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 (S&T)

Jeff Finke
MITRE

Final
Revision 1

June 2023

mdl-nccoe@nist.gov

This revision incorporates comments from the public.

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 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 standards ISO/IEC 18013-5, use of mobile driver's licenses (mDLs) in attended[1] use cases, and ISO/IEC 18013-7, use of mDLs in unattended[2] (e.g., over-the-internet) use cases, is a digital credential model that shows promise.

While this project is centered on mDLs defined in ISO/IEC 18013-5, the concepts explored in this project will be extended to any credentialed Identity such as federal government issued credentials for agency employees or program beneficiaries, corporate credentials, travel credentials, health credentials, etc.

Abstract

There are several new digital credentials-based standards emerging and they are all silos operating in specific environments and written for specific contexts. 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 will enable participants to jointly demonstrate how solutions based on ISO/IEC 18013-5 and ISO/IEC 18013-7 can address specific real-world transactions, by disparate stakeholders, requiring digital identity. 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

[1] Attended use case is a transaction where the mDL holder and the mDL verifier are in close proximity to each other.

[2] Unattended use case is a transaction where the mDL holder and the mDL verifier are not in close proximity.

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 reader reference implementation
2. Demonstrations of mDL use cases
3. Practice guide for implementing mDLs

Furthermore, there will be an Outreach and Engagement (O&E) effort that will champion, socialize, and help to spread the word externally with the goal of getting as much involvement as possible.

Keywords

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

Acknowledgements

The NCCoE would like to thank the following individuals for their discussions and insights during the development of this project description: William Fisher, Ryan Galluzzo, Connie LaSalle, and Andy Regenscheid.

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

Commenting period for this project description is over. However, organizations are encouraged to review future 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/.

Table of Contents

1 EXECUTIVE SUMMARY

Purpose

This document defines an NCCoE project focused on accelerating the adoption of digital identity on mobile devices, specifically Mobile Driver's Licenses (mDL) and mobile documents (mdocs[3]), for which the NCCoE is seeking collaborators.

Challenge

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. If these digital identities on mobile devices are to meet the demands of varying use cases, there must be technological interoperability, security, and cross-domain trust. The nascent nature of this technology leaves many challenges to be addressed, including but not limited to:

- Lack of guidance and governance for identities on devices
- Limited capability to evaluate and validate compliant, standards-based deployments
- Limited understanding of the privacy and usability considerations

Goal

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 concepts of cybersecurity, privacy, and adoptability are critically important to this overall effort and will be interweaved into the work of this project from the beginning. The NCCoE intends to help accelerate the adoption of standards, investigate what "works" and "what does not" based upon current efforts being performed by various entities[4], and provide a forum/environment to discuss and resolve challenges in implementing ISO/IEC 18013-5 (attended) and ISO/IEC 18013-7 (over-the-internet) standards.

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 transaction types detailed below, and provide opportunities for validation of use cases. This effort may also consider other relevant standards-based initiative around W3C's Mobile Document Request API (GitHub - WICG/mobile-document-request-api) for mdoc presentation.

Specific outcomes of this project will be:

1. **Open-Source Reader Reference Implementation** – This will be a freely available tool for testing and evaluating compliance of mDL implementations with international standards

[3] An mdoc is a document or application that is stored on a mobile device or requires a mobile device in order to gain access to the document or data contained within the document/application.

[4] 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 mDL apps for both iOS and Android platforms. 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.

and will be used as part of the demonstration efforts to confirm interoperability of mDL and mdoc applications for use in the lab.

2. **Demonstrations of mDL Use Cases** – These will demonstrate end-to-end uses of mDL in attended and over-the-internet use cases. This will include multiple parties such as issuers of mDL, mdoc application providers, digital identity service providers, and verifiers (aka, relying parties) that consumes mDL, all collaborating to bring practical uses to life.
3. **Practice Guide** – This will capture the lessons of the demonstrations to provide a usable guide for implementing mDLs in attended and over-the-internet scenarios. This will include design, architecture, integration information inclusive of leading practices for security, usability, and privacy based on the work conducted with our collaborators.

While these standards address the needs of mDLs, most parts of these standards apply to mdoc in general. Accordingly, this effort will include presentation of documents other than mDLs using mdoc data model, see Figure 2 of ISO/IEC 18013-5.

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[5] to protect document Personally Identifiable Information (PII). The requirements for implementations are provided in Section 2.

