PROJECT DESCRIPTION

ACCELERATE ADOPTION OF DIGITAL IDENTITIES ON MOBILE DEVICES

Identity Management

Ketan Mehta
National Institute of Standards and Technology (NIST)

Arun Vemury
Jon Prisby
Department of Homeland Security (DHS)
Science and Technology Directorate (S&T)

Jeff Finke
MITRE

DRAFT

March 2023

NIST | 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 challenges. Through this collaboration, the NCCoE develops modular, adaptable example cybersecurity solutions demonstrating how to apply standards and best practices by using commercially available technology. To learn more about the NCCoE, visit https://www.nccoe.nist.gov/. To learn more about NIST, visit https://www.nist.gov/.

Over the last two decades, mobile devices have become a commodity technology with users of all economic backgrounds and ages across the globe. These devices have become convenient platforms for many uses, including ordering a ride, making payments, checking in to a flight, accessing the gym, storing concert tickets, etc. More recently, demand has surfaced to use the mobile devices to replace physical identification cards such as government issued driver's licenses with a digital equivalent.

Historic approaches to digital identity have typically leveraged web-based solutions that rely heavily on third party services and techniques to derive an identity from core breeder documents such as driver's licenses and passports. However, with the proliferation of mobile devices, new digital credentials are emerging that can support both greater individual control of identity attributes and more direct validation with issuing sources. This provides the potential for both improved usability and convenience for the end user and stronger assurance in identity for organizations. The advent of international standard ISO/IEC 18013-5, use of mobile driver's licenses (mDL) in attended use cases, ISO/IEC 18013-7 use of mDLs in unattended (online) use cases, are a digital credential model that shows promise.

ABSTRACT

There are several new digital credentials-based standards emerging and they are all silos operating in specific environments and written for specific contexts. And as such, there is a lack of foundational, strongly verifiable, and trustable digital credentials available to make transition to today's mobile device platforms. NCCoE cybersecurity experts will address this challenge through collaboration with Issuing Authorities, digital identity solutions providers, Verifiers (also known as Relying Parties), and third party trust service providers. This effort, based on ISO/IEC 18013-5 and ISO/IEC 18013-7, will enable participants to jointly demonstrate the utility of a robust interoperable reference design that will facilitate the consumption of digital credentials by disparate stakeholders. This effort will also enable more equitable, secure, and convenient commerce along with easier access to government services.

The NCCoE, in cooperation with industry / government agencies / academic institutions, will study, evaluate, implement, and test interoperability and security claims of the international standards, ISO/IEC 18013-5 (published), ISO/IEC 18013-7 (currently a working draft), and the ecosystem surrounding these standards. Specific outcomes of this project will be:

1. an open-source reference implementation for this new technology,
2. prototypes and demonstrations in the lab, and
3. leading practices for secure, resilient and interoperable mDL deployment.

Further there will be an outreach and engagement effort that will champion, socialize and help to spread the word externally with the goal of getting as much involvement as possible.

NOTE: While these standards address the needs of mDLs, most parts of these standards apply to mobile documents (mdoc) and verifiable presentation in general. Accordingly, this effort will include presentation of documents other than mDLs using the mdoc and OpenID for Verifiable Presentation schemes defined in these standards.

KEYWORDS

digital identification; digital identity; digital credential, document presentation; driver's license; mDL; mobile devices

DISCLAIMER

Certain commercial entities, equipment, products, or materials may be identified in this work in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST or NCCoE, nor is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

COMMENTS ON NCCOE DOCUMENTS

Organizations are encouraged to review all draft publications during public comment periods and provide feedback. All publications from NIST's National Cybersecurity Center of Excellence are available at https://www.nccoe.nist.gov/.

Any stakeholder (Issuing Authorities, digital identity solutions providers, Verifiers, and trust service providers) can participate in a fashion that suits them best. Go to https://www.nccoe.nist.gov/projects/mobile-drivers-license for more information and also instructions on how to show intention to collaborate, get involved, and to participate.

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

Public comment period: March 15th, 2023 to March 31st, 2023

The NCCoE will host a virtual workshop for interested parties and stakeholders following the release of this Project Description.

A NOTE TO REVIEWERS

In response with your comments, please indicate if you intend to participate in this project by contributing products and / or use cases. Please indicate if you intend to participate as an Issuing Authority, a digital identity solutions provider, a Verifier, or a third party trust service provider.

