

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

For a Federal Agency

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



Science and
Technology

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 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

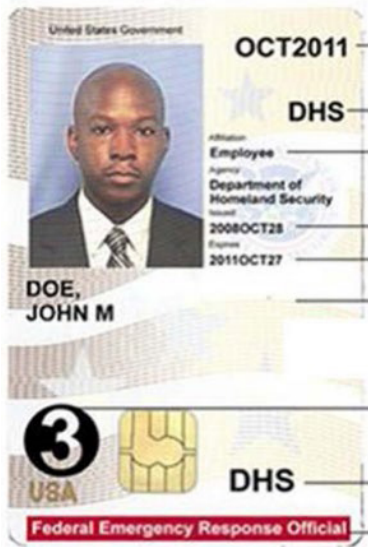


Photo of sample PIV card, based on an image in DHS PIC Credential Issuers (PCI) Operations Plan, version 4, dated February 2014

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



PURPOSE OF THIS DOCUMENT



This document highlights the federal PIV issuance process as a use case that can potentially benefit from mDLs. This is a high-level, conceptual depiction of the federal HSPD-12 issuance processes generally, abstracted from the HSPD-12 issuance processes of multiple federal agencies, and meant to broadly outline the situation for any federal agency.

View 1 provides an overview of the current state of the end-to-end federal 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 Federal PIV issuance process.



Potential mDL solutions: Description and visual representation of potential mDL solutions to streamline federal 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.

