capabilities as described in section 4.3.2 and chose Fineract as the development banking platform.

6.2.6 Attribute Validation Capabilities

Not all attributes needed for alignment with CIP are available from the mDL data model. Additionally, financial institutions may want to compare user (e.g., phone number or email address) or device attributes against established fraud services to further increase confidence in transaction security. As a result, the project team identified early on that any architecture would need to illustrate the capability to validate additional attributes. This capability would acknowledge mDLs as a complement to current identity verification processes rather than a wholesale replacement. Time and scoping constraints prevented the integration of a commercial, SaaS-based attribute validation and fraud detection platform; therefore, the project team decided to develop a system that mimicked the electronic Consent Based Social Security Number Verification (eCBSV) Service created by the Social Security Administration (SSA). SSA developed eCBSV to facilitate "accepting and comparing fraud protection data provided electronically by a permitted entity." eCBSVs open specification and wide acceptance as a valuable service for FIs, made it an ideal choice to mock in our demonstration, which enabled our banking system

to verify if an applicant's Social Security Number, name, and date of birth combination matches (test) Social Security records.

6.2.7 Use of mDL for Authentication

VDCs can feasibly be used for a number of purposes in potential customer-facing processes, including identity verification, authentication, account recovery, and high-risk transaction authorization. However, using mDLs for authentication requires the driver's license number (along with the state issuer) to be conveyed at each usage to support account linking. For this reason, the project team decided not to use mDLs for authentication.

> ⚠ **Caution:** Frequently conveying a reusable identifier for transactions, coupled with conditioning users to routinely present a credential that contains identity information, is undesirable. Technology specifically designed for authentication scenarios—such as passkeys (see section 6.4.2.2)—should be chosen for day-to-day user authentication.

Due to the far less frequent nature of identity proofing (typically one-time per institution or for account recovery) and high-risk transactions (only when certain thresholds were met), these were deemed the most valuable scenarios for mDL as a credential type.

6.2.8 Local Versus Server-Side Holder Verification

As discussed in the use case, FIs must understand the third party risk they are accepting from issuers and wallets, and will seek to implement risk mitigations where appropriate. Some FIs may choose to implement a server-side biometric match during mDL presentment to address the lack of information available about the wallet's ability to authenticate the user locally. This match would compare the portrait image on the mDL with a selfie image collected from the user during mDL presentment. The NCCoE and its collaborators decided not to demonstrate this as part of the mDL project. While server-side biometric matching may give RPs additional confidence that the person presenting the mDL is the rightful mDL holder, it also introduces user friction which might result in orphaned accounts, creates privacy concerns through the collection of a biometric reference that must be managed by the RP and is susceptible to biometric injection attacks at scale. Ultimately, the NCCoE team determined that the risks of server-side biometric matching outweighed its marginal security benefit.

Instead, the NCCoE chose to demonstrate online presentation flows using local device authentication to unlock the mDL. This was done for several reasons: 1) local authentication preserves the privacy of users and enables a more efficient workflow, and 2) the signed, device bound nature of the credential coupled with local authentication, and proximity enforced through CTAP mitigates the vast majority of attacks that threaten FIs at scale today (e.g., fake documents, social engineering, and presentation attacks). This provides a streamlined, privacy-preserving workflow that is notably more secure than current CIP processes. It does not, however, eliminate all threats.

The NCCoE recognizes there are inconsistencies in how wallets perform holder authentication—some make use of device unlock, others use a biometric specific to the credential. Each of these permutations provides different security characteristics. Notably, wallets that make use of device unlock are susceptible to a close associate presenting an mDL for which they are not the rightful holder. However, to achieve this they would need to have physical access to the device and either 1) be enrolled on the

device (for example having your spouse's face enrolled to unlock your phone), or 2) have knowledge of an unlock secret (for example sharing the pin to unlock your phone with child) from presenting an mDL that does not represent them. In either case, this type of compromise is limited to a single device and user credential and is not subject to the same level of scalability of most threats to identity proofing that banks face today. Furthermore, as the mDL ecosystem evolves, standards, best practices and wallet capabilities for device holder authentication are expected to improve as well as the availability of information on holder authentication practices to the FIs and other RPs.

> **Caution:** FIs should evaluate the risk to individual transactions they support and determine whether the benefits of server-side biometric match outweigh the potential drawbacks. Information from the issuers about the holder authentication processes supported by wallets into which they issue credential should be evaluated to determine if local holder authentication is available and sufficiently mitigates anticipated risks.

6.2.9 Cross-Device and Same Device Presentation

mDLs are presented by holders in two scenarios – cross and same device. In a cross-device scenario, the mDL holder presents their credential from a mobile device through an interaction with a website on a separate desktop or laptop computer. In same device scenarios, all interactions occur on the mobile device. This demonstration chose to implement the cross-device flow to narrow the project scope. This practice guide will be updated in the future to include same-device scenarios.

6.3 Build Components

This section highlights the architecture components we deployed in the NCCoE lab environment. For a more general overview of components in the mDL ecosystem, please consider the "Digital Identities: Getting to Know the Verifiable Digital Credential Ecosystem" blog post. Implementers are encouraged to visit the project's supplementary website, which describes configuration details of each component.

> **Tip:** Video demonstrations of the NCCoE build are available here. Readers may benefit from taking a few minutes to see this architecture in action before reading through the components, flows, and how it was built.

Table 1 enumerates the products we used to build out the NCCoE Architecture. This includes a mix of products from our CRADA collaborators and components developed by the NCCoE using open-source software. Column 4 highlights the function of each component, demonstrating our capabilities listed in Section 6.1.

784 **Table 2. Architecture Technology Contributions**

Component	Collaborator(s)	Product	Function
Mobile Driver's License Issuer	Maryland Department of Transportation California Department of Motor Vehicles	State mDL test credentials	Test mDL credentials were issued to state-approved wallets and presented to the MATTR verifier to test and demonstrate the NCCoE Architecture
Wallet Applications	Google MATTR SpruceID	Google Wallet MATTR Kakapo Wallet California DMV Wallet	• mDL Storage and Protection • mDL holder authentication • mDL holder consent • Presentation of the mDL to the verifier
Trust Service	AAMVA	Digital Trust Service (DTS)	Provide the Verifier with access to the valid public keys that correspond to the test mDL credentials
Identity Management System	Microsoft	Microsoft Azure Active Directory Business to Consumer (B2C)	• Passkey enrollment and authentication • Directory services storing credentials, profile data, and the banking system's application registration • Create account application and digital enrollment identity validation workflows • Create and protect Encryption keys used for signing and validating tokens

Component	Collaborator(s)	Product	Function
Verifier	MATTR	MATTR VII	• Initiating verification via QR codes (cross-device flows) or deep links (same-device flows) • Requesting a verifiable presentation from a credential stored in a digital wallet • Verifying the cryptographic signature of received verifiable presentations • Verifying the cryptographic signature of the received verifiable credential and accepting the issuer
Bank-end Banking Services	NCCoE Developed	Laravel Open-Source Software	A system that enables a scoped set of banking functions, provides an API to facilitate front-end interactions, and provides a client to the core banking services
Core Banking Services	NCCoE Developed	Apache Fineract Open-Source Software	System(s) that facilitate financial services such as opening new accounts and processing transactions (e.g., deposits, withdrawals, and transfers).
Verifier Mediation Service	NCCoE Developed	Azure Functions	A proprietary API that facilitates mDL verifier attribute retrieval on behalf of the IDMS. This service was custom developed using Azure's serverless functions and leveraged the verifier's documented management API.
SSN Validation Service	NCCoE Developed	Laravel Open-Source Software	A system that emulates the functionality of the Electronic Consent Based SSN Verification (eCBSV) Service designed to validate social security numbers.

> **Caution:** The NCCoE used open-source products to build out the example NCCoE Bank, its back-end services and the SSN validation service. Since this technology was used for demonstration purposes only and FIs will already have their banking services implemented, the NCCoE does not intend to release configuration files or code for these architectural elements. The NCCoE will publish the configuration used for the IDMS and verifier to support the deployment of mDLs and passkeys.

6.3.1 Reference Architecture

Figure 4 is a graphical representation of the representative architecture we have implemented as part of the NCCoE Lab demonstration. This architecture is based on criteria that resulted from discussions with our industry collaborators and illustrates the general interactions between key components found in Table 1, while also highlighting some of the important protocols that were implemented as part of the architecture.

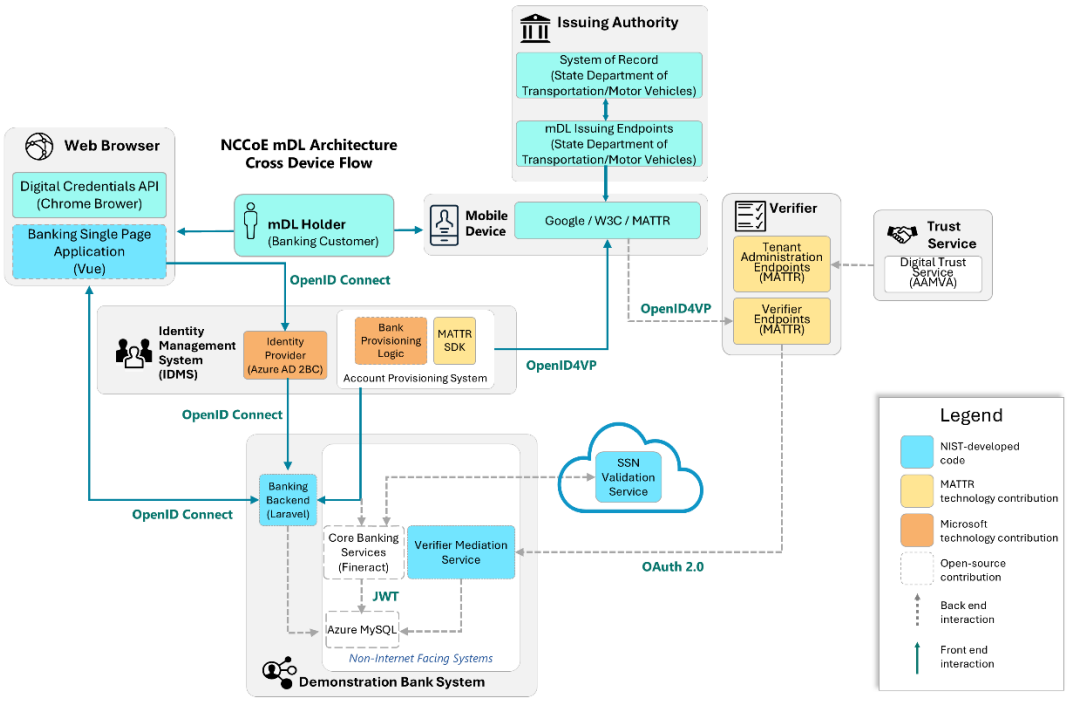


Figure 4. Reference Architecture Cross-Device Flow

As mentioned in section 6.2.8 this figure illustrates the cross-device flow we implemented. The cross-device flow occurs when the user needs to present their mDL to a website or service that is not being accessed from the same device where the mDL is stored. The most common example is a user presenting an mDL stored in a wallet on their mobile phone to a website or service they have navigated to in the browser on their desktop or laptop.

> **Definition:** Cross-device flow, as defined by OpenID4VP, is "*when an End-User presents a Credential to a Verifier interacting with the End-User on a different device than the device on which the Wallet resides.*"

While same-device flows are possible and will be common in the mDL ecosystem, this project chose to implement the cross-device flow initially to limit project scope.

> **Note:** The architecture above refers to cross-device scenarios in which the user accesses an online service. Cross-device flows could occur in person, such as a user walking up to a terminal and scanning a QR code or tapping an NFC reader.

The cross-device flow makes the following assumptions:

1. A banking customer navigates to a banking service and engages in an action that requires them to present their mDL. For the NCCoE project, the customer will be required to present their mDL for identity proofing when opening a new financial account and for step-up verification when a user conducts a high-risk transaction.
2. The customer has an mDL provisioned to the digital wallet on their mobile device and chooses to present it to the banking website, which they are accessing from a browser on a separate device.

6.4 Architecture Capabilities

This section details how our reference architecture in Figure 4 enables the capabilities we discussed in Section 6.1. The flows detailed in this section are all cross-device flows.

> **Note:** The NCCoE is building a demonstration mobile app that will connect to our back end and implement the same device architecture. This guide will be updated as the build progresses to highlight specific considerations related to same-device presentation.