This is not a formal call for participation; however, your response will help us in resource planning. Also, note we may not be able to incorporate all demonstrations and use cases but we will start with two use case per scenario on first come first serve basis.

We anticipate opening a formal call for participation through Federal Register Notice (FRN) process by end of April/May this year. Organizations participating in this project should submit their capabilities in response to an open call in the FRN for all sources of relevant capabilities. The respondents will be required to signed a Cooperative Research and Development Agreement (CRADA) to collaborate with NIST in a consortium to build these prototype solution(s).

TABLE OF CONTENTS

1 Executive Summary

Purpose

This document defines an NCCoE project focused on digital identity, for which the NCCoE is seeking feedback. Current digital implementations are incongruent with each other which poses challenges for interoperability and trust across domains and use cases. This project aims to publish leading implementation practices that entities can leverage to plan for their own digital identity goals.

Digital identities are supplementing and supplanting traditional physical identity cards. Customers, consumers of services, law enforcement, vendors, suppliers, businesses, and health care entities may require a method of verifying a person via a mobile device. This is not currently feasible due to the various and different technical implementations currently in place. Other issues plaguing digital identities include:

- Lack of proper guidance and governance for identities on devices
- Lack of awareness or care for protection of PII on mobile devices
- Risky adoptions e.g., self-certified implementations, using unsecure areas (not encrypting) to store and process digital data, etc.

The goal of this project is to define and facilitate a reference architecture(s) for digital identities that protects privacy, is implemented in a secure way, enables equity, is widely adoptable, and easy to use. The NCCoE intends to help accelerate the adoption of the standards, investigate what "works" and "what does not" based upon current efforts being performed by various entities[1], and provide a forum/environment to discuss and resolve challenges in implementing ISO/IEC 18013-5 (attended) and ISO/IEC 18013-7 (unattended / online) standards.

Outcomes of this project could result in contributions to the ISO standards and NIST SP 800-63-4 standard. In addition, this project will also produce an open-source reader reference implementation and provide protypes for mDL and other identity documents implemented on mobile devices by setting up lab demonstrations for both attended and unattended use cases. This project may influence the policy making process as well. Finally, this project will result in a freely available NIST Cybersecurity Practice Guide (NIST 1800 Series document), which can be leveraged by organizations to align their digital identity goals towards a standardized, secured, and trustable digital identity.

Scope

The scope of this project will include developing an implementable reference architecture for the ISO/IEC 18013-5 and ISO/IEC 18013-7 standard, based upon the scenarios detailed below, and provide opportunities for validation of use cases. Also, within scope will be prototyping of

[1] As per the AAMVA mDL website (Jurisdiction Data Maps - American Association of Motor Vehicle Administrators - AAMVA), there are at least 7 States that issue mDLs. There are several suppliers of mdoc (not just mDL) App for both iOS and Android platform. Also, as per DHS website (When will the phased digital ID rollout start? Which airports/states will be first in line for this new technology? | Transportation Security Administration (tsa.gov)), there are at least 12 airports where TSA accepts mDLs.

solutions and the development of leading practices in the form of a NIST 1800 Series Practice Guide.

Note: While mDL is specifically called out in this document, other documents complying with the namespace requirements of ISO/IEC 18013-5 will be accepted and included in this effort.

Assumptions/Challenges

Readers are assumed to know concepts and terms presented in ISO/IEC 18013-5 and ISO/IEC 18013-7.

Participation in this project will be limited to ISO/IEC 18013-5 and ISO/IEC 18013-7 implementations that use Secure Area[2] to protect document Personally Identifiable Information (PII). The requirements for implementations are provided in Section 2.

This project requires as many participants from varying use cases as possible to gain deeper understanding of the needs for digital identity on mobile devices in a given context (for a given use case).

2 Audience and Participation

Figure 1 provides a notional view of an mDL credential lifecycle. As depicted in the figure, the usual sequence of interactions is as follows:

1. In order to receive an mDL credential from the Issuing Authority, the mDL Holder first must download an mdoc App (or a Wallet App) from the App Store. Generally, the Issuing Authority will inform the mDL Holder which App to download. Also, it is possible, as in case of iOS, wallet already exists on the device that supports mdoc functionality.
2. The Issuing Authority identity proofs that mDL Holder and provisions mDL credential to the Holder's mobile device.
3. Over a separate communication channel, the Verifier obtains master list of Issuing Authorities from a trusted third party that will be used to validate Issuing Authority signed objects in mDL credential.
4. Once provisioned, the mDL Holder can present mDL credential to the Verifier (in person or websites) to authenticate themselves to the Verifier to get access to services.