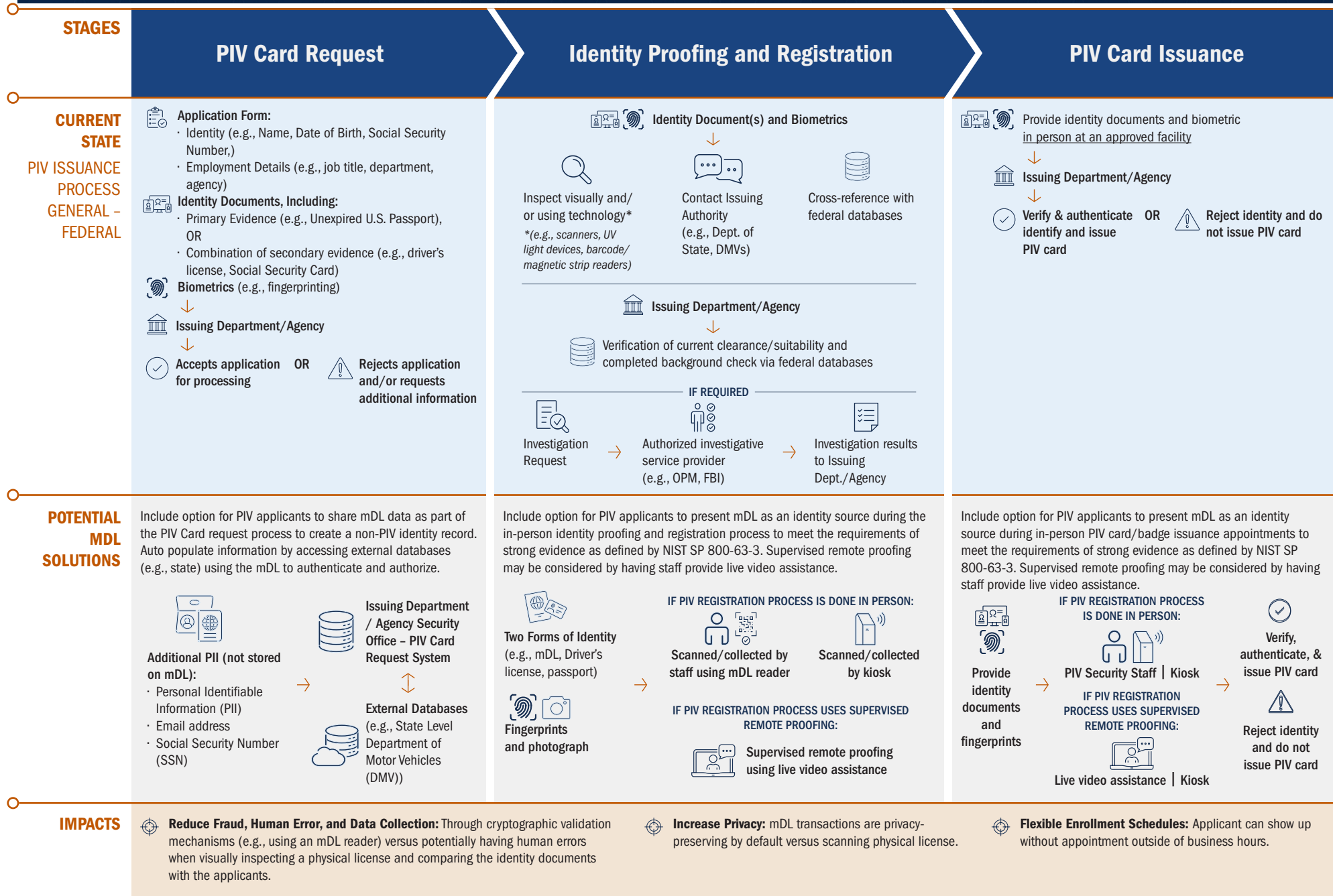
Standards, Guidelines, and Regulations

- 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

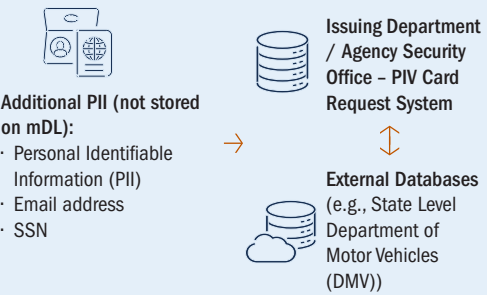
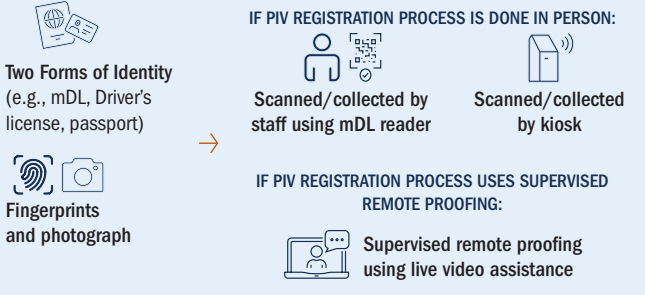

Limitations

- 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 federal departments and agencies. This document generalizes common PIV issuance processes (across the people, process, and technologies involved).

View 1: PIV Issuance – mDL Opportunities



View 2: mDL Implementation Considerations

| STAGES | PIV Card Request | Identity Proofing and Registration | PIV Card Issuance |
|-------------------------------|--|--|--|
| POTENTIAL MDL SOLUTION | <p>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.</p>  | <p>Include option for PIV applicants to present mDL as an identity source during the in-person identity proofing and registration process 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.</p>  | <p>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.</p>  |
| PEOPLE & PROCESS | <p>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.</p> <p>Fraud Detection: Ensure that analysis tools capture critical mDL validation events per best practices.</p> | <p>Training: Train staff that are operating in-person kiosks/proofing system on how to cryptographically validate an mDL using a scanner and how to provide technical support to PIV applicants in-person and/or remotely.</p> <p>Centralized Staffing: Consider centralizing the overall number of staff in in-person and remote scenarios.</p> | <p>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.</p> <p>Centralized Staffing: Consider centralizing the overall number of staff in in-person and remote scenarios.</p> |
| TECH | <p>Interface: mDL validation will require interfacing with external databases to authenticate the PIV applicant's identity and automatically populate information in NIH Enterprise Directory (NED) system.</p> <p>Biometrics: PIV applicant should use their biometrics to unlock their wallet to deliver the mDL as evidence of the validity of the mDL.</p> | <p>Kiosk: 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.</p> <p>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.</p> | <p>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.</p> <p>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.</p> |
| CROSS - CUTTING | <p>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.</p> | <p>Technical Support: Health and Human Services (HHS) and HHS agencies 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).</p> | <p>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.</p> |



Engage with Us



@dhsscitech



dhs.gov/scitech



Technologically Speaking Podcast



Science and
Technology