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

2 mDL Ecosystem and Participation

mDL Ecosystem

Figure 1 provides a notional view of an mDL credential lifecycle. Other topologies that provide equivalent or better mDL data security will be considered. 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 must already have an mdoc App (or a Wallet App) on their device. Generally, the Issuing Authority will inform the mDL Holder which App or Apps they may use. The App could have been pre-installed on the device out-of-the-box (OOB), or could have been installed after market, for example from an app store or by mobile device management (MDM).
2. The Issuing Authority identity proofs the mDL Holder and provisions the mDL credential to the Holder's mobile device.
3. Over a separate communication channel, the Verifier obtains the master list of Issuing Authorities from a trusted third party that will be used to validate Issuing Authority signed objects in the mDL credential.

[5] Secure Area is defined as an area that provides additional protection of sensitive mDL related data.

4. Once provisioned, the mDL Holder can present the mDL credential to the Verifier (in person or websites) to authenticate themselves to the Verifier to get access to services.

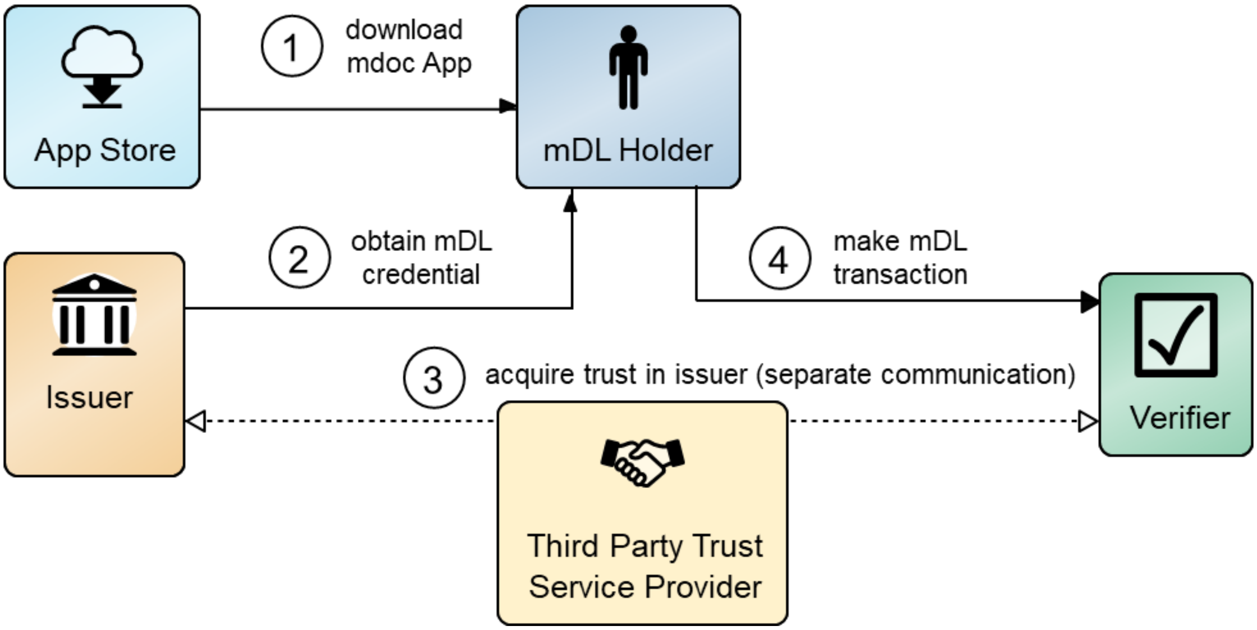

Figure 1: mDL Credential Lifecycle

Stakeholders in mDL Ecosystem

As depicted in Figure 1, the following stakeholders play a role in the mDL ecosystem.

mdoc App Developer

The mdoc App developer is an entity that writes software logic necessary to interface with the Issuer and the Verifier systems. The mdoc App developer implements the interfaces defined in ISO/IEC 18013-5 and ISO/IEC 18013-7, so Verifiers can interoperate with Issuers when retrieving mDL credentials. mdoc App developers also write 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.

mDL

An mDL is a driver's license that is provisioned to a mobile device with the capability to be updated in real time. It is comprised of the same data elements that are used to produce a physical driver's license; however, the data is transmitted electronically to a Verifier's reader device and authenticated. An mDL represents the identity of the mDL holder.

mDL Holder

The mDL Holder is an individual to whom the mDL credential is issued. This individual must be identity proofed to determine if they are who they claim to be.

Issuer

An Issuer is an entity that issues the mDLs or mobile documents. Issuer is responsible for identity proofing the individual seeking the mDL, for provisioning the mDL to the individual's mobile device, and for maintaining the mDL lifecycle after it is provisioned.

Verifier

The Verifier, aka Relying Party, is an entity that consumes mDLs for access and eligibility decision to provide services to the mDL Holder. The Verifier implements an mDL reader and consumes the mDL holder attributes retrieved from the mobile device; this is a service/product provider that the mDL Holder is seeking a transaction with.