6.4.1 Account Application Flow

The account application flow is the beginning of the user journey where the goal is to use an mDL to identity proof an "applicant" applying to open a financial account. A video demonstration of this flow can be seen here. In this flow, the applicant navigates to the NCCoE Bank webpage, selects the type of account they wish to apply for, and is then entered into the identity proofing process. This process includes three steps:

1. **Email address and phone number verification.** To ensure the bank can contact the applicant, they must link an email address and phone number to their account. This linking is accomplished by sending separate 6-digit codes via email and SMS to verify that the applicant is in possession of and controls the email and phone number provided to the bank. These codes are then entered by the applicant into the bank's web form and verified by the bank.
2. **Social Security Number (SSN) or Tax ID Number (TIN) validation.** CIP compliance requires that financial institutions collect and validate the applicant's SSN or TIN. For the NCCoE build, we opted to demonstrate the SSN and built out an example SSN validation service as discussed in Section 6.2.6. The applicant enters their SSN in the web form, and the banking back-end validates that the

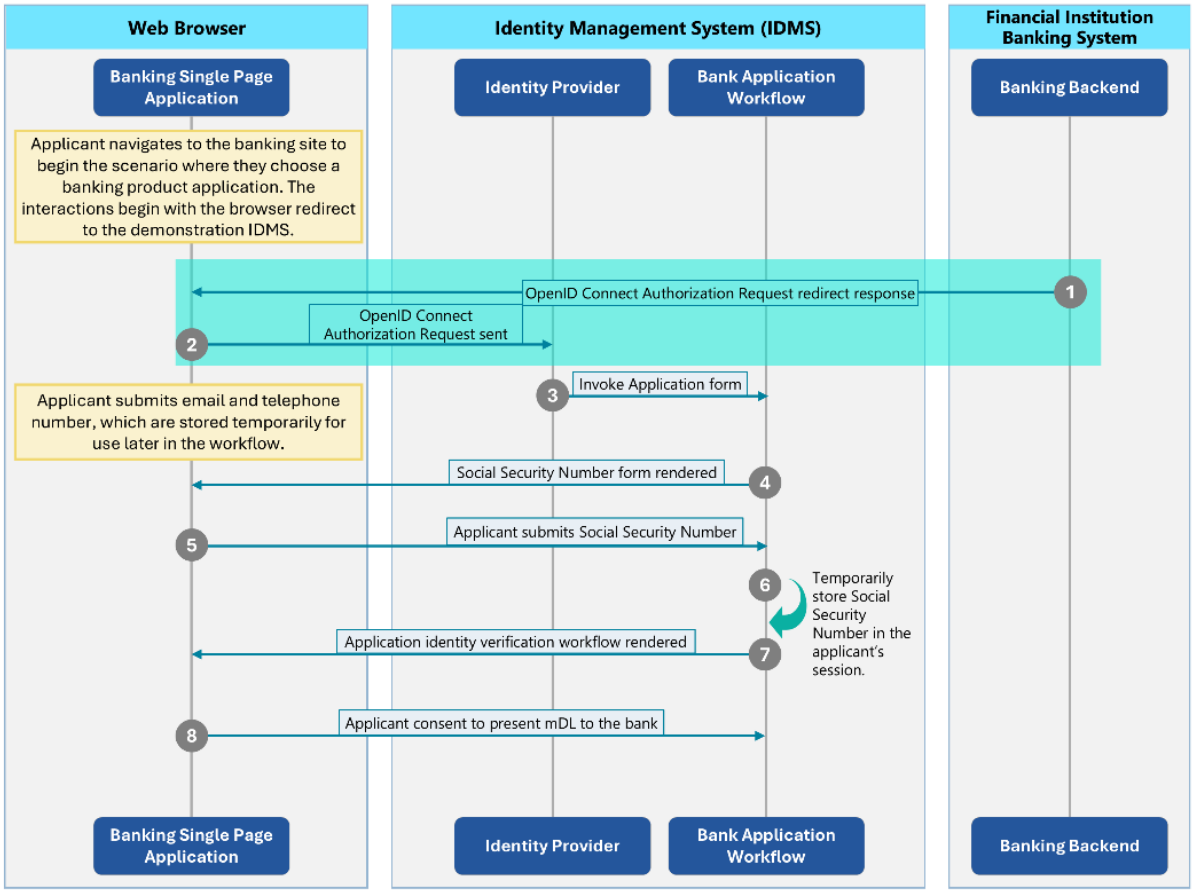
applicant's name, date of birth, and SSN match a valid record. In production, this would often be a third-party service; however, for the purposes of this build, the SSN validation service resides on the bank of NCCoE infrastructure.

3. **Presentment of the mDL and collection of the remaining CIP attributes.** The applicant may use their mDL to prove their identity. When selected, they are presented with a QR code that they scan with their device camera to invoke their wallet. To access their mDL, the applicant is asked to complete verification on device (biometric or PIN, based on what the wallet supports). Upon successful authentication, the applicant consents to presenting their information and the wallet responds to the initial request with the applicant's information from the mDL needed to meet CIP requirements. The verifier cryptographically verifies the data and passes it to the IDMS.

Upon completing the above three steps, the applicant confirms their information is accurate and submits their account application.

> **Note:** This project specifically chose to allow the applicant to apply for a financial account before digitally enrolling them and provisioning an authenticator. This choice was made based on explicit feedback from our financial institution partners: that the applicant's goal is to be approved for and open the financial account, and that any additional steps in that process could be detrimental to that goal.

To demonstrate how our architecture supports the account application flow, Figure 5, Figure 6, and Figure 7 below detail the sequential interaction of our components.



839 **Figure 5. User Initiates Application Process**

Steps 1-3	The applicant initiates the flow at the banking website by selecting the account they wish to create. The banking website logic then triggers the identity verification process with a browser redirect to the IDMS via an OpenID Connect authorization request,[3] which includes the Account Application user journey identifier to indicate which workflow Azure AD B2C will use. [4]
Steps 4-6	The IDMS recognizes the Account Application user journey identifier in the authorization request and proceeds to collect the applicant's email address, phone number, and SSN/TIN.
Steps 7-8	Upon successful validation of the email address and phone number, the IDMS requests the applicant's consent to collect mDL attributes.

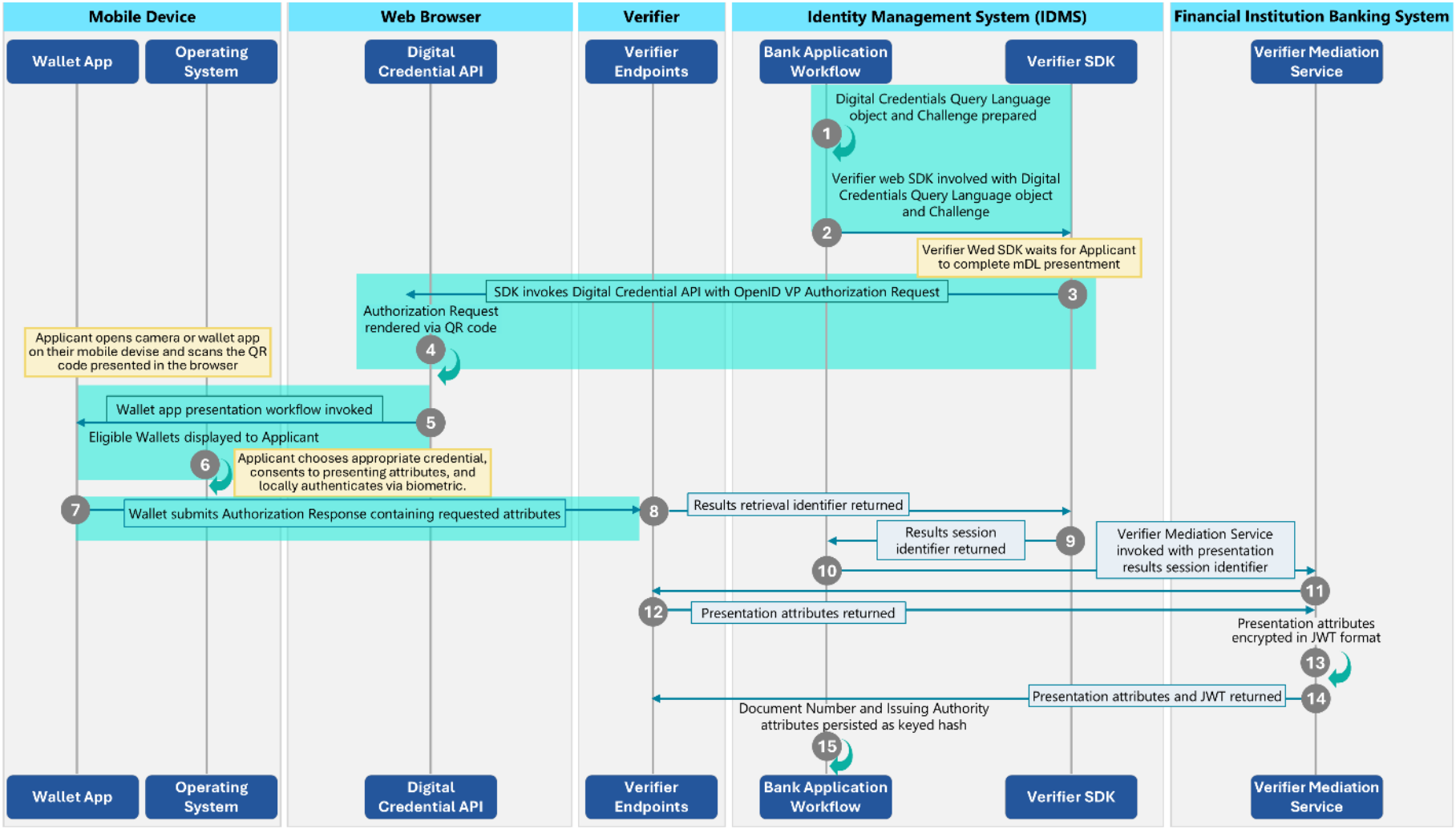
840 At this stage the IDMS invokes the verifier SDK with a query language—Digital Credential Query
841 Language (DCQL)—that allows a verifier to request a verifiable presentation from a wallet that matches

[3] The demonstration uses the authorization code flow with Proof Key for Code Exchange (PKCE). The details of these interactions are not shown in Figure 5 or Figure 6. Review Azure AD B2C documentation for detailed implementation details.

[4] The demonstration IDMS extends the standard OAuth 2.0 flows by adding a policy parameter which specifies the user flow to run. Review Azure AD B2C documentation for detailed implementation details.

a query. When used in an OpenID4VP transaction, a DCQL query enables the wallet to display to applicants the attributes being requested and credentials on their device that meet the parameters of the request. The SDK also requires a challenge (i.e. nonce) to be generated by the relying party. The challenge ensures the security and integrity of the credential verification process by preventing replay attacks and verifying the authenticity of each request and response [14]. Finally, the SDK is instructed to use a "cross-device" flow (as described in section 6.2.8) in which the applicant's wallet is invoked via a QR code device engagement. To complete the transaction, the applicant scans the QR code presented in their browser as part of the DC API.

