Proposed Rules

Federal Register
Vol. 86, No. 73
Monday, April 19, 2021

This section of the FEDERAL REGISTER contains notices to the public of the proposed issuance of rules and regulations. The purpose of these notices is to give interested persons an opportunity to participate in the rule making prior to the adoption of the final rules.

DEPARTMENT OF HOMELAND SECURITY

6 CFR Part 37

[Docket No. DHS–2020–0028]

Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes; Mobile Driver's Licenses

AGENCY: Office of Strategy, Policy and Plans, Department of Homeland Security (DHS).

ACTION: Request for comment.

SUMMARY: The Department of Homeland Security (DHS) is issuing this request for information (RFI) to inform an upcoming rulemaking that would address security standards and requirements for the issuance of mobile or digital driver's licenses to enable Federal agencies to accept these credentials for official purposes as defined in the REAL ID Act and regulation.

DATES: Interested persons are invited to submit comments on or before June 18, 2021.

ADDRESSES: You may submit comments through the *Federal e-Rulemaking Portal at http://www.regulations.gov*. Use the Search bar to find the docket, using docket number DHS–2020–0028. See the ''Public Participation and Request for Comments'' portion of the **SUPPLEMENTARY INFORMATION** section for further instructions on submitting comments.

FOR FURTHER INFORMATION CONTACT: Steve Yonkers, Director, REAL ID Program, Office of Strategy, Policy, and Plans, United States Department of Homeland Security, Washington, DC 20528, *steve.yonkers@hq.dhs.gov,* 202–447–3274; and, George Petersen, Program Manager, Enrollment Services and Vetting Programs, Transportation Security Administration, Springfield, VA 20598, *george.petersen@tsa.dhs.gov,* 571–227–2215. Please do not submit responses to these addresses.

SUPPLEMENTARY INFORMATION:

Public Participation and Request for Comments

DHS invites interested persons to comment on this RFI by submitting written comments, data, or views. *See* **ADDRESSES** above for information on where to submit comments. Except as stated below, all comments received may be posted without change to *http://www.regulations.gov,* including any personal information you have provided.

Commenter Instructions

DHS invites comments on any aspect of this RFI, and welcomes any additional comments and information that would promote an understanding of the broader implications of acceptance of mobile or digital driver's licenses by Federal agencies for official purposes. This includes comments relating to the economic, privacy, security, environmental, energy, or federalism impacts that might result from a future rulemaking based on input received as a result of this RFI. In addition, DHS includes specific questions in this RFI immediately following the discussion of the relevant issues. DHS asks that each commenter include the identifying number of the specific question(s) to which they are responding. Each comment should also explain the commenter's interest in this RFI and how their comments should inform DHS's consideration of the relevant issues.

DHS asks that commenters provide as much information as possible, including any supporting research, evidence, or data. In some areas, DHS requests very specific information. Whenever possible, please provide citations and copies of any relevant studies or reports on which you rely, as well as any additional data which supports your comment. It is also helpful to explain the basis and reasoning underlying your comment. Although responses to all questions are preferable, DHS recognizes that providing detailed comments on every question could be burdensome and will consider all comments, regardless of whether the response is complete.

Handling of Confidential or Proprietary Information and SSI Submitted in Public Comments

Do not submit comments that include trade secrets, confidential business information, or sensitive security information [1] (SSI) to the public regulatory docket. Please submit such comments separately from other comments on the RFI. Commenters submitting this type of information should contact the individual in the **FOR FURTHER INFORMATION CONTACT** section for specific instructions.

DHS will not place comments containing SSI, confidential business information, or trade secrets in the public docket and will handle them in accordance with applicable safeguards and restrictions on access. DHS will hold documents containing SSI, confidential business information, or trade secrets in a separate file to which the public does not have access and place a note in the public docket explaining that commenters have submitted such documents. DHS may include a redacted version of the comment in the public docket. If an individual requests to examine or copy information that is not in the public docket, DHS will treat it as any other request under the Freedom of Information Act (FOIA) (5 U.S.C. 552) and DHS's FOIA regulation found in 6 CFR part 5.

Abbreviations and Terms Used in This Document

AAMVA—American Association of Motor Vehicle Administrators
DL/ID—Driver's License/Identification
DMV—Department of Motor Vehicles (or equivalent agency)
NFC—Near Field Communication
IEC—International Electrotechnical Commission
ISO—International Organization for Standardization
mDL—Mobile or Digital Driver's License/Identification Card
NIST—National Institute for Standards and Technology
PKI—Public Key Infrastructure
QR Code—Quick Response Code
RFI—Request for Information

[1] ''Sensitive Security Information'' or ''SSI'' is information obtained or developed in the conduct of security activities, the disclosure of which would constitute an unwarranted invasion of privacy, reveal trade secrets or privileged or confidential information, or be detrimental to the security of transportation. The protection of SSI is governed by 49 CFR part 1520.