[2] Secure Area is defined as an area on the mobile device that provides additional protection of sensitive mDL related data.

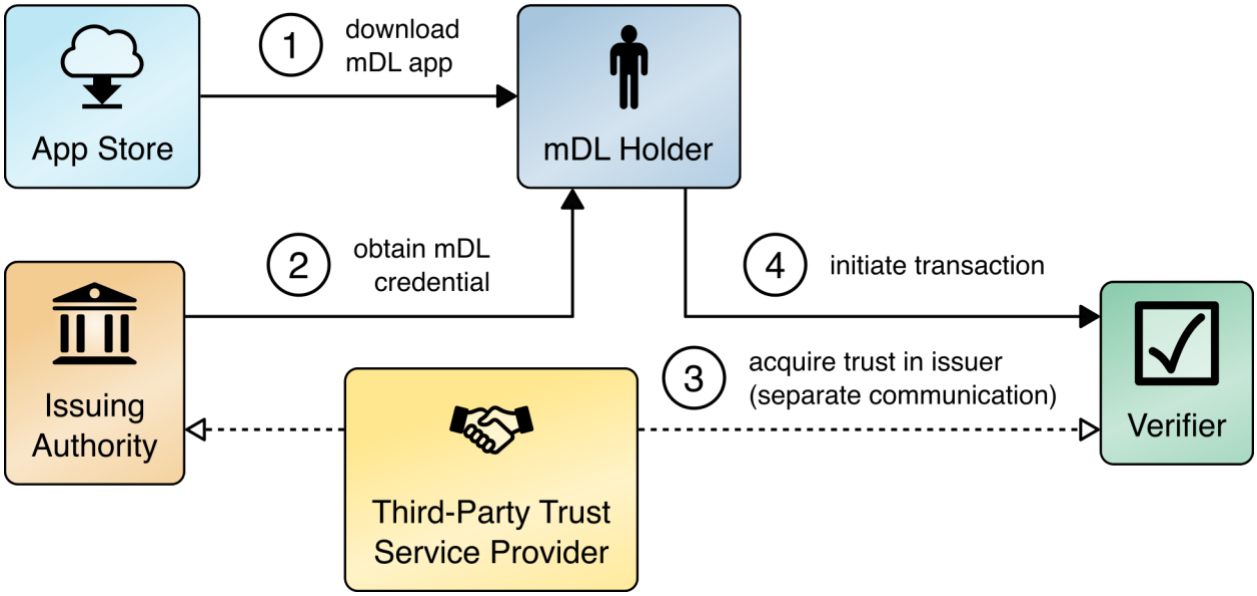

Figure 1: mDL Credential Lifecycle

Stakeholders in mDL Ecosystem

As depicted in Figure 1, the following stakeholders play a role in this process.

mDL Holder-

mDL Holder is an individual to whom the mDL credential is issued and it's that individual's identity.

mDL Issuer (Issuing Authorities)

mDL Issuer is responsible for identity proofing the individual seeking the mDL credential, for provisioning the mDL to the individual's mobile device, and for maintaining the mDL after it is provisioned.

mDL Verifier (Relying Parties)

mDL verifier, also known as a relying party, is an entity that implements an mDL reader and consumes the holder attributes retrieved from the mobile device; this is a service/product provider that mDL Holder is seeking a transaction with.

mdoc App Developer (Technology Providers)

mdoc App developer is an entity that writes software logic necessary to interface with the mDL Issuer and the mDL Verifier systems. The mdoc App developer implements the interfaces defined in ISO/IEC 18013-5 and ISO/IEC 18013-7 so mDL Verifier can retrieve mDL credential interoperably. mdoc App developer also writes software necessary to provision mDL credential to the mobile device, secure the credential on the mobile device, and secure mDL holder authorization to release the credential. mdoc App logic could be implemented in a stand-alone application or in a digital wallet where other documents may also be present.