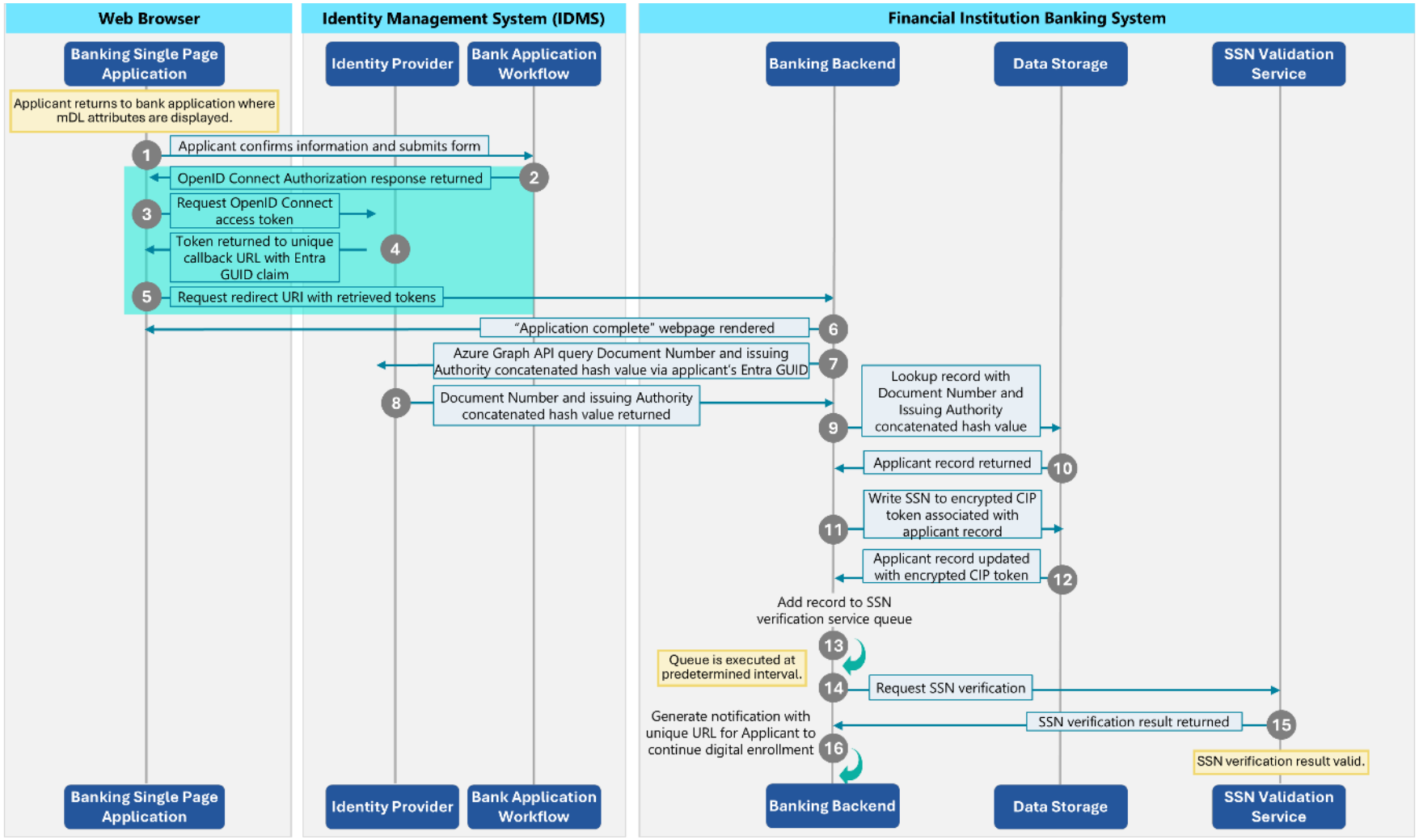
850



851 **Figure 6. mDL Verification Using the DC API**

Steps 1-6	The DCQL query (see Figure 14) requests attributes that support the bank's Customer Information Program. The SDK then creates an OpenID4VP authorization request which is relayed to the applicant's wallet via the Digital Credential API operating out of the applicant's browser.
Steps 7-14	After the applicant completes the Digital Credential API cross-device workflow, the mDL attributes are transmitted to the verifier and a session identifier is returned to the IDMS through the verifier SDK. The IDMS creates an association, which is accessible later in the flow through temporary storage, of the session verifier identifier and the active application. The IDMS then submits the verifier session identifier to the bank verifier mediation service API where it retrieves the mDL attributes which are subsequently encrypted in a JSON Web Token formatted token.
Step 15	The attributes, including the encrypted JWT, are returned from the bank's verifier mediation service to the IDMS where the mDL Document Number and Issuing Authority attributes are hashed and persisted as an identifier for the applicant. This identifier is stored in the applicant's directory object which is created as the final step of the IDMS user journey.

852



853 **Figure 7. Collection of Additional User Identity Information and Application Completion**

Steps 1	The Account Application flow concludes with the IDMS displaying the returned attributes from the verifier mediation service to the applicant. The applicant confirms that the attributes are accurate and submits the web form.
Steps 2-6	The IDMS processes the form and redirects the applicant's browser back to the banking website via an OpenID Connect Authorization response. The banking backend then uses the returned authorization code to retrieve an access token from the IDMS. The returned token signals to the bank that the application has been completed, and the flow should proceed.[5]
Steps 7-12	Next, the banking system uses the IDMS' internal identifier returned in the token to retrieve the applicant's SSN via a backchannel API call to the IDMS. The SSN is added to the existing encrypted JWT associated with the applicant's profile in the banking system's data storage.
Steps 13-15	The banking system checks the applicant's SSN against the validation service to ensure that the name and date of birth attributes correlate to the mDL. Upon successful validation, the banking system considers the applicant a customer and creates the requested account product.
Step 16	The bank notifies the new customer that their account has been approved and that they should initiate the digital enrollment flow via a one-time-use URL. This is presented via email for this demonstration.

6.4.2 Digital Enrollment Flow

The digital enrollment flow is the second step in our user journey. The goal of digital enrollment is to allow an approved applicant, who is now a "customer", to setup online access and management of their financial account. This includes provisioning the customer with an authenticator for subsequent login to the account.

6.4.2.1 Synchronous and Asynchronous Digital Enrollment Flows

Once the applicant has completed the application process, the financial institution must approve or reject the application. This process will differ based on the type of financial account requested, the information provided during identity proofing, and internal financial institution checks (e.g., fraud, OFAC, credit checks). For some applications, the financial institution might offer instant account approval, while others might have a waiting period as the bank executes its internal decision-making processes. We refer to these user experiences as the synchronous (instant approval) and the asynchronous (user must wait for account approval) flows. The type of flow that occurs affects how the approved applicant progresses to phase two of the user journey, the digital enrollment flow.

In the synchronous flow, the applicant is instantly approved and immediately offered the option to digitally enroll. Because the customer remains in the same browser session used to apply for the account, the bank has high confidence that the applicant who applied for the account is the same

[5] In all demonstration capabilities, a unique OpenID Connect callback URL is used to differentiate between user journeys. In the future, an Authentication Context Class Reference (ACR) claim will be included in the access token to closer align with a standards-based method to inform the relying party which authentication methods were satisfied.

person as the customer who is digitally enrolling. This allows for a streamlined user experience with no additional steps needed for the applicant to begin digital enrollment.

In the asynchronous flow, however, the initial browser sessions are closed. This might occur because the applicant is told that the financial institution will reach out to them once a decision has been made on their application (i.e., "you'll receive an email in the next 24 to 48 hours") or could occur if the applicant is instantly approved but opts to end the browser session and digitally enroll at the later period in time. In either case, when the applicant, now a customer, initiates digital enrollment in a new browser session, the financial institution must verify that the person entering the digital enrollment flow is the same person who applied for and was approved for the financial account. Our demonstration accomplished this by having the customer re-present their mDL to facilitate the account linking.

Note: Account Linking - When using an mDL to link the customer to an account, the financial institution needs only to collect those attributes from the mDL necessary to uniquely resolve the individual to their account. In our demonstration, we used a hash value of the driver's license number + the state issuer. Since driver's license numbers should be unique within each state's system of record, this combination of attributes was enough to constitute a unique identifier. This account linking is expected to be infrequent and not a solution for recurring authentication as discussed in Section 6.2.7. It may also be used to support account recovery in the event of a lost authenticator.

Figure 8 below details the asynchronous flow for digital enrollment, where the mDL is used for account linking, after the user initiates the flow through a link sent to them via email.

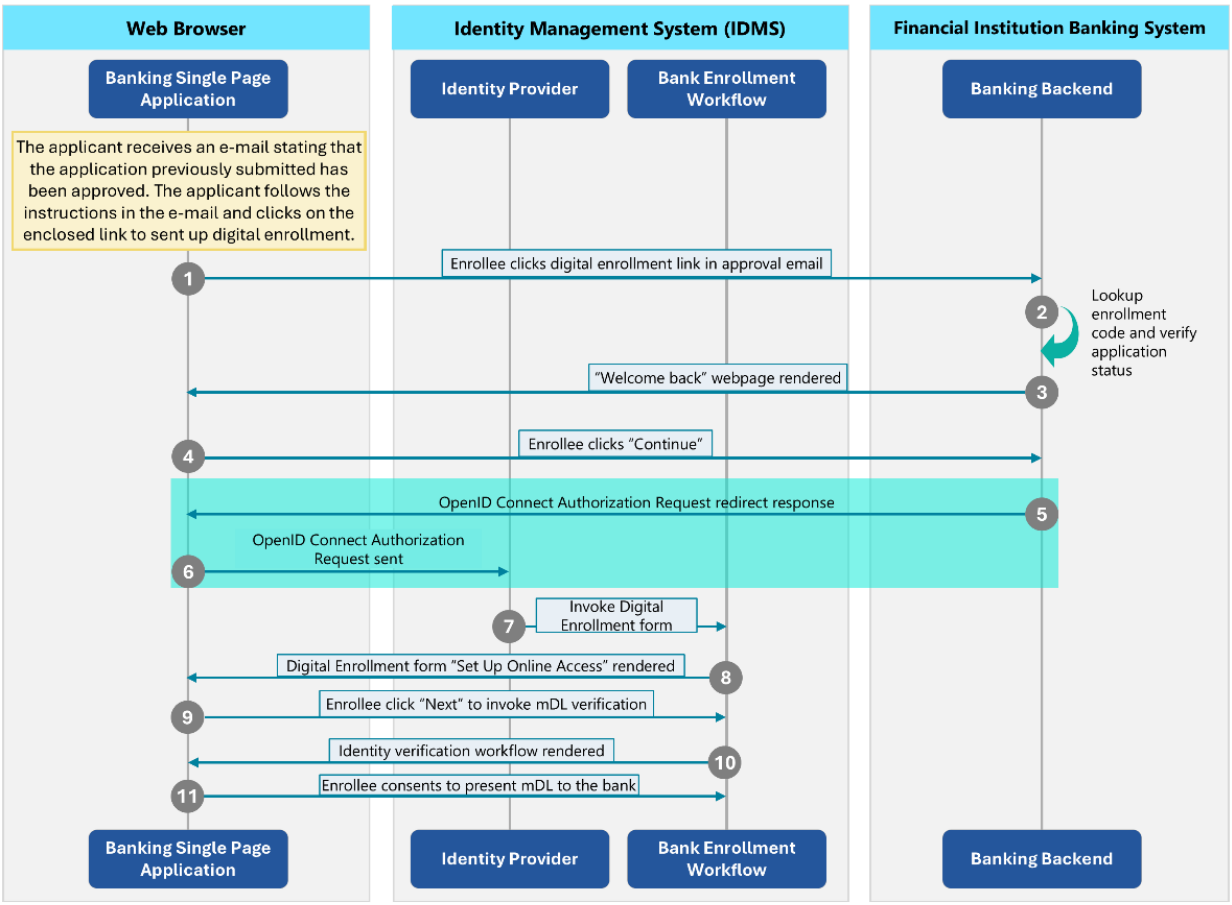


Figure 8. Initiating the Digital Enrollment Process from the Banking System

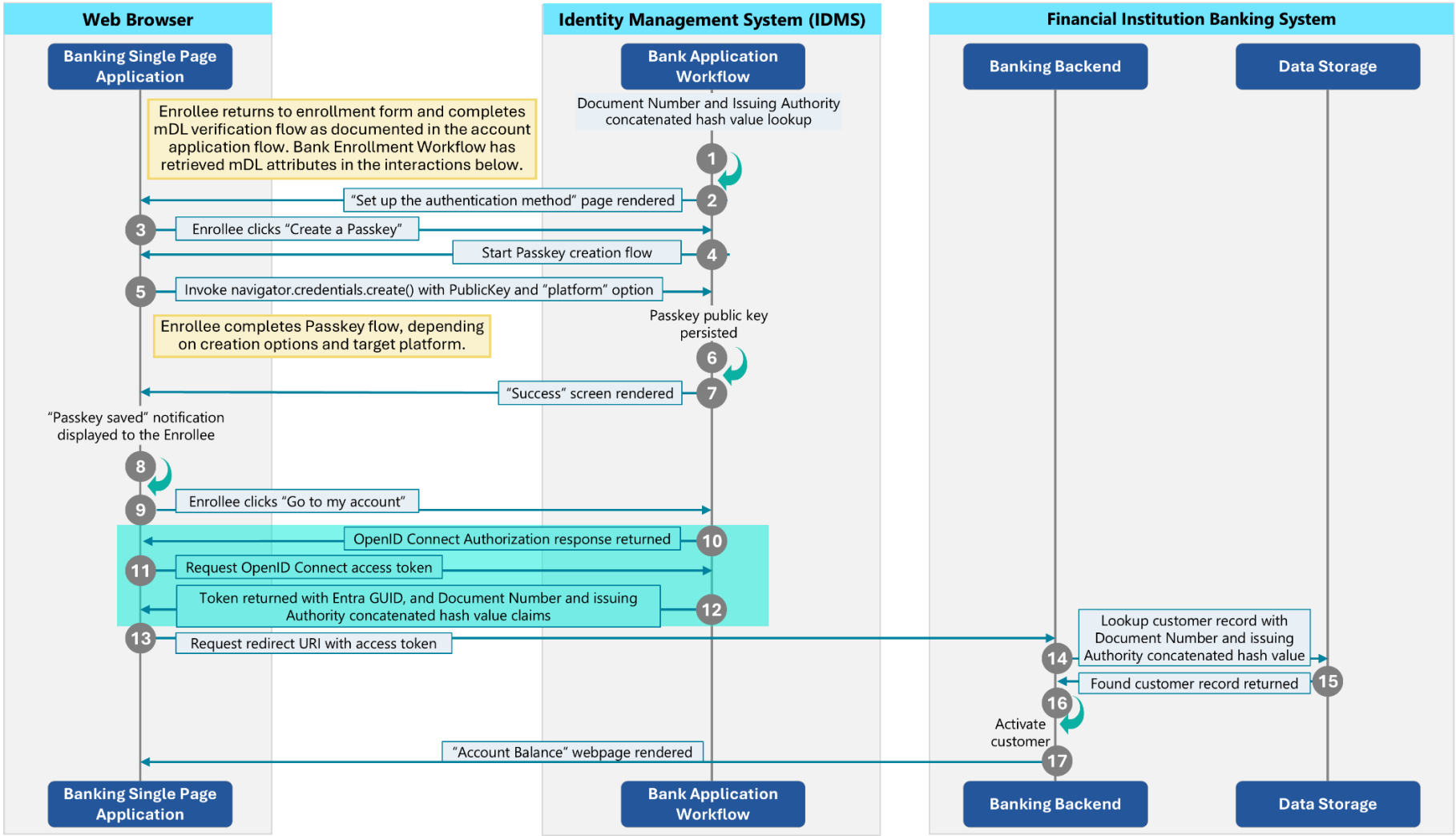
Step 1	The customer receives an e-mail stating that their application has been approved. The customer is directed to click on the enclosed link to set up online access to their account.
Steps 2-11	The banking system ensures the enrollment code in the link is valid, then redirects the customer to the IDMS via an OpenID Connect Authorization Request where they are prompted for consent for mDL re-verification. *Note: when this step is completed the user will present their mDL, the flow is the same what is illustrated in Figure 5. In this flow, the enrollee presents only their mDL driver's license number and issuing authority attributes as described in the Account Linking note above, supported by the DQCL query in Figure 15 .*

6.4.2.2 Provisioning the Customer a Passkey

While mDLs are highly useful during identity proofing, for day-to-day access to the financial account, it makes sense to provision the customer with a pseudonymous authenticator that does not require or pose the risk of revealing identity attributes. For this project, the consortium chose to provision Passkeys on the customer's device, enabling phishing-resistant authentication with the convenience of not typing a username or password or managing a security key.