While Verifier in Figure 1 is depicted as a single participant, real world implementations will likely require the participation of multiple collaborators or types of entities to support a complete use case or a business process.

Third Party Trust Service Providers

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

Participation in the NCCoE Project

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 a first come first serve basis. Specifically, NCCoE will build and host two demonstrations per Transaction Types identified in Section 4 to ensure variety of use cases. NCCoE encourages—but does not limit—participation from the following types of entities:

Table 1 Project Participants

Collaborator Type	Contributions
mDL and mdoc Application Providers	This project builds off the critical work already accomplished to provide standards-based credentials. We seek collaborators who can bring compliant credentials, wallets, and applications to our use cases.
State DMVs and other Issuing Sources	To act as our issuing authorities and provide identities that can support our use cases and implementation efforts.
State, Local, and Federal Benefits Programs	To act as verifiers and to provide business process and workflows for consuming mDLs. Participation from such parties will make sure that our practice guide will reflect end-to-end considerations

Collaborator Type	Contributions
	including how to practically integrate with benefits programs.
Online Retail and Commercial Services	To act as verifiers and to provide business process and workflows for consuming mDLs. Participation from such parties will make sure that our practice guide will reflect end-to-end considerations including how to practically integrate with retail and commercial processes.
Identity Providers, Credential Service Providers, Identity Management Software and Identity As A Service Providers (IDaaS)	To bring to bear existing identity infrastructure and processes to integrate with an mDL-enable issuer applications or verifier applications to issue mDLs and / or to support consumption of mDLs.
Third Party Trust Services	To provide VICAL and underlying trust capabilities that can support our identified use cases and demonstrate real-world, practical implementations.
Mobile Device and OS Providers	To provide platform-level security capabilities for mDL applications and standards-based mechanisms for mDL conveyance and consumption.

Expectation from Participants

NCCoE expects the following from different stakeholders:

- Verifiers are to bring use cases and business processes with use cases that
  - Already support mDL / mdoc functionality,
  - Be willing to work and integrate with other participants that provide mDL / mdoc related infrastructure, products, and services to mDL-enable / mdoc-enable their use case, or
  - Be willing to integrate NIST open-source reader reference implementation to mDL-enable / mdoc-enable their use case.
- mDL / mdoc Apps that meet the minimum requirements as specified below
- Test mDLs / mdocs from mDL / mdoc Issuers
- VICAL from a Third-Party Trust Service Providers

mdoc App Qualifications

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.
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 a 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.

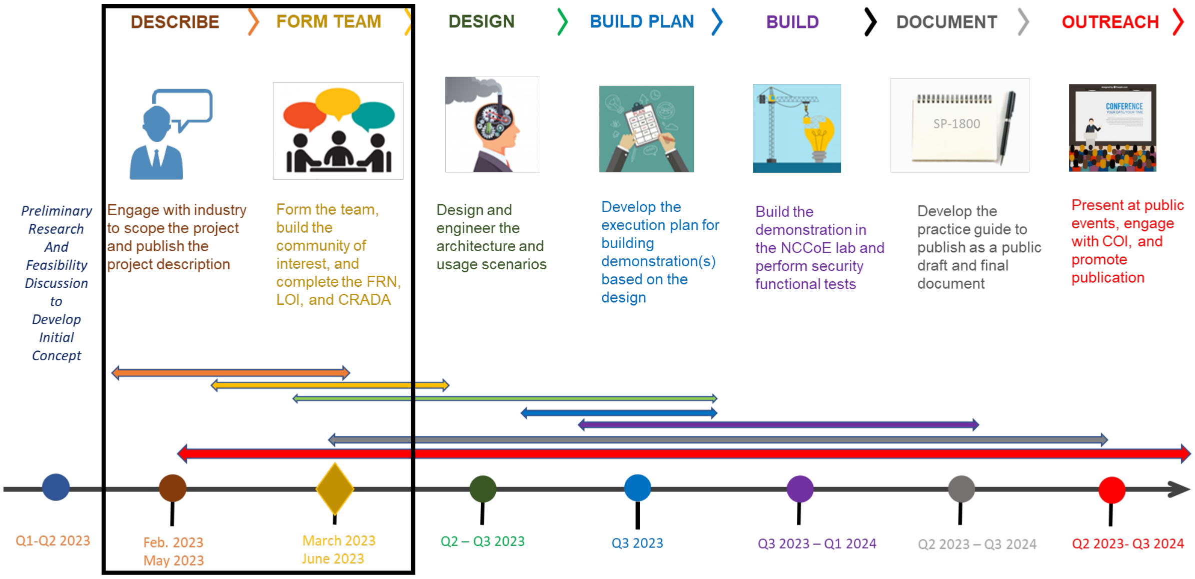
DESCRIBE
FORM TEAM
DESIGN
BUILD PLAN
BUILD
DOCUMENT
OUTREACH
SP-1800
CONFERENCE
Preliminary Research And Feasibility Discussion to Develop Initial Concept
Engage with industry to scope the project and publish the project description
Form the team, build the community of interest, and complete the FRN, LOI, and CRADA
Design and engineer the architecture and usage scenarios
Develop the execution plan for building demonstration(s) based on the design
Build the demonstration in the NCCoE lab and perform security functional tests
Develop the practice guide to publish as a public draft and final document
Present at public events, engage with COI, and promote publication
Q1-Q2 2023
Feb. 2023
May 2023
March 2023
June 2023
Q2 – Q3 2023
Q3 2023
Q3 2023 – Q1 2024
Q2 2023 – Q3 2024
Q2 2023- Q3 2024