Third Party Trust Service Providers

The Third Party Trust Service Providers is an entity that provides Verified Issuer Certificate Authority List (VICAL) after the entity performs independent verification and validation of each Issuing Authority and establishes trust in Issuing Authority's issuance process. While optional in the standard, this decentralized PKI trust model requires a mechanism to distribute and disseminate the set of certificates by Issuing Authorities.

Participation

The NCCoE is inviting Issuing Authorities, digital identity solutions providers, verifiers, and third-party trust service providers who implement ISO/IEC 18013-5 and ISO/IEC 18013-7 standards to collaborate and contribute towards building mDL (also other document types) demonstrations in the NCCoE lab. NCCoE plans to build and host up to 10 prototypes / demonstrations on first come first serve basis. Specifically, NCCoE will build and host two demonstrations per Scenario identified in Section 4 to ensure variety of use cases.

Participation is invited from all stakeholders[3] identified in Figure 1. NCCoE expects the following from different stakeholders:

- Verifiers to bring use cases and business processes
  - Verifier web application / service that consumes mDLs, and / or
  - Verifier web application / service that needs NIST mDL reader reference implementation to enable mDL retrieval
- mdoc Apps that meets the minimum requirements as specified below
- Test mDLs from mDL Issuing Authorities
- VICAL from a Third Party Trust Service Providers

The NCCoE plans to develop an open-source reader reference implementation of ISO/IEC 18013-5 and ISO/IEC 18013-7 which can be used as a stand-alone reader or can be integrated into an existing Verifier's web application / service.

The NCCoE anticipates receiving the mdoc App (or wallet) implementations on mobile devices. The minimum requirement for these implementations to be accepted in the demonstration are as follows:

1. Meets the requirements of Authenticator Assurance Level 2 or 3 of [SP 800-63-3].
2. The mobile device provides a Secure Area (e.g., hardware cryptographic module) for security-critical functions that utilizes a FIPS 140 validated cryptographic module.
3. The mdoc App uses that Secure Area to protect mdoc keys and holder attributes.
4. The device signing key pair is generated in the Secure Area of the device and the private key is non-exportable.

[3] mDL User, real life entity, may participate in this project by using their State issued mDL to interact with demonstrations.

5. Holder attributes are protected in the Secure Area or are stored encrypted outside Secure Area but the encryption key pair is generated in the Secure Area and the private key is non-exportable.
6. The mDL/mdoc, including the device signature key and holder attributes, remains locked or inaccessible until entry of the correct activation secret or presentation of a biometric factor.
7. The mdoc App implements trust framework to support Reader Authentication / Reader Verification
8. The mdoc App protects holder attribute privacy by protecting against user tracking, supporting selective disclosure of identity attributes, and ensuring user consent prior to release.

3 Project Plan and Timeline

The below figure is a draft tentative plan and timeline subject to change.