Tip: For all high assurance use cases, NIST recommends the use of phishing resistant authenticators. Phishing resistance is important because phishing attacks remain a common and effective way to gain unauthorized access to accounts and systems. Phishing attacks attempt to lure a user (usually through an email) into interacting with a counterfeit webpage or application and trick the user into revealing information (typically passwords or one-time codes) that can be used to masquerade as that user to the real web page or application. This project provisioned a phishing-resistant passkey to the customers device for authentication. For more info on phishing resistance authentication, please read our blog post on the topic.

889



890 **Figure 9. Passkey Registration and Linkage to the Application**

At this stage, the IDMS invokes mDL verification as documented in Figure 6 except for the attributes that are requested from the customer. In this flow, only the document number and issuing authority mDL attributes are requested through the DCQL query.

Steps 1-8	Once the IDMS validates the customer's mDL identifier,[6] passkey registration begins. The customer's browser generates a cryptographic keypair, with the public portion transmitted and persisted in the customer's account profile at the IDMS per the WebAuthn API.[7] The customer will then be asked to authenticate on their device using a previously established biometric or PIN to complete the Passkey enrollment.
Steps 9-17	The IDMS prompts the customer to access their online account and redirects the customer's browser back to the banking website via an OpenID Connect Authorization response. The banking backend then uses the returned authorization code to retrieve an access token from the IDMS. The returned token signals to the bank that the customer has completed passkey enrollment and should be given access to their account, which is rendered in their browser.

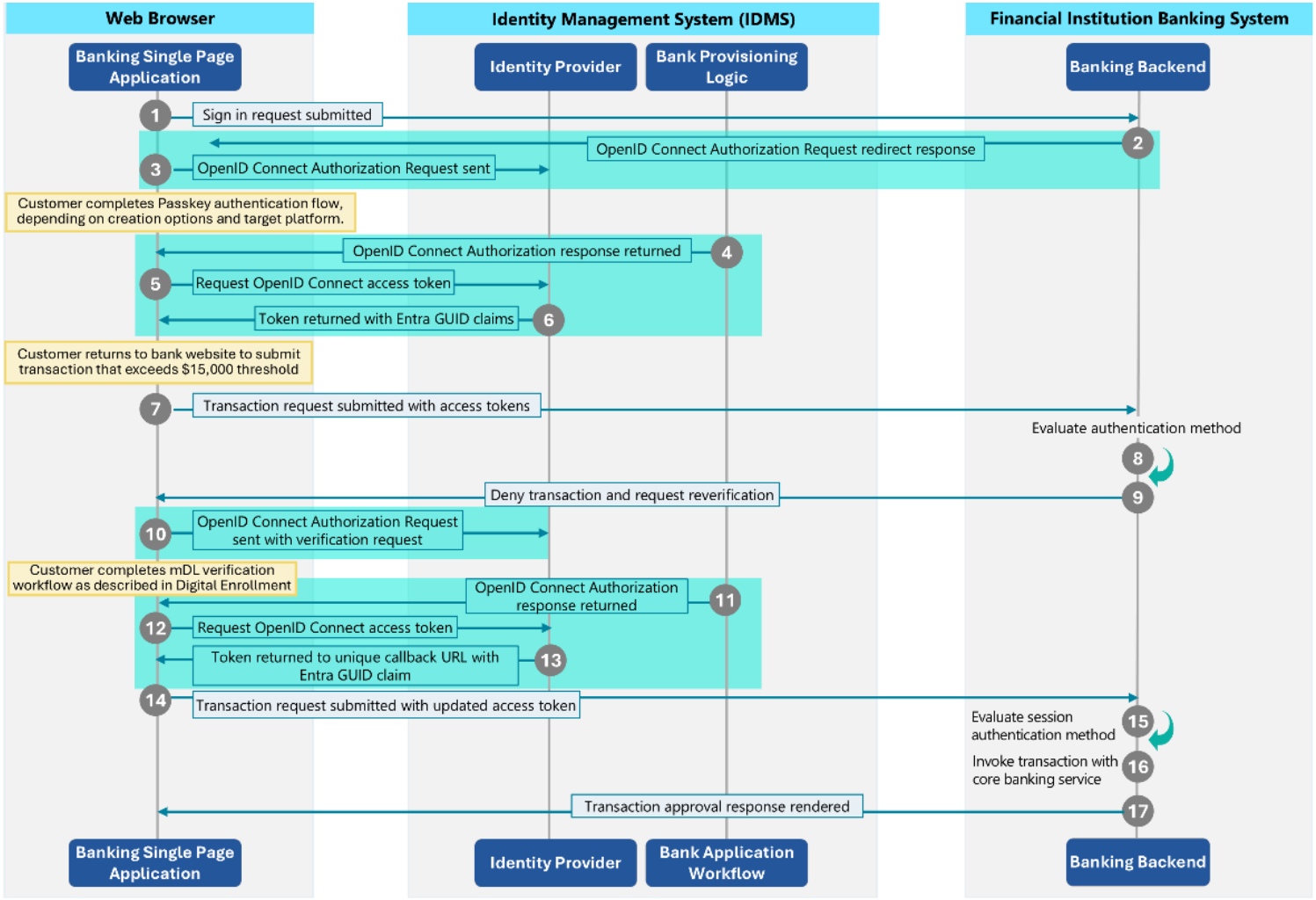
Note: While we did not demonstrate account recovery as part of this project, financial institutions may consider using mDLs as security signal and convenient element of the account recovery process, when a customer is unable to successfully authenticate.

6.4.3 High Risk Transaction Authorization

This flow is not part of the initial user journey but rather occurs when a customer attempts a transaction that is deemed high risk by the financial institution's policy and triggers a step-up re-verification of the mDL. The financial institution may offer mDL re-verification as one of several options for authorizing a high-risk transaction but may also specifically ask for an mDL when the bank knows that the customer presented an mDL during the identity proofing process. mDL re-verification is one of many signals a financial organization might use to decide whether to authorize a specific transaction. Each FI should consider how to integrate mDL re-verification with additional signals when authorizing high risk transactions.

[6] Hashed value of document number and issuing authority concatenation.

[7] Passkeys in this demonstration's context are configured to prefer native platform biometrics or a PIN to verify the user, however, implementations may differ across ecosystems.



903 **Figure 10. Re-Verification for High-Risk Transaction Authorizations**

Steps 1-6	The customer authenticates to the bank system via the IDMS using the passkey registered in Figure 8. The returned token contains an Authentication Context Class Reference value that denotes passkey authentication.
Steps 7-10	The customer submits a transaction request exceeding the bank risk threshold, which triggers a redirect to the IDMS via an OpenID Connect Authorization Request with a parameter that requests mDL verification. The customer completes the mDL presentation as described in Figure 8.
Steps 11-13	The customer's browser is redirected back to the banking website via an OpenID Connect Authorization response. The banking backend then uses the returned authorization code to retrieve an access token from the IDMS.
Steps 14-17	The updated access token is used with a new transaction request to the banking system, which is subsequently approved, granting the customer the ability to complete the high-risk transaction.

6.5 Storage of Attributes and Meeting CIP Requirements

Prior to the build phase, the project team agreed to a specific criterion in which the representative financial institution demonstrated storage of digital documents and associated data elements in a discrete repository in alignment with CIP retention requirements [15] (five years after the account has closed). The demonstration persists the required attributes in an encrypted format associated with the bank system's customer profile record in the bank system's internal database. A web-based administrative interface enables auditors (or other personnel) to decrypt and view the token associated with the banking customer. However, since the project timeline is much shorter than five years and only representative, it does not demonstrate production-level controls that an actual financial institution might implement (e.g., encryption key management, database access controls, etc.). A mapping of the minimum CIP retention requirements [16] to the representative demonstration can be found in the table below. Specific implementation details can be found on the project's supporting resources site.

Table 3. mDL Online CIP Threats and Mitigations

CIP Retention Requirement	Demonstration Capability
All identifying information about a customer (e.g., name, date of birth, address, and TIN).	The demonstration stores the following attributes from the customer's mDL in an encrypted token: First Name, Last Name, Birthdate, Issue Date, Expiry Date, Issuing Country, (State) Issuing Authority, Document (License) Number, Address, City, State, Zip Code The customer's Social Security Number is also stored as a token attribute.
A description of the document that the bank relied upon to identify the customer.	The encrypted token defines a *Verification Type* attribute. The demonstration uses a value *mdl* to indicate a *mobile security object* document type as defined by ISO 18013-5. This is associated with a timestamp indicating the customer's verification date.
A description of the non-documentary methods and results of any measures the	Non-documentary methods were not in the scope of the demonstration.

CIP Retention Requirement	Demonstration Capability
bank took to verify the identity of the customer.	
A description of the bank's resolution of any substantive discrepancy discovered when verifying the identifying information obtained.	Discrepancy scenarios were not in the scope of the demonstration.

917

7 Threat Model

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

7.1 mDL Security Capabilities

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

This combination of security capabilities also positions mDLs to mitigate threats from generative AI and the presentation or injection of "deepfakes". [8,9] As the 2025 FS-ISAC annual cyber threat report notes, generative AI has made it fast, inexpensive, and accessible for criminals to produce images of convincing fake IDs.[10] Rather than relying exclusively on images of IDs or videos of a face, mDLs enable relying parties to cryptographically validate identity attributes against a trusted authority.

Table 4 below highlights common threats to identity proofing systems and ways in which mDLs are resistant to those threats.

Table 4. CIP Requirement to Demonstration Capability Mapping

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, AI-generated ID images)	Cryptographic validation of data using the issuer's public key confirms the integrity and authenticity of evidence and identity data.

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

Threat	Threat Description	mDL Mitigation Capabilities
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 Real ID flags associated with issuance as discussed in the following use case."
Fraudulent Use of Identity	Use of someone else's valid documents to claim their 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 FI. 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 OID4VP (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.

A concise comparison of the relative benefits of mDL over traditional CIP techniques from a security and privacy perspective can be found in our website.

7.2 mDL Threats & Mitigations

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

- The hardware and software capabilities of mobile devices and their operating systems
- The digital wallet applications used to access and present mDLs
- The issuer processes that establish trust in mDLs
- 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.[11,12] It is also specific to the architecture NIST deployed, addressing threats to data communication between the distinct SaaS components. With any new technology adoption, financial institutions 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's recommended that organizations conduct their own threat assessment and integrate it with their organization-specific risk appetite, risk tolerance, and impacts.

