Mobile Driver's License (mDL) Opportunities in Federal Personal Identity Verification (PIV) Issuance (DHS)

Identifying Opportunities to Streamline the PIV Issuance Process Using Mobile Driver's Licenses (mDLs) for DHS Stakeholders

Science and Technology

04-2024

OVERVIEW

A Mobile Driver's License (mDL) is a digital representation of a physical driver's license provisioned to a mobile device. This new form of digital identity is gaining traction across the nation, though implementation varies by state. As mDL usage continues to grow, the Department of Homeland Security (DHS) has an emerging opportunity to streamline the federal PIV issuance processes for mDL use in identity validation.

Per Homeland Security Presidential directive (HSPD) 12, all federal agencies utilize a common format of access cards for access provisioning and identity validation. DHS refers to these cards as personal identity verification (PIV) cards. For more information, see https://www.dhs.gov/homeland-security-presidential-directive-12.

Sample PIV Card

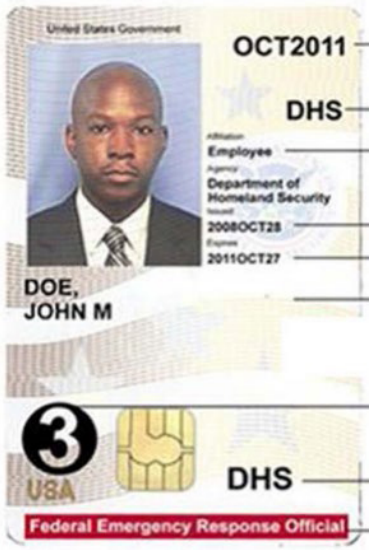

Photo of sample PIV card, based on an image in DHS PIC Credential Issuers (PCI) Operations Plan, version 4, dated February 2014

Photo Source: Department of Homeland Security, Office of Inspector General (OIG)

PURPOSE OF THIS DOCUMENT

This document highlights the DHS PIV issuance process as a use case which can potentially benefit from mDLs.
View 1 provides an overview of the current state of the end-to-end DHS PIV issuance process and suggests potential mDL solutions and impacts.
View 2 elaborates on the potential use of mDLs people, process, technology, and cross-cutting considerations.

Layout – View 1 (PIV Issuance – mDL Opportunities)

- **Current State:** A high-level depiction of the existing DHS PIV issuance process.
- **Potential mDL solutions:** Description and visual representation of potential mDL solutions to streamline the DHS PIV issuance processes.
- **Impacts:** Description of the improvements that would result from implementing the potential mDL solution.

Layout – View 2 (mDL Implementation Considerations)

- **People & Process Considerations:** List of people and process considerations that would need to be addressed to implement the potential mDL solution.
- **Technology Considerations:** List of technology considerations that would need to be addressed to implement the potential mDL solution.
- **Cross-Cutting:** List of overarching considerations that would need to be addressed to implement the potential mDL solution.

Assumptions

The mDL issuers and verifiers will follow the standards, guidelines, and regulations identified below.

Standards, Guidelines, and Regulations

- ISO/IEC 18013-5: Mobile Driving License application
- ISO/IEC 18013-7: Mobile Driving License add-on functions
- AAMVA Mobile Driver's License Implementation Guidelines
- NIST SP 800-63-3 Digital Identity Guidelines
- Homeland Security Presidential Directive 12: Policy for a Common Identification Standard for Federal Employees and Contractors

Limitations

- ISO standards for unattended use cases (ISO/IEC 18013-7) are currently under development.
- Some variations and nuances may exist in PIV issuance processes between DHS Headquarters (HQ) and DHS components. This document generalizes common PIV issuance processes (across the people, process, and technologies involved).

View 1: PIV Issuance – mDL Opportunities

STAGES	Personnel Security and Suitability Process	PIV Issuance Process
CURRENT STATE PIV ISSUANCE PROCESS (DHS)	In this stage, information is collected from an applicant to obtain DHS Suitability.	In this stage, biographic and biometric information is collected from applicant to be issued a DHS PIV card.
POTENTIAL MDL SOLUTIONS	Include option for PIV applicants to share mDL data as part of the PIV Card request process to create a non-PIV identity record. Auto populate information by accessing external databases (e.g., state) using the mDL to authenticate and authorize.	Include option for PIV applicants to present mDL as an identity source during in-person PIV card/badge issuance appointments to meet the requirements of strong evidence as defined by NIST SP 800-63-3. Supervised remote proofing may be considered by having staff provide live video assistance.