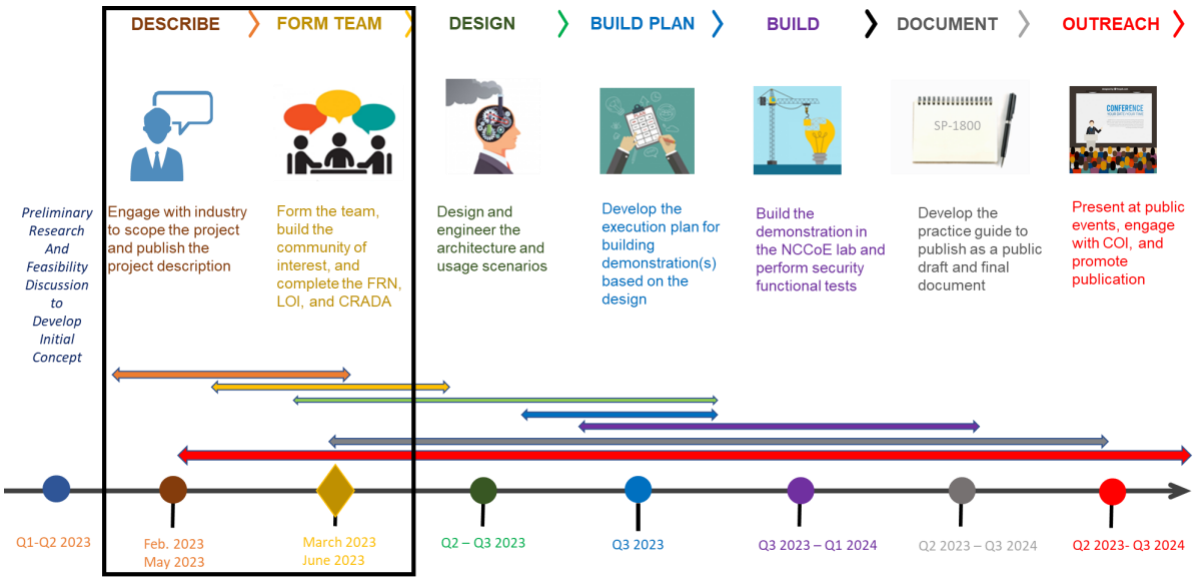

Figure 2: Tentative Project Timeline

An overall timeline can be distilled into three phases.

1. Define: Collaborate with the industry to define scope of work. Members of the community are invited to talk about their challenges, ask questions, and listen - to understand the challenge at hand. During this phase, a draft project description for public comment is published. The comments are adjudicated, and a final version is published to the NCCoE website that outlines purpose, scope of work, and the process.
2. Assemble: Teams of industry organizations, government agencies, and academic institutions are assembled to address all aspects of the project at hand. A Federal Register Notice is published to announce the opportunity to collaborate and explain what capabilities the NCCoE is looking for. Potential collaborators respond with a completed Letter of Interest (LOI). Submitted LOIs are accepted on a first-come basis. When the collaborators join the build team, they sign a Cooperative Research and

Development Agreement (CRADA) to provide their commercially-available product and their expertise. All the work is open, transparent, publicly accessible, and informed by both the general public and technology providers.

3. Build: A practical, usable, repeatable modules / prototypes to address the cybersecurity challenge is built. During this phase, a reference architecture is finalized. The collaborators provide support to install and configure their technologies and then they provide support throughout the build to address issues, such as security, privacy, and interoperability.

4 Scenarios (Transaction Types)

Scenarios are high level transaction types while use cases are specific uses of an mDL within an industry. The NCCoE is looking to receive possible use cases that will be organized into the appropriate scenario categories. At this juncture there are five scenario categories described below.

The ISO/IEC 18013-5 standard makes it possible to present an mDL to a Verifier in attended use cases. The ISO/IEC 18013-7 specification makes it possible to present an mDL to a Verifier over the internet to the websites (unattended use case). Considering there are all kinds of use cases and possibilities, there is no limit to how the mDL could be used. As shown in Figure 2, mDL Holder Transactions, once an mDL is issued, the same mDL could be used in different ways with a different Verifier as needed for specific use cases. Since the possibilities are too many, this NCCoE project will focus on at least one or two use case demonstrations from the following five categories of Scenarios.

Note: Categories may shift during the project if new use cases are presented that do not fall under any of the following categories.

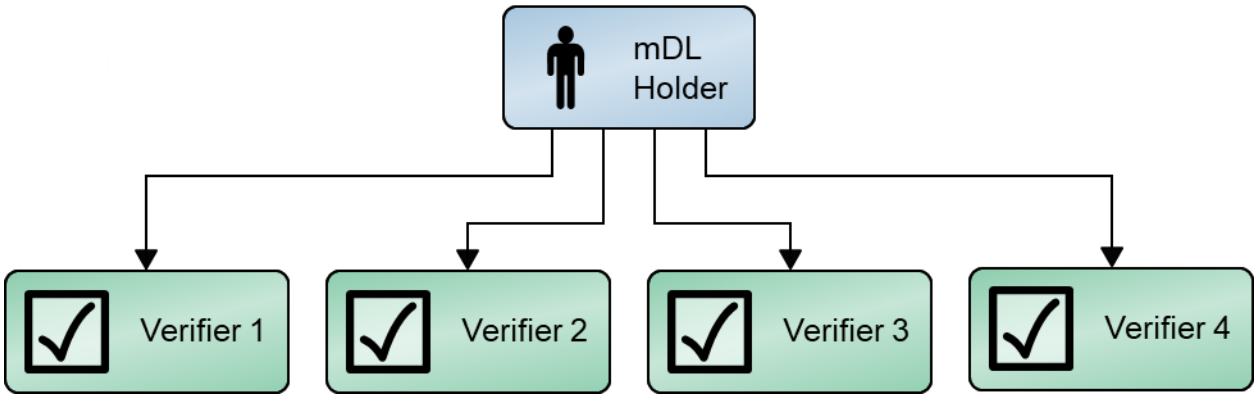

Figure 3: mDL Holder Transactions

The plan for this project is to investigate the use of mDL and other mobile documents in following categories of scenarios:

Scenario 1: Attended Use Cases

This involves a user "providing" their mDL via a mobile device. Could be as simple as producing or showing the QR code or tagging the reader device and approving holder attributes being requested. These are fairly straight forward and therefore the emphasis will be on the more complicated unattended use cases.

For example, the mDL reader of a Law Enforcement Officer (LEO) and the mDL of a holder are exchanged and authenticated at proximate distance. In this scenario, a session is created in which the mDL reader of the LEO attests that the LEO is empowered to perform traffic stops and requests that the holder submit an mDL that may be authenticated. Upon successful authentication of the LEO by the holder, the mDL is exchanged enabling the LEO to authenticate the Driver of the vehicle.

Scenario 2: Un-Attended Use Cases (Identity Proofing)

mDL is used as evidence (validated source of attributes) in the identity proofing process. In this case, the attributes are retrieved from an mDL to verify real-life identity and associate it to a unique account in the Issuing Authority's system. For instance, the mDL is consumed by an identity provider who upon successful identity proofing would issue another credential relevant to the application.

Scenario 3: Un-Attended Use Cases (Attribute Presentation)

An mDL is used to present Holder's attributes to access a Verifier's online service (one time event). For example, an mDL is used to purchase alcohol online. Or an mDL is used to present identity attributes for access to government benefits (e.g., prove state residency). There is no account creation or account linking in this scenario.

Scenario 4: Un-Attended Use Cases (Authentication)

mDL is used as an authenticator to recursively access a Verifier's services where an account is setup and transaction linking[4] is required. This case covers both scenarios where there may be an existing account and the mDL is registered as an authenticator or there is no existing account, but an account is created, and the mDL is registered as an authenticator to that new account. For example, an mDL is used to initially authenticate an individual when purchasing an airline ticket and subsequently used to authenticate that individual when traveling under that ticket and signing into TSA to update trusted travel status.

The mDL of a pilot is mutually authenticated to a smart device (car, drone, plane, IoT system) that can mutually authenticate and determine appropriate access. This may be done in proximity or online depending on what is being operated and how it is being operated, i.e., drones can be operated at great distance as well as in line of sight.

Scenario 5: Un-Attended Use Cases (Single Sign-on)

An mDL is used in a single sign on (SSO) event. In this scenario, upon successful authentication by the holder, a session is established for the holder in a network which enables the account holder access to several services, such as email, login to server, local application(s), etc.

The investigation will examine data fidelity in terms of minimum validated data required. In all the scenarios above, there will be situations where a user will only need to provide a very

[4] There are use cases where a mDL Holder may need to make two or more atomic transactions using the same mDL in order to complete one transaction.

limited set of information (least required), for example, purchasing controlled substances (e.g., alcohol, tobacco) and only needs to provide their portrait and binary age 21 or below 21. Another example is a user proving they live within a certain area, incorporated limit and/or precinct—they would provide name, address and portrait; or a case where a user just provides a piece of biometric information and nothing else.

APPENDIX A REFERENCES

[1] ISO/IEC 18013-5, *Cards and security devices for personal identification – ISO-Compliant Driving Licence*

[2] ISO/IEC 18013-7, *Cards and security devices for personal identification – ISO-Compliant Driving Licence – Add On Functions*

[3] NIST. SP 800-63-3 *Digital Identity Guidelines*. Available: NIST SP 800-63 Digital Identity Guidelines.

APPENDIX B ACRONYMS AND ABBREVIATIONS

CoI	Community of Interest
DHS	Department of Homeland Security
LEO	Law Enforcement Officer
mDL	Mobile Driver's License
mdoc	Mobile Documents
NCCoE	National Cybersecurity Center of Excellence
NIST	National Institute of Standards and Technology
O&E	Outreach and Engagement
SP	Special Publication
SSO	Single Sign On
VICAL	Verified Issuer Certificate Authority List