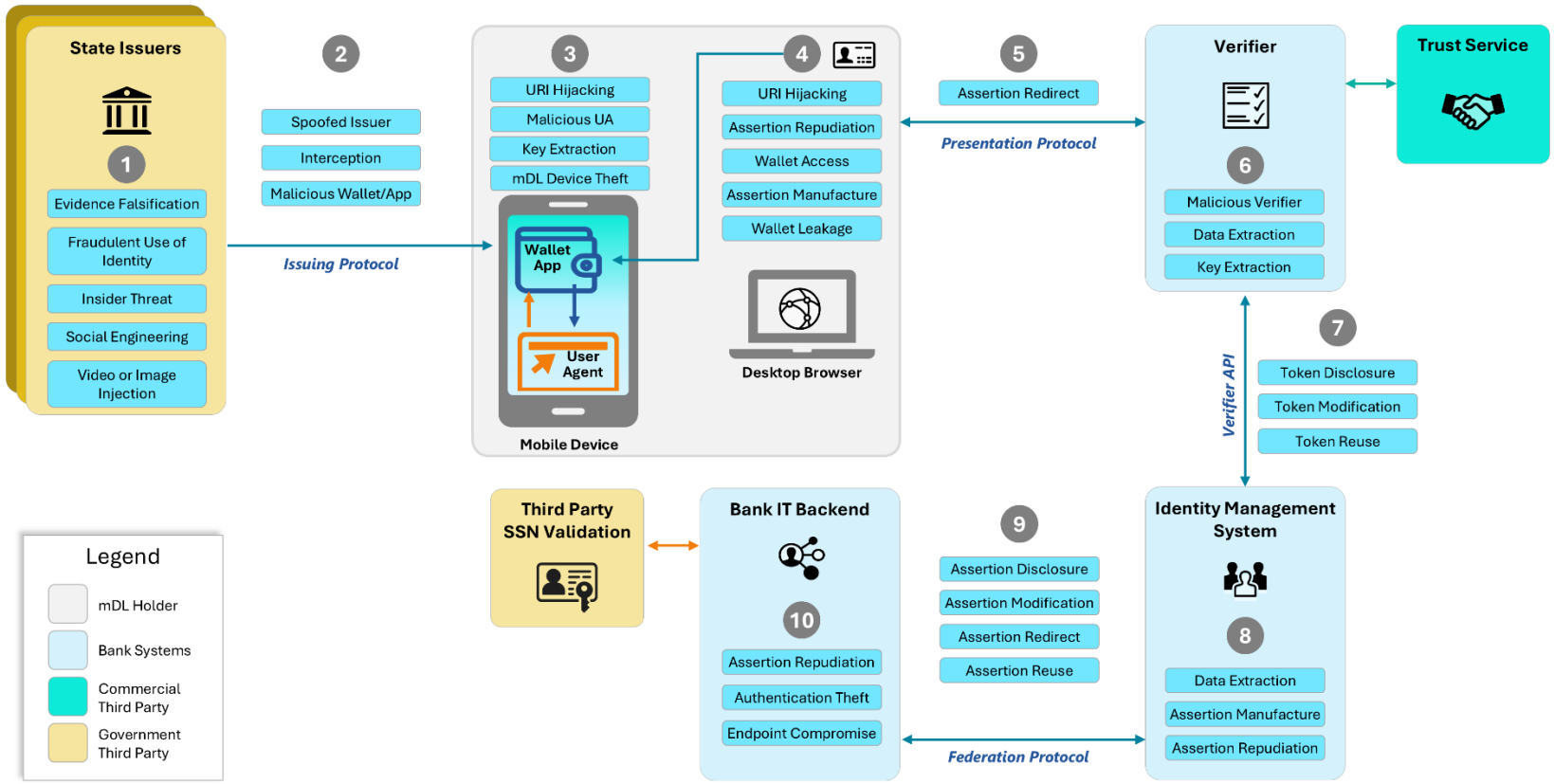
Figure 11 below overlays threats to each of the major components and interactions of the NCCoE architecture. Each threat is denoted with a numeric identifier. These identifiers are mapped to Table 5, which details the associated threat description and mitigations.

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 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, we recommend that 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 continue with 7 through 9 which 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, our demonstration banking system. This includes verifications that result from bank account applications, digital enrollment, and re-verification processes. Finally, interaction 10 considers indirect authenticator threats (mDL credential or passkey) that a relying party addresses in a federated architecture.

[11] ISO/IEC 18013-7 Annex C, which is support 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.
[12] 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.



985 **Figure 11. Threats to mDL Ecosystem**

986 **Table 5. mDL Remote Usage mDL Threats & 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.

Threat	Threat ID	Threat Description	Mitigation
	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., QR code 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 that the banking system is the intended recipient (e.g., audience claim).
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.

Threat	Threat ID	Threat Description	Mitigation
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 presents 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 Section 6.2.8 for considerations on device-

Threat	Threat ID	Threat Description	Mitigation
			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

Threat	Threat ID	Threat Description	Mitigation
			(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.
URI Hijacking	3	An attacker conducts an injection attack that uses a QR code to redirect mDL issuance messages to a compromised endpoint or similarly conducts a phishing attack to redirect the issuance process.	Use Wallets that preconfigure trusted issuers and reject untrusted issuer metadata (e.g., a non-trusted issuer). 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.

Threat	Threat ID	Threat Description	Mitigation
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

Threat	Threat ID	Threat Description	Mitigation
			authentication and 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 AI 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 at this time 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

Threat	Threat ID	Threat Description	Mitigation
			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's 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.

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

8 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.

8.1 Privacy Overview

Consumers spend a significant portion of their lives online. The way organizations manage data throughout its lifecycle, 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 their processing by a system.
- **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 12 illustrates this relationship, showing that some privacy risks stem from cybersecurity risks, while others are unrelated to cybersecurity risks.

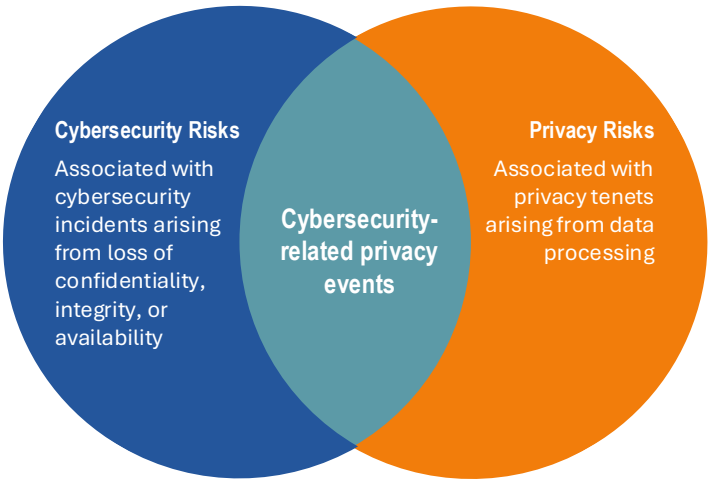


Figure 12. Cybersecurity and Privacy Risk Relationship

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

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

Definition: Problematic Data Actions - data actions that may cause an adverse effect for individuals.

Problematic data actions might arise by data processing simply for mission or business purposes. Privacy risk is the likelihood that individuals will experience problems resulting from data processing, and the impact should these problems occur. As reflected in the overlap of Figure 12, analyzing these risks in parallel with cybersecurity risks can help organizations understand the full consequences of data processing within their system. Section 8.2 describes scenarios where privacy problems may arise and potential mitigations.

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

8.2 Privacy in the mDL Architecture

Managing privacy risk is essential to protecting individuals and organizations. Emerging identity verification technology should seek to improve on the current state of privacy and provide users with greater protections. Mobile Driver's Licenses (mDL) and other Verifiable Digital Credentials provide opportunities to improve not only security, but also privacy. Through the selective disclosure of attributes, improved user control of credentials, the reduction of calls to third party services to validate user data, and the potential for future use of zero-knowledge proofs, mDLs can pave the way for a more privacy-preserving ecosystem.

For Financial Institutions (FIs), safeguarding customer privacy is important for several reasons:

- **Compliance**: FIs must comply with federal laws and regulations, such as:
    - Gramm-Leach-Bliley Act (GLBA);
    - Consumer Financial Protection Bureau (CFPB)'s guidelines and requirements for privacy, and;
    - Federal Deposit Insurance Corporation (FDIC)'s Customer Identification Program (CIP), Customer Due Diligence (CDD) regulations, and safety and soundness standards.

Individual states may have additional regulations that may apply; for example, California has four additional laws: California Financial Information Privacy Act (CFIPA), California Consumer Privacy Act (CCPA), California Privacy Rights Act (CPRA), and California Right to Financial Privacy Act (CRFPA).

In general, these laws and regulations require FIs to implement systems and processes to protect customer privacy and their financial records. For example, by prohibiting the disclosure of such records without the customer's consent, except under specific circumstances such as complying with law enforcement investigations.

- **Consumer Trust and Confidence**: Protecting privacy fosters trust and confidence among customers. When customers know their sensitive financial information is secure and that organizations take additional measures to protect privacy, they are more likely to remain loyal and continue using the FI's services. Privacy failures can lead to problems for individuals, such as identity theft, embarrassment, or distress—as well as problems for organizations, such as reputational damage, financial loss, and customer attrition. Privacy can become a key differentiator and provide a competitive edge to FIs that demonstrate robust privacy protections, attracting and retaining customers who place a premium on their privacy.
- **Due Care**: FIs handle vast amounts of personal and financial data and have an ethical obligation to protect the confidentiality and integrity of this data. Unauthorized access can result in identity theft, fraudulent transactions, and significant financial losses. Strong security practices, including encryption, access controls, and incident response protocols, help mitigate these security risks, as well as some privacy risks, and protect both the FI and its customers from harm.
- **Transparency:** As digital banking expands, customers expect transparency and control over how their information is used, making privacy protection a fundamental part of business. It's empowering customers to decide, under certain circumstances, what data to share. Further, it

improves transparency to provide customers with visibility into how their data is processed, with whom it is shared, and for what purposes.

mDLs present privacy benefits for both in-person and online identity verification flows that are not possible with traditional physical IDs. The following table illustrates a few of the benefits mDL may introduce. See Appendix E for a more thorough comparative analysis of mDL and other CIP models.

Table 6. mDL Privacy Benefits

Privacy Benefits	Description
User Control and Selective Disclosure	Only data *required* for opening the account is shared, minimizing the data collected and stored—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 biometric comparison at the FI and limiting the amount of biometric data regularly transmitted to support account onboarding.

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

The PRAM helps organizations tackle five major questions:

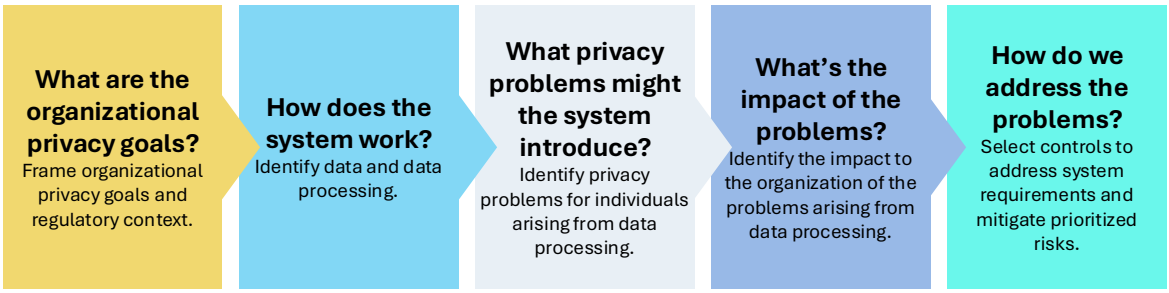


Figure 13. Five Privacy Questions

Taking on the role of an FI, the NCCoE applied the PRAM to assess the privacy risk of using an mDL to establish a financial account through online remote identity proofing. The NCCoE developed

representative responses of how an FI may complete this assessment. Table 5 below offers a sampling of the content in our mDL PRAM. A more robust assessment can be found on our website.

To demonstrate how an FI can apply the PRAM, the NCCoE created an example data flow diagram to enumerate each data action. The NCCoE identified a variety of problems individuals may encounter arising from mDL, along with a set of controls that are valuable for managing these privacy risks when implementing mDL.