CURRENT STATE – PIV ISSUANCE PROCESS (DHS)

Application Form and e-Qip:
- Identity (e.g., Name, Date of Birth, Social Security Number)
- Employment Details (e.g., job title, department, agency)

Identity Documents, Including:
- Primary Evidence (e.g., Unexpired U.S. Passport), OR
- Combination of secondary evidence (e.g., driver's license, Social Security Card)

Biometrics (e.g., fingerprinting)

→ **Submit Investigation Request**

→ **DHS Personnel Security (PERSEC) or Component PERSEC submit checks** (e.g., criminal, financial)

→ **Authorized investigative service provider** (e.g., FBI, DHS Automated Biometric Identification System (IDENT))

→ **DHS HQ/ DHS component**

→ **DHS HQ/ DHS component**

→ **Accepts applicant for Entry on Duty (EOD)**

OR

Denies applicant for EOD

→ **Accept applicant – suitability granted**

OR

Deny applicant – applicant removed

Provide identity documents and biometrics (fingerprint and photo) in person at an approved DHS PIV Card Issuance Facility (PCIF)

↓

Inspect visually and/or using technology *(e.g., scanners, UV light devices)*

↓

DHS HQ/DHS component

↓

Verify & authenticate identify and issue PIV card

OR

Reject identity and do not issue PIV card

POTENTIAL MDL SOLUTIONS

Additional PII (not stored on mDL):
- Personal Identifiable Information (PII)
- Email address
- Social Security Number (SSN)

→

Issuing Department / Agency Security Office – PIV Card Request System

↕

External Databases (e.g., State Level Department of Motor Vehicles (DMV))

Two Forms of Identity (e.g., mDL, driver's license, passport)

Fingerprints and photograph

→

IF PIV REGISTRATION PROCESS IS DONE IN PERSON:

Scanned/collected by staff using mDL reader

Scanned/collected by kiosk

IF PIV REGISTRATION PROCESS USES SUPERVISED REMOTE PROOFING:

Supervised remote proofing using live video assistance

→

Verify, authenticate, & issue PIV card

Reject identity and do not issue PIV card

IMPACTS

- **Reduce Fraud, Human Error, and Data Collection:** Through cryptographic validation mechanisms (e.g., using an mDL reader) versus potentially having human errors when visually inspecting a physical license and comparing the identity documents with the applicants.
- **Increase Privacy:** mDL transactions are privacy-preserving by default versus scanning physical license.
- **Flexible Enrollment Schedules:** Applicant can show up without appointment outside of business hours.

Please note: The issuing department/agency may leverage one or more of the listed identity proofing procedures.

Science and Technology

View 2: mDL Implementation Considerations

STAGES	Personnel Security and Suitability Process	PIV Issuance Process
POTENTIAL MDL SOLUTION	Include option for PIV applicants to share mDL data as part of the PIV Card request process to create a non-PIV identity record. Auto populate information by accessing external databases (e.g., state) using the mDL to authenticate and authorize. **Additional PII (not stored on mDL):** · PII · Email address · SSN **Issuing Department / Agency Security Office – PIV Card Request System** **External Databases** (e.g., State Level Department of Motor Vehicles (DMV))	Include option for PIV applicants to present mDL as an identity source during in-person PIV card/badge issuance appointments to meet the requirements of strong evidence as defined by NIST SP 800-63-3. Supervised remote proofing may be considered by having staff provide live video assistance. **Two Forms of Identity** (e.g., mDL, driver's license, passport) **Fingerprints and photograph** **IF PIV REGISTRATION PROCESS IS DONE IN PERSON:** **Scanned/collected by staff using mDL reader** **Scanned/collected by kiosk** **IF PIV REGISTRATION PROCESS USES SUPERVISED REMOTE PROOFING:** **Supervised remote proofing using live video assistance** **Verify, authenticate, & issue PIV card** **Reject identity and do not issue PIV card**
PEOPLE & PROCESS	**Communications and Outreach:** Advertise and provide a user's guide for PIV applicants to understand how to use an mDL as part of the PIV card request and prescreening process. **Fraud Detection:** Ensure that analysis tools capture critical mDL validation events per best practices.	**Training:** Train staff that are operating in-person kiosks/proofing system on how to cryptographically validate an mDL using a scanner (not just a visual inspection) and how to provide technical support to PIV applicants in-person and/or remotely. **Centralized Staffing:** Consider centralizing the overall number of staff in in-person and remote scenarios.
TECH	**Interface:** mDL validation will require interfacing with external databases to authenticate the PIV applicant's identity and automatically populate information in applicable DHS database. **Biometrics:** PIV applicant should use their biometrics to unlock their wallet to deliver the mDL as evidence of the validity of the mDL.	**Kiosk:** Operators must ensure that there is connectivity to support two-way video as well as the physical security of the kiosk and the network the kiosk uses to connect to the remote agent for remote supervised proofing. **mDL Scanners:** There are multiple technologies supported by various mDL wallet implementations. The choice(s) for the mDL scanner built into a kiosk will be driven by which technology or technologies are supported by wallets in the state where the kiosk is deployed.

CROSS – CUTTING

Standards: ISO 18013-7 is still in committee. How that standard works will impact the technical implementation for mDL to web browser validation of remote proofing.

Technical Support: DHS HQ and DHS Operational Components will need to provide technical support to applicants who have trouble using their mDL and wallet. Technical support will vary depending on the mDL implementation (e.g., in-person proofing versus supervised remote proofing).

Data Privacy and Security: mDL standards were created with privacy-preserving considerations capabilities, but the implementation is decided by the validator based on the use case. Whether online or offline mDL interactions are supported, it is critical that implementations validate in alignment with best practices.

Engage with Us

@dhsscitech

dhs.gov/scitech

Technologically Speaking Podcast

Science and Technology