Figure 2: Tentative Project Timeline

How the NCCoE Works/Steps Taken

An overall timeline can be summarized into three phases.

1. **Define:** Collaborate with the industry to define the 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:** Practical, usable, repeatable modules / prototypes to address the cybersecurity challenge are 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 MDOC Transaction Types

The NCCoE is looking to receive use cases from Verifiers that will be organized into the appropriate transaction types defined in this section. At this juncture, there are five transaction types as described below.

NCCoE experts will work with the participants to build up to 10 demonstrations of selected use cases. Up to two use cases will be selected per transaction type such that the first use case demonstrates use of mDL and the second use case would preferably add a demonstration of other document(s) as proposed by the participant. Our goal would be that each demonstration will demonstrate something unique or different from the other, as shown in Figure 3.

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

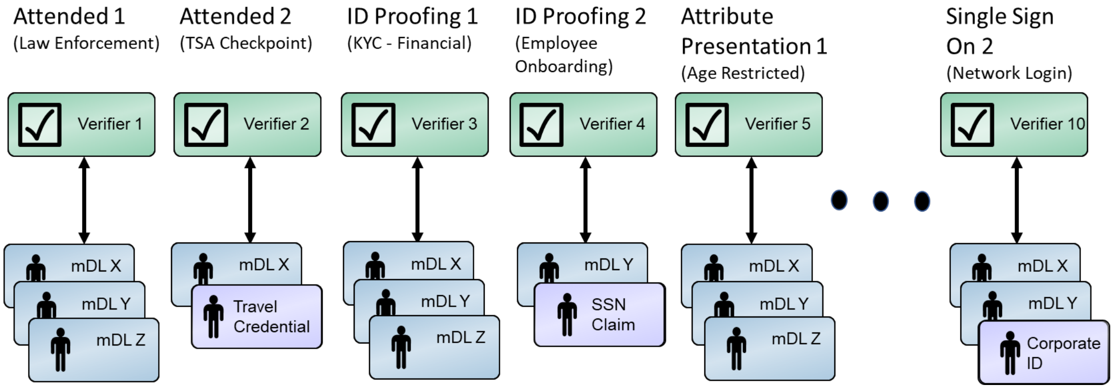

Figure 3: mdoc Demonstration Examples

The plan for this project is to investigate the use of mDL and other mobile documents in the following five transaction types.

Transaction Type 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 a 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.

Transaction Type 2: Remote Identity Proofing

An 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.

Transaction Type 3: Attribute Presentation

An mDL is used to present a 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.

Transaction Type 4: Authentication to a website

An mDL is used as an authenticator to recursively access a Verifier's services where an account is setup and transaction linking[6] 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 the Transportation Security Administration (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 within line of sight.

Transaction Type 5: 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 also consider the minimum validated data elements required in each scenario. In all the scenarios above, there will be situations where a user will only need to

[6] 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.

provide a very limited set of information (least required). For example, purchasing controlled substances (e.g., alcohol, tobacco) and only needs to provide their portrait and binary information about age, whether it's greater than or equal to the drinking age, or if it's below the drinking age. 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 presents 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 License*

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

API	Application Programming Interface
CoI	Community of Interest
DHS	Department of Homeland Security
IAM	Identity and Access Management
IDaas	Identity-as-a-service
LEO	Law Enforcement Officer
mDL	Mobile Driver's License
MDM	Mobile Device Management
Mdoc	Mobile Documents
NCCoE	National Cybersecurity Center of Excellence
NIST	National Institute of Standards and Technology
OOB	Out Of the Box
O&E	Outreach and Engagement
PACS	Physical Access Control System
PKI	Public Key Infrastructure
SP	Special Publication
SSO	Single Sign On
TSA	Transportation Security Administration
VICAL	Verified Issuer Certificate Authority List
W3C	The World Wide Web Consortium