Table 7. mDL Problems and Controls

Potential Problems for Individuals	Controls
Loss of Trust Customers could lose trust if their data is processed beyond what they predict. **Surveillance** With mDL for account enrollment, there is a chance for surveillance if the verifier or the issuer creates a pattern of the users' behaviors and actions online with the mDL. **Dignity Loss** If customers' activities are known in a way they could not predict, they could experience emotional distress. For instance, if the verifier tracks customer activities across transactions, it could create a narrative the customer never wanted to be known or a false narrative that could be misused. **Loss of Autonomy** Customers may feel like they have lost control over the processing of their data (e.g., if it is shared with third parties they did not expect to have access to it, if it is retained beyond a predictable timeframe, or if it is used for	**Device retrieval:** This verification model allows the verifier to independently verify the integrity and accuracy of the user's attributes without contacting the issuer at transaction time. Device retrieval supports data quality, while also preventing the issuer from getting a notification each time an individual uses their mDL (which could more easily lead to surveillance of an individual across their financial transactions). Server retrieval is not supported. **Cryptographic protection:** Leveraging mDL for account enrollment and step-up verification introduces new parties (e.g., the verifier) into the data processing ecosystem. This inherently introduces risk as data is transferred between partners. As in all scenarios that involve the processing of different data in a process flow, it is crucial to protect customer data at rest and in-transit using cryptographic techniques. For mDL this includes the signing of requests and responses between the verifier and wallet to increase confidence in participating entities and encrypting responses. It also includes the encryption of attributes when at rest in different FI backend systems as well as connected vendors. **Supplier assessments and reviews:** The introduction of mDL adds new parties to the account enrollment process (e.g., verifiers). Each additional party increases risk; thus, it is important to ensure that organizational risk management processes account for the broader supply chain. Supply chain participants should be evaluated to confirm they implement controls sufficient to meet the FI's privacy and compliance objectives. For example, if a third-party software is processing customer data, the FI should assess whether the software only processes the data for the agreed-upon purposes and deletes the data at the end of the retention period, whether the data is securely stored, and whether the data is shared downstream with additional third parties. **Notice and consent:** With the addition of an mDL, it may be harder for customers to predict how their data is processed—and

Potential Problems for Individuals	Controls
processing to which the customer never consented).	predictability is an important part of maintaining trust in an FI. Further, FIs have regulatory requirements for notice and consent before collecting personal information. Providing real-time notice for individuals is important to ensure predictability of how their data is processed, and it provides an opportunity to highlight that the only attributes collected from the mDL are those required for compliance. Consent empowers customers by giving them choice over which processing activities they do and do not agree to, such as whether they want to proceed with mDL or choose an alternative path to account enrollment. **Data retention:** FIs must retain certain customer data for seven years after a customer closes their account. However, not all parties in the ecosystem will need to comply with this same retention schedule. It is ideal for a third party to delete customer data promptly, and in accordance with its own retention obligations, to reduce the risks of holding that personal data.

The above problems for individuals, if realized, can translate to impacts on a financial institution, for example:

- **Reputational Damage**: Customers are becoming increasingly aware of and interested in how their data is handled, and some companies are even positioning privacy as a competitive advantage. If an FI uses customer data outside of the agreed-upon purposes, or a third party working with the FI surveils a customer across their transactions, this could become known to customers and impact the FI's reputation. Reputational damage can, in turn, have tangible downstream effects on the institution, such as costs associated with noncompliance with privacy regulations or direct business costs resulting from customers ending their relationship with an FI.
- **Direct Business Costs**: There are many reasons customers may not trust an FI with handling their data; for instance, a customer may have requested the deletion of their data, only to receive a personalized mailer indicating that their data wasn't deleted after all. They may have received notification of a breach at an institution. They may have read an article about ineffective access management processes that expose their data beyond what they expected. In any of these situations and more, a customer may choose to take their business to a competitor with different data handling policies. This can hurt the company's revenue and ability to attract new customers.
- **Noncompliance Costs**: FIs operate under strict regulatory environments, where problems for individuals may also be indicative of noncompliance with a financial regulation. For instance, FIs must obtain consent from individuals before collecting certain data. If they fail to demonstrate compliance with the swath of privacy regulations, they may face regulatory scrutiny and financial or other consequences.

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 an FI 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 mDL can be realized while minimizing the risk to individuals and organizations. The above is a brief sampling of problems and controls. A more detailed PRAM can be accessed on the supplementary resources website.

9 Usability Considerations & Evaluation Summary

9.1 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. FIs collaborating on this project made it clear that any user friction added to the identity proofing process could lead to application 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. The NCCoE conducted usability testing of our demonstration solution to identify usability issues, understand user behavior, and gather feedback on the application's functionality and overall UX.

Tip: Previous research indicates that having as few as 5 participants can reveal around 80% of usability issues, while 10 to 15 participants are enough to identify 95-97% of usability problems. Usability evaluations do not need to be resource intensive. Conducting them early in the development lifecycle can be a cost-effective measure, helping to avoid expensive rework later after deployment. For this project's usability evaluation, we recruited 12 NIST staff, none of whom were involved in this 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]

This evaluation employed a range of metrics and measures to assess the usability of the build, as listed in Table 7.

Table 8. 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*

9.2 Usability Best Practices

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

9.2.1 Preserve the positive characteristics of mDL-based verification

The evaluation demonstrated that users consistently perceived mobile driver's license (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.

9.2.2 Improve QR-code scanning reliability and predictability

Participants encountered difficulties when QR codes expired before they could complete actions on the mobile device. In several instances, expiration resulted in the display of a new QR code 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 QR code validity periods, maintaining consistent QR code 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.

9.2.3 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.

9.2.4 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.

9.2.5 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

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

9.2.6 Consider factors and potential barriers to adoption

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

9.2.7 Evaluate and plan for additional, user-driven use cases

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

10 mDL Challenges & Recommendations

10.1 Trust Models and Trust Establishment

In project discussions with the Financial Sector, FIs have expressed a need for greater clarity on the processes for enrolling, issuing, and presenting mDLs. Specifically, FIs must have a clear understanding of the assurances they are getting and the potential risk they are accepting when implementing mDLs.

Traditionally, FIs own and control their identity verification systems, which allows for agility when responding to threats and mitigating risks associated with identity verification. While the mDL ecosystem offers potential benefits to FIs across security, fraud reduction, privacy, and usability, adoption of this technology requires trust in third parties, such as the mDL issuer and the wallet that stores the mDL.

To accept this third-party risk, FIs are seeking assurances to assuage their concerns around the processes used to enroll, issue and present mDLs. The table below summarizes these concerns. For a more detailed discussion on this topic, please review our supplementary resources webpage.

Table 9. Assurance in the mDL Ecosystem

Issue	Discussion	Solution
Issue #1: Enrollment into the System of Record (SOR) at the DMV	FIs are concerned about the lack of visibility into the process used to identity-proof and enroll a user into the SOR at the DMVs when issuing the user with their initial,	This is addressed by the inclusion of the AAMVA-mandated "Real ID" compliance field in the mDL. This provides issuer signed

Issue	Discussion	Solution
	physical credentials on which the mDL will be based.	indicators of how the initial issuance was achieved.
Issue #2: Issuance of the mDL or Digital Credential to the Holder's Digital Wallet	FIs are concerned about the limited visibility they have into issuance processes for mDL and other forms of verifiable digital credentials. As mDLs become more valuable, the issuance processes are increasingly likely to be targeted by attackers.	The project proposed addressing this in two ways: 1. By providing a profile of NIST SP 800-63A for the issuance of mDLs. This can be referenced as a baseline for consistent issuance processes; and 2. Encoding security characteristics of issuance process into the credential itself. Using attribute sets such as those in the OpenID for Identity Assurance, this security "metadata" can be signed by the issuer and stored in the mobile security object of the mDL.
Issue #3: Holder Binding during mDL Presentment	FIs are concerned that processes used to authenticate the holder of an mDL vary in implementation and security assurances across wallet and mobile operating systems. Absent clear signals or more consistent implementations FIs are likely to adopt server-side biometric match whenever an mDL is used, which presents significant privacy concerns.	This could be addressed by adding data to the presentation protocols that defines a set of holder authentication methods supported by wallet, that can be requested by verifiers. This would provide RPs with insight into the degree to which the mDL holder is bound to the credential during presentation. ISO working group 10 is currently undertaking efforts to define these authentication values to be included in ISO 18013-7.

In addition to these items, most FIs expressed a desire to have greater confidence in a wallet's underlying security and ability to meet existing and emerging features (such as those identified above). A more robust trust ecosystem that includes wallet certification against well-defined requirements has emerged as a critical step toward adoption, particularly as the overall mDL and VDC ecosystem begins to solidify. In the US, the Fast Identity Online (FIDO) Alliance, recently announced a working group focused on developing wallet certification criteria to address this gap area. Additionally, organizations like the

OIDF have developed testing tools to determine conformance with their presentation protocols and issuance protocols. Taken together, these efforts provide a foundation for the expansion of trust across the ecosystem.

10.2 Standards Maturity Levels

A notable feature of this project was consistent evolution of the underlying standards and protocols that support online presentation. Over the course of the build, OID4VP, HAIP, DC API, and ISO/IEC 18013-7 underwent substantive changes, 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.

Fortunately, there is good news here as well. 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.

Even with this momentum, there remain some broader standards items that need resolution. The first - is completion of the W3C DC API. At the time of writing, the API is an initial draft. And, while several initial implementations are already shipping in browsers such as Chrome and Safari, the specification is still in its early stages 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 in and of itself 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. While consolidation of presentation protocols is desirable, and there is some movement to make this a reality, the stability of presentation protocols is a fundamental precursor to adoption. As these standards have evolved the NCCoE mDL team and project collaborators have acted as a conduit to relevant standards bodies, conveying learnings, issues, and challenges distilled from the project. This has included engaging with OIDF, 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 sought to provide 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 such engagement will continue as additional phases of work progress.

10.3 Regulatory Uncertainty

Perhaps one of the most common refrains the NIST project team heard during the discussions with FI collaborators was, “but will the regulators allow us to use this?” Regulation and compliance are core to the risk management and decision-making processes for FIs, who face potentially costly impacts of non-compliance, which makes early adoption complicated.

While it is not within NIST's capacity to make authoritative determinations of whether mDL is compliant with CIP requirements, the project team has attempted to minimize this barrier to adoption through two resources: 1) a Regulatory Mapping that compares the capabilities demonstrated through the project to the requirements defined in Title 31 Code of Federal Regulations 1020.220 (commonly referred to as *Customer identification Program for banks*), and 2) the CIP/KYC Documentary Considerations appendix provides a simple reference for risk management professionals that compares existing CIP documentary methods to our built demonstration. The tables compare documentary methods along three axes: security, privacy, and usability.

Ideally, these contributions can help advance conversations between FIs and their regulators to demonstrate that mDLs provide risk reduction that is equal to or exceeds that of current identity proofing processes.

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] Internation 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] Internation 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*. 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
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/.

[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 Supporting Resources website.

Resource Name	Location
CIP Use Case Criteria	https://pages.nist.gov/nccoe-mdl-project-static-website/use-case-1/criteria.html
Sample Bank mDL Information Page	https://pages.nist.gov/nccoe-mdl-project-static-website/use-case-1/nccoe-bank-faq.html
Wire Frames	https://pages.nist.gov/nccoe-mdl-project-static-website/use-case-1/wireframes.html
Financial Use Case Reference Architecture	https://pages.nist.gov/nccoe-mdl-project-static-website/use-case-1/architecture/kyc-cip-onboarding.html
Interaction Diagrams	https://pages.nist.gov/nccoe-mdl-project-static-website/use-case-1/architecture/interaction-diagrams.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
CIP Regulatory Mapping	TBD
Privacy and Security Comparative Analysis	TBD
Demonstration Videos	https://pages.nist.gov/nccoe-mdl-project-static-website/use-case-1/demonstration-videos.html

Appendix C Regulatory Mapping

The primary outcome from this demonstration is to ensure that digital credentials and associated relying party workflows align with the Bank Secrecy Act. To support this outcome, the core project team along with project collaborators, Federal agency and NIST subject matter experts have developed a mapping in the table below between the technical implementation capabilities and Title 31 Code of Federal Regulations 1020.220 commonly referred to as *Customer identification program for banks*.

Note: This mapping is an effort to illustrate the alignment of mDL and the process implemented as part of the NCCoE build with the requirements defined in the CIP. It does not guarantee regulatory acceptance or compliance.

1358 **Table 10. CIP Requirement to Capability Mapping**

CIP Requirement	Demonstrated Capability or Process	Capability Relationship to CIP Requirement	Relationship Explanation
31 CFR 1020.220(a)(2) ***Identity verification procedures.*** The CIP must include risk-based procedures for verifying the identity of each customer to the extent reasonable and practicable. The procedures must enable the bank to form a reasonable belief that it knows the true identity of each customer. These procedures must be based on the bank's assessment of the relevant risks, including those presented by the various types of accounts maintained by the bank, the various methods of opening accounts provided by the bank, the various types of identifying information available, and the bank's size, location, and customer base. At a minimum, these procedures must contain the elements described in this paragraph (a)(2).	Customer Identification with mDL Verification and TIN Validation	Aligned to CIP general requirement.	This requirement defines the general expectation that financial services organizations apply a risk-based approach to determine the "true identity" of each customer. mDL verification provides means to mitigate risk associated with identity theft or fraudulent account opening by **leveraging cryptographic security features embedded** within the digital credential. Coupled with holder verification to the mobile device through biometrics and other local authentication factors, this provides financial institutions with an increased degree of confidence over existing methods that **1) the evidence is real and not forged**, and **2) in the possession of the individual who is represented by the credential**. Note: see Section 6.2.8 for discussion of local v. server-side verification of holders.
31 CFR 1020.220(a)(2)(i)(A)(1) – 31 CFR (a)(2)(i)(A)(3)(iii) (A) ***In general.*** The CIP must contain procedures for opening an account that specify the identifying information that will be obtained from each customer. Except as permitted by paragraphs (a)(2)(i)(B) and (C) of this section, the bank must obtain, at a	Verifiable mDL Attributes.	Aligned to CIP Requirements for identity and address attributes.	The following attributes are mandatory and encoded and signed into all mDL presentations. - Family Name - Given Name - Date of Birth - Address Each of these elements is mandatory in the AAMVA Implementation Guidelines and necessary to meet CIP requirements. The presence of these attributes within the

CIP Requirement	Demonstrated Capability or Process	Capability Relationship to CIP Requirement	Relationship Explanation
minimum, the following information from the customer prior to opening an account: (*1*) Name; (*2*) Date of birth, for an individual; (*3*) Address, which shall be: (*i*) For an individual, a residential or business street address; (*ii*) For an individual who does not have a residential or business street address, an Army Post Office (APO) or Fleet Post Office (FPO) box number, or the residential or business street address of next of kin or of another contact individual; or (*iii*) For a person other than an individual (such as a corporation, partnership, or trust), a principal place of business, local office, or other physical location; and			Mobile Security Object (MSO) ensures their integrity and accuracy. Additionally, these attributes are compared against access policy requirements in the financial services IDMS—meaning if the credential did not contain the necessary data an enrollment attempt would not be successful. APO/FPO may be available on an mDL in addition to a physical address depending on the state policy, though this was not tested or observed during the project. At this time, mDL's are for individuals only and would not support clause (ii) which allows for next of kin/contact individuals, or clause (iii) which refers to corporations.
31 CFR 1020.220(a)(2)(i)(A)(*4*)(*i*)	Tax Identification Number (e.g., Social Security Number) Applicant	Aligned to requirements for an identification, specifically a Tax Identification Number for U.S. persons	A TIN[13] attribute is not included in US State issued mDLs. The demonstration collects TIN (social security number) as part of

CIP Requirement	Demonstrated Capability or Process	Capability Relationship to CIP Requirement	Relationship Explanation
(*4*) Identification number, which shall be: (*i*) For a U.S. person, a taxpayer identification number;	Identifier Request and validation		the account opening web workflow and validates this information against a mock third-party data source.[14]
31 CFR 1020.220(a)(2)(i)(A)(4)(B) & (C) (B) ***Exception for persons applying for a taxpayer identification number…*** (C) ***Credit card accounts…***	Not Addressed	Not Addressed	These two clauses related to those without a TIN and allowances for credit card accounts to be opened with third party data. The build is not intended to address risk-based decisions on those who do not have TINs or processes for extending credit. As such they are out of scope for the build, and in NIST's view do not impact the ability for an mDL based process to support compliance with CIP requirements.
31 CFR 1020.220 (a)(2)(ii) ***Customer verification.*** The CIP must contain procedures for verifying the identity of the customer, using information obtained in accordance with paragraph (a)(2)(i) of this section, within a reasonable time after the account is opened. The procedures must describe when the bank will use documents, non-documentary methods, or a combination of both methods as described in this paragraph (a)(2)(ii).	mDL Verification with TIN Validation	Aligned to requirements in both documentary (mDL) and non-documentary (TIN) verification processes	The mDL process as defined in this demonstration uses **both documentary and non-documentary processes** to verify the identity of an individual applying for an account. The mDL itself conforms to documentary verification processes, proving identity based on the existence of a verifiable digital credential (mDL) signed by the issuing state, while the non-documentary process validates the existence of a TIN. These are discussed in more detail below.

[14] Note that an exemption in June 2025 was granted from the requirement to collect a TIN from a customer before opening an account so long as a TIN could be validated for the user based on third party sources. This means the mDL workflow could be implemented without an additional data request to the user so long as the attributes provided off the mDL are able to resolve to a TIN in third party data sources used by the bank.

CIP Requirement	Demonstrated Capability or Process	Capability Relationship to CIP Requirement	Relationship Explanation
31 CFR 1020.220 (a)(2)(ii)(A)(1) & (2) (A) ***Verification through documents.*** For a bank relying on documents, the CIP must contain procedures that set forth the documents that the bank will use. These documents may include: (*1*) For an individual, unexpired government-issued identification evidencing nationality or residence and bearing a photograph or similar safeguard, such as a driver's license or passport; and (*2*) For a person other than an individual (such as a corporation, partnership, or trust), documents showing the existence of the entity, such as certified articles of incorporation, a government-issued business license, a partnership agreement, or trust instrument.	mDL Verification including verifiable attributes and holder authentication	Aligned to documentary verification processes.	An mDL is a digital document issued to an individual by **a state government authority** (e.g., DMV) through an identity proofing process. It contains attributes and data elements which have been signed using public key cryptography ensuring the integrity and accuracy of the data. They are also signed by a unique device key preventing them from being shared to other devices and are protected during online presentation through local authentication mechanisms (often biometrics). In addition to the user's personal attributes an mDL also contains signed attributes such as the **License Expiration date** and **the holder's portrait,** and **physical address** as mandated by this requirement. While nationality is not indicated on driver's license (mDL or otherwise), DLs and mDL do serve as proof of residence. This is further supported by the inclusion of a realID compliance flag which has elevated expectations for residency status. The portrait can be used to 1) augment local authentication by enabling a bank biometric verification at the time of account opening and 2) physical verification in branches. This project only focused on identification of individuals and therefore does not cover example (2) at this time. It is NIST's

CIP Requirement	Demonstrated Capability or Process	Capability Relationship to CIP Requirement	Relationship Explanation
			view that this does not impact the ability of an mDL to be used as part of a compliant CIP process.
31 CFR 1020.220 (a)(3)(i)(A) – (D) (3) ***Recordkeeping.*** The CIP must include procedures for making and maintaining a record of all information obtained under the procedures implementing paragraph (a) of this section. (i) ***Required records.*** At a minimum, the record must include: (A) All identifying information about a customer obtained under paragraph (a)(2)(i) of this section; (B) A description of any document that was relied on under paragraph (a)(2)(ii)(A) of this section noting the type of document, any identification number contained in the document, the place of issuance and, if any, the date of issuance and expiration date; (C) A description of the methods and the results of any measures undertaken to verify the identity of	CIP record establishment with representative financial institution	Representative of record keeping requirements	The NIST Bank of NCCoE is not a real financial institution. The demonstration records are established to represent a real-world architecture and process but are not as robust as real-world record systems. Attributes collected during the customer identity verification process in this demonstration were stored in an encrypted structured token within a database accessible to the banking system. The following information is captured in these tokens for all mDL related test transactions: • (A) Verified user attributes (see above for details) • (B) Document Identification Number (i.e., license number) • (B) Identification Expiration Date • (B) Issuing Entity (i.e., issuing state) • (B) Issuance Date • (C) A value of “mDL” stored in the token indicating the CIP method used. Other methods were not included as

CIP Requirement	Demonstrated Capability or Process	Capability Relationship to CIP Requirement	Relationship Explanation
the customer under paragraph (a)(2)(ii)(B) or (C) of this section; and (D) A description of the resolution of any substantive discrepancy discovered when verifying the identifying information obtained.			values since they were not tested, though FIs should expand and include values for all of their supported CIP methods. • (D) Existence of a token was provided as an indication of successful identity verification – Financial Institutions should expand on the token or an associated supplementary record to include more detailed information related to the CIP processes used.
31 CFR 1020.220 (a)(3)(ii) (ii) ***Retention of records.*** The bank must retain the information in paragraph (a)(3)(i)(A) of this section for five years after the date the account is closed or, in the case of credit card accounts, five years after the account is closed or becomes dormant. The bank must retain the information in paragraphs (a)(3)(i)(B), (C), and (D) of this section for five years after the record is made.	Not Addressed	Not Addressed	Since the project is demonstration only, no information is being retained. However, the demonstrated records may be retained for as long as an FI is required. It is NISTs view that this does not impact the ability of the project to demonstrate conformity of mDL based process to CIP requirements.
31 CFR 1020.220 (a)(4) (4) ***Comparison with government lists.*** The CIP must include procedures for determining whether the customer appears on any list of known or suspected terrorists or terrorist organizations issued by any Federal	Mocked government identifier check	Aligned to Requirement for Government Records Check	The representative financial service application runs the applicant provided SSN against a mocked service for external checks. This is not however, an external service check as such checks cannot be done with against test SSNs. OFC and other sanctions checks were out of scope for our effort. Financial Institutions have existing processes for

CIP Requirement	Demonstrated Capability or Process	Capability Relationship to CIP Requirement	Relationship Explanation
government agency and designated as such by Treasury in consultation with the Federal functional regulators. The procedures must require the bank to make such a determination within a reasonable period of time after the account is opened, or earlier, if required by another Federal law or regulation or Federal directive issued in connection with the applicable list. The procedures must also require the bank to follow all Federal directives issued in connection with such lists.			checking government restrictions that will continue to operate alongside mDL based CIP processes. It's NIST's view that mocking this service has no impact on the ability of mDL based CIP to conform to regulatory requirements.
31 CFR 1020.220 (a)(5)(i) – (iii) (i) ***Customer notice.*** The CIP must include procedures for providing bank customers with adequate notice that the bank is requesting information to verify their identities. (ii) ***Adequate notice.*** Notice is adequate if the bank generally describes the identification requirements of this section and provides the notice in a manner reasonably designed to ensure that a customer is able to view the notice, or is otherwise given notice, before opening an account. For example, depending upon the manner in which the account is opened, a bank may post a notice in the lobby or on its Web site, include the notice on its	Notice and consent collection – prior to starting the CIP process and prior to collection of identity attributes	Aligned to notice requirements	The demonstration includes notice and consent throughout the CIP process. This includes: - (i) General notice to the customer of the reasons for conducting CIP processes, the data to be collected, and information on why data collection is required. - (ii) Specific notice with respect to mDL verification process and consent to collect specific attributes from the user's mDL is presented prior to a request being sent to the user's mobile device for the attributes. This also includes a link to more detailed information on mDL's. - (ii) Specific consent at the wallet prior to the release of the attributes to the financial institution. **Note**: This consent is presented and managed by the wallet itself not the FI. - (iii) Our language is available at our supporting resources website. It is similar but not the same as the sample

CIP Requirement	Demonstrated Capability or Process	Capability Relationship to CIP Requirement	Relationship Explanation
account applications, or use any other form of written or oral notice. (iii) **Sample notice.** If appropriate, a bank may use the following sample language to provide notice to its customers…			language. It was developed with UX experts and collaborators from FIs.
31 CFR 1020.220 (a)(6) ***(6) Reliance on another financial institution.*** The CIP may include procedures specifying when a bank will rely on the performance by another financial institution (including an affiliate) of any procedures of the bank's CIP, with respect to any customer of the bank that is opening, or has opened, an account or has established a similar formal banking or business relationship with the other financial institution to provide or engage in services, dealings, or other financial transactions, provided that: (i) Such reliance is reasonable under the circumstances; (ii) The other financial institution is subject to a rule implementing 31 U.S.C. 5318(h) and is regulated by a Federal functional regulator; and	Not Addressed	Not Addressed	This project does not demonstrate processes that rely on other Financial Institutions. It's NIST's view that this does not impact on the project's ability to demonstrate the use of mDL to comply with CIP requirements.

CIP Requirement	Demonstrated Capability or Process	Capability Relationship to CIP Requirement	Relationship Explanation
(iii) The other financial institution enters into a contract requiring it to certify annually to the bank that it has implemented its anti-money laundering program, and that it will perform (or its agent will perform) the specified requirements of the bank's CIP.			
(b) Exemptions. The appropriate Federal functional regulator, with the concurrence of the Secretary, may, by order or regulation, exempt any bank or type of account from the requirements of this section. The Federal functional regulator and the Secretary shall consider whether the exemption is consistent with the purposes of the Bank Secrecy Act and with safe and sound banking, and may consider other appropriate factors. The Secretary will make these determinations for any bank or type of account that is not subject to the authority of a Federal functional regulator.	N/A	N/A	This clause is not relevant to the project as it focuses on overall exemptions from CIP compliance.
(c) ***Other requirements unaffected.*** Nothing in this section relieves a bank of its obligation to comply with any other provision in this chapter, including provisions concerning information that must be obtained, verified, or maintained in connection with any account or transaction.	N/A	N/A	This clause is not relevant to the project as it addresses the regulation's impact on other aspects of the regulation.

1359

Appendix D CIP/KYC Documentary Considerations

This appendix summarizes security, privacy, and usability implementation considerations when compared to the following CIP documentation models as defined below:

Non-Documentary - Self-asserted data (e.g. name, address, tax identifier) checked against third party data sources, SMS verification, and email verification.

Government Identification Check - Self-asserted data coupled with software-driven document authentication against an uploaded image of a physical identification card, SMS verification, email verification.

Government Identification Check (Biometric Match) - Self-asserted data coupled with document authentication and a biometric comparison of the user to their presented evidence, SMS verification, email verification.

Government Identification Check (mDL) - Presentation of signed mDL data and local holder authentication, SMS verification, email verification, 3rd party validation of SSN.

1373 **Table 11. Comparative Analysis of CIP Techniques: Security**

		CIP Model			
		Non-Documentary	**Gov ID Check**	**Gov ID Check (Biometric)**	**Gov ID Check (mDL)**
Security Considerations	**Accuracy & Authenticity**	**Low** – manual data entry provides no confidence that attributes are associated with the individual presenting them. There is no ability to confirm the authenticity of any evidence.	**Moderate** – Document analysis provides some confidence in authenticity of a DL.	**Moderate** – Live document capture and liveness biometric comparison provide increased assurance Gov ID is legitimate.	**High** – mDL verification provides means to mitigate risk associated with identity theft or fraudulent account opening by **leveraging cryptographic security features embedded** within the digital credential that can attest to the authenticity and integrity of the information presented.
	User Verification & Binding	**Low** – SMS verification provides minimal binding to the legitimate users and are subject to sim swap, phishing, and account compromise.	**Low** – SMS/Email verification provides minimal binding to the legitimate users. Government ID images can be easily generated using artificial intelligence.	**Moderate** – User verification and binding confidence increases with sufficient presentation attack detection (PAD) controls.	**High** – Authentication to the mobile device through biometrics and other local authentication factors, this an increased degree of confidence that **1) the evidence is real and not forged**, and **2) in the possession of the individual who is represented by the credential**.
	Common Attack Types	- Phishing - Reuse of compromised PII - SIM Swapping - Guessing attacks - Automated & scripted data entry	- Phishing - Reuse of compromised PII - SIM Swapping - Deepfakes	- Deepfakes - Image/Video Injection	Refer to Threats to mDL Verification Environments section.
	Threat Scale	**High** – Attacks have been and will continue to be highly scalable in nature due to automation and minimal ability to verify the end user's identity.	**High** – The quality of generative image AI continues to improve. Scaling attacks become more feasible as the AI compute price decreases.	**Moderate** – An attacker would have to defeat PAD mechanisms, requiring sophistication and/or higher level of resources.	**Low** – Attacks would require a high degree of sophistication in one or more mDL ecosystem pillars – issuance, presentation, and verification.

1374 **Table 12. Comparative Analysis of CIP Techniques: Privacy**

		CIP Model			
		Non-Documentary	**Gov ID Check**	**Gov ID Check (Biometric)**	**Gov ID Check (mDL)**
Privacy Considerations	**Notice & transparency**	**Low** – Customers may not know which third party sources are verifying their data; additionally, risk scoring and fraud management based on user submitted data and transaction data may not be clear to the user and may not have appropriate mechanisms for redress.	**Low** – The customer may consent to the use of their ID in onboarding processes but rarely knows what happens to the data captured of the ID, which parties are processing it, and what happens to unnecessary data captured during the process.	**Moderate** – A customer may not predict how much information is exposed when they share a government ID, vs. how much data is required. Also, a customer may not have visibility into what happens to their biometric data after verification.	**High** – Customers see which specific attributes are requested from their mDL before sharing with the FI, and they maintain a record in their mobile wallet of their transactions for easy review. Biometrics are performed locally on the device and not provided to the FI.
	User control & selective disclosure	**Low** – While customers execute data entry, the accuracy and validation processes are outside of their control. Inaccurate or incomplete data at third party services are not easily corrected and the processes for doing so are outside of user control.	**Low** – Customers have no control over which attributes are shared when images are captured of identity evidence (e.g., driver's license or passport). Even when paired with limited retention and privacy policies, more user attributes are exposed than required for the transaction.	**Low** – Customers lack choice in what data they provide; government ID and selfie are required. They can't control which specific attributes are shared, as they provide entire documents with more information than is required. Their biometric template is typically shared with a 3rd party vendor for review, reducing user	**High** – Individuals only share the specific attributes that are required for identity verification. Biometric verification can be performed locally on the device and not provided to the FI.

		CIP Model			
		Non-Documentary	**Gov ID Check**	**Gov ID Check (Biometric)**	**Gov ID Check (mDL)**
				control over their own biometric data.	
	User verification	**Low** – There is minimal ability to confirm the participating individual is the one represented by the data. Even with SMS verification, which is highly phishable, these approaches leave past victims of PII theft and privacy breaches highly vulnerable.	**Low** – There is minimal ability to confirm the participating individual is the one represented by the data.	**Moderate** – Customers provide biometric data before they're otherwise verified; selfie does add a layer of protection, but there's some risk that the individual in the ID is not the same individual applying for the account.	**High** – Authentication occurs before attributes are sent; local biometric authentication provides user verification.
	Data retention/exposure	**Low** – Since there is no cryptographic signing to support authenticity and accuracy, all data goes to third party data sources for validation. This increases the exposure of customers' personal data. Third parties may have long retention periods for customers' personal data.	**Low** – Since there is no cryptographic signing to support authenticity and accuracy, all data goes to third party data sources for validation. This increases the exposure of customers' personal data. Overcollection of data on the government ID exposes the user to increased risks if images of IDs are	**Low** – Biometric authentication is done server-side (rather than locally)—and typically is done by a third-party vendor, not the financial institution. This biometric matching in a centralized location by a third-party vendor is greater exposure for the customer. It may be unclear what happens to	**High** – Provides the option for local biometric authentication, reducing the amount of data the user sends server-side. Integrity and authenticity of the mDL attributes come from being cryptographic signed, alleviating the need for third party data validation. Only those attributes needed for identity verification are collected.

		CIP Model			
		Non-Documentary	**Gov ID Check**	**Gov ID Check (Biometric)**	**Gov ID Check (mDL)**
			compromised or the proofing services are compromised.	the biometric data after verification.	

1375

1376 **Table 13. Comparative Analysis of CIP Techniques: Usability**

		CIP Model			
		Non-Documentary	**Gov ID Check**	**Gov ID Check (Biometric)**	**Gov ID Check (mDL)**
Usability Considerations	**Effectiveness**	**High** – this method is effective if the third-party data sources are accurate and up-to-date, and customers provide reliable information.	**High** – this method effectively confirms a customer's identity by verifying a physical document.	**Very High** – by combining document verification with biometric liveness checks, this process is a robust and effective.	**Very High** – this method effectively verifies a customer's identity using a secure and standardized digital identity credential.
	Efficiency	**High** – the process is typically fast and efficient, requiring only the customer's input to verify their identity via SMS and email.	**Moderate** - customers must upload a form of Gov ID, which may involve scanning or taking a photo, potentially adding time to the verification process.	**Low to Moderate** – this process requires customers to upload a Gov ID and perform a biometric liveness check, which can complicate and prolong the verification process.	**High** – this process is relatively fast and seamless, as customers can present their mDL digitally.
	Satisfaction	**Moderate** - while the process is convenient, some customers may be skeptical about the security and safety of this method.	**Moderate** - while the process is generally straightforward, some users may struggle with issues related to document quality or formatting.	**Low to Moderate** - while this process is secure, some users may face difficulties with document quality or formatting. Additionally, some may find the biometric liveness check intrusive or encounter technical issues.	**High** - customers with compatible mobile devices and mDLs may find the process both convenient and secure.
	User Experience	The process is familiar to most users and consists of only a few steps. The user experience is usually straightforward. However, some users might be concerned about the lack of tangible verification, which can impact their trust in the method.	The user experience is generally acceptable, but document quality or formatting issues could impact it. Some customers might also be concerned about the security and privacy of uploading sensitive documents.	Issues related to document quality, formatting, and technical challenges during the biometric liveness check could impact the user experience. However, if executed correctly, the process can be both seamless and secure.	The user experience is generally positive, as the process is streamlined and secure. However, users without compatible devices or mDLs, or those not familiar with mDLs, may face difficulties or distrust the process.

		CIP Model			
		Non-Documentary	**Gov ID Check**	**Gov ID Check (Biometric)**	**Gov ID Check (mDL)**
	Summary	Ensuring third-party data sources are accurate and up-to-date is crucial to reduce false negatives or false positives. Clear explanations of the verification process and data protection measures can help alleviate user concerns. Implementing additional verification steps can further enhance security and build user trust.	It's important to make the document upload process user-friendly, with clear guidance on acceptable document types and formats. Ensuring secure transmission and storage of sensitive documents is essential. Feedback mechanisms can help customers resolve upload issues, reducing frustration and potential drop-off.	To ensure a positive user experience, the document upload process and biometric liveness check should be user-friendly with clear instructions. Reducing technical challenges and providing feedback mechanisms can help customers troubleshoot problems, decreasing frustration. Clearly explaining the purpose and benefits of the biometric liveness check can help alleviate user concerns and increase acceptance.	Ensuring compatibility with a range of devices and platforms is crucial. Clear explanations of the benefits and requirements of using mDL verification can also help educate customers and encourage adoption. Providing alternatives for those without compatible devices or mDLs is essential for a positive onboarding experience.

Appendix E List of Symbols, Abbreviations, and Acronyms

AAMVA
American Association of Motor Vehicle Administrators

AAL
Authentication Assurance Level

BSA
Bank Secrecy Act

CIO
Chief Information Officer

CIP
Customer Identification Program

CISO
Chief Information Security Officer

CTAP
Client-to-Authenticator Protocol

DC API
Digital Credentials Web Platform API

DHS
Department of Homeland Security

DOJ
Department of Justice

eCBSV
Electronic Consent Based Social Security Number Verification

FAL
Federation Assurance Level

FI
Financial Institution

FIDO
Fast Identity Online

HTTPS
Hypertext Transfer Protocol Secure

IDMS
Identity Management System

IdP
Identity Provider

IR
Interagency Report or Internal Report

ISO

1415 International Organization for Standardization

1416 JSON
1417 JavaScript Object Notation

1418 JWT
1419 JSON Web Token

1420 KYC
1421 Know Your Customer

1422 KBV
1423 Knowledge-Based Verification

1424 mDL
1425 Mobile Driver's License

1426 mDoc
1427 Mobile Document

1428 MFA
1429 Multi-Factor Authentication

1430 OIDC
1431 OpenID Connect

1432 OpenID4VCI
1433 OpenID for Verifiable Credential Issuance

1434 OpenID4VP
1435 OpenID for Verifiable Presentations

1436 OS
1437 Operating System

1438 OTP
1439 One-Time Passcode

1440 PII
1441 Personally Identifiable Information

1442 POC
1443 Point of Contact

1444 QRC
1445 Quick Response Code

1446 REST
1447 Representational State Transfer

1448 RP
1449 Relying Party

1450 SaaS
1451 Software as a Service

1452 SDO
1453 Standards Development Organization

SP
Special Publication

SSN
Social Security Number

SSO
Single Sign-On

TIN
Taxpayer Identification Number

TLS
Transport Layer Security

URI
Uniform Resource Identifier

VDC
Verifiable Digital Credential

Appendix F DCQL Queries

A DCQL query enables verifiers to signal to wallet the attributes requested by the RP. The wallet can then display to applicants the attributes requested and the credentials on their device that meet the parameters of the request. The figures below contain the DCQL queries used in this demonstration to support the NCCoE Bank's Customer Information Program and account linkage during digital enrollment and reverification. These queries support relying party data minimization by providing a structured means to request only the attributes needed to complete CIP requirements and account linkage. The query also supports consent processes enabling the credential holder to choose whether to share these attributes.

```
"dcql": {
  credentials: [
    {
      id: "mdl",
      format: "mso_mdoc",
      meta: {
        doctype_value: "org.iso.18013.5.1.mDL"
      },
      claims: [
        { path: ["org.iso.18013.5.1", "given_name"] },
        { path: ["org.iso.18013.5.1", "family_name"] },
        { path: ["org.iso.18013.5.1", "birth_date"] },
        { path: ["org.iso.18013.5.1", "issue_date"] },
        { path: ["org.iso.18013.5.1", "expiry_date"] },
        { path: ["org.iso.18013.5.1", "issuing_country"] },
        { path: ["org.iso.18013.5.1", "issuing_authority"] },
        { path: ["org.iso.18013.5.1", "document_number"] },
        { path: ["org.iso.18013.5.1", "portrait"] },
        { path: ["org.iso.18013.5.1", "resident_address"] },
        { path: ["org.iso.18013.5.1", "resident_city"] },
        { path: ["org.iso.18013.5.1", "resident_state"] },
        { path: ["org.iso.18013.5.1", "resident_postal_code"] }
      ]
    }]
}
```

Figure 14. Demonstration CIP DQCL Query

```
"dcql": {
  credentials: [
    {
      id: "mdl",
      format: "mso_mdoc",
      meta: {
        doctype_value: "org.iso.18013.5.1.mDL"
      },
      claims: [
        { path: ["org.iso.18013.5.1", "issuing_authority"] },
        { path: ["org.iso.18013.5.1", "document_number"] }
              ]
    }]
}
```

1478 **Figure 15. Demonstration Account Linkage DQCL Query**