WiFi—Wireless Fidelity

Table of Contents

I. Introduction

DHS is issuing this RFI to solicit comments from the public to help inform a potential rulemaking that would amend 6 CFR part 37 to set the minimum technical requirements and security standards for mobile or digital driver's licenses/identification cards (collectively ''mobile driver's licenses'' or ''mDLs'') to enable Federal agencies to accept mDLs for official purposes under the REAL ID Act and regulation.[2] This RFI is not related to the previously published DHS request for comment on November 7, 2019, entitled, ''Automated Solutions for the Submission of REAL ID Source Documents.'' [3] The scope of that request for comment concerned the process for presenting the identity and lawful status documentation during the application process for obtaining a REAL ID compliant driver's license or identification card. Specifically, the request for comment sought input on technologies that could assist states and their residents in the digital submission, receipt, and authentication of such documentation.

This RFI supports the Administration's general goals of reducing or eliminating unjustified complexity and excessive administrative burdens, consistent with the law and statutory goals. This effort is also consistent with the principles set forth in Executive Order 13563, ''Improving Regulation and Regulatory Review,'' as reaffirmed by President Biden's Memorandum on Modernizing Regulatory Review (January 20, 2021), calling for periodic review of existing rules with attention to those that ''may be outmoded, ineffective, insufficient, or excessively burdensome.''

For this new RFI, DHS seeks input concerning technical approaches, applicable industry standards, and best practices to ensure that mDLs can be issued and verified/authenticated with features to ensure security, privacy, and identity fraud detection. We also are interested in any data that can be provided on the cost of requirements necessary to permit federal acceptance of mDLs and the benefits of such requirements, as well as the benefits of permitting use of mDLs (*e.g.,* quantifiable cost-savings from being able to use a REAL ID-compliant mDL rather than a REAL ID-compliant physical driver's license or identification card (DL/ID)).[4]

DHS requests comments from the public and interested stakeholders, including entities engaged in the development, testing, integration, and implementation of mDLs and related technologies into systems or processes which historically relied upon physical DL/ID. To facilitate development of the regulation, DHS is primarily seeking comments that identify specific capabilities and technologies, actionable data, security and privacy risks and benefits, and economic (*i.e.,* cost/benefit) data.

Comments received may enable the Department to consider potential regulatory amendments that realize the benefits of mDLs in a competitively-neutral, technology-agnostic manner, complementary to the rapid technological innovations occurring in this space. DHS may contact individual commenters for more information. DHS reserves the right to use and share the information submitted with other federal agencies for purposes related to administering the REAL ID Act and implementing regulations.

II. Background

A. Digital Identity and mDLs Generally

Digital identity is generally recognized as the digital representation of an individual in an electronic transaction.[5] An mDL is a digital representation of the identity information contained on a state-issued physical DL/ID.[6] An mDL may be stored on, or accessed through, a diverse range of portable or mobile electronic devices, such as smartphones, smartwatches, and storage devices containing memory.[7] Like a physical DL/ID, mDL data originates from identity information about an individual that is maintained in the database of a state Department of Motor Vehicles (DMV) or equivalent agency. Although mDLs are a recent development, many states have begun to pilot or issue mDLs, and public interest in mDLs is high.

B. REAL ID Act, Current Regulatory Requirements, and the Need To Amend the Regulation

The REAL ID Act of 2005 and implementing regulation set minimum requirements for state-issued DL/ID accepted by Federal agencies for official purposes, including accessing Federal facilities, boarding federally regulated commercial aircraft, entering nuclear power plants, and any other purposes that the Secretary shall determine.[8] Full enforcement of the REAL ID regulation begins October 1, 2021.[9] Beginning on that day, Federal agencies may only accept state-issued DL/ID for official purposes if that DL/ID is REAL ID-compliant DL/ID and issued by a REAL ID compliant state.[10]

The Act defines a driver's license as ''a license issued by a State authorizing an individual to operate a motor vehicle on public streets, roads, or highways,'' and an identification card as ''an identification document issued by a State or local government solely for the purpose of identification.'' [11] Because an

[2] The REAL ID Act of 2005—Title II of division B of the FY05 Emergency Supplemental Appropriations Act, as amended, Public Law 109–13, 49 U.S.C. 30301 note; REAL ID Driver's Licenses and Identification Cards, 6 CFR part 37.

[3] 84 FR 60104 (Nov. 7, 2019).

[4] Regardless of whether DHS amends the regulation, and consistent with the REAL ID Act and regulation's applicability to physical DL/ID, compliant states may issue mDLs that are not REAL ID compliant, provided they are appropriately marked and use a unique design or color to indicate that they are not acceptable by Federal agencies for official purposes. *See* 6 CFR 37.71.

[5] *See* generally NIST Special Pub. 800–63–3, Digital Identity Guidelines (June 2017) at 2, available at *https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf.*

[6] A technical description of mDLs as envisioned by the American Association of Motor Vehicle Administrators may be found at *https://www.aamva.org/Mobile-Drivers-License/.*

[7] One notable feature of mDLs is the ability of an mDL Holder to control what data fields are released to a Federal agency. An mDL holder can authorize a Federal agency to receive only the data fields that the agency requires for its transaction.

[8] REAL ID Act of 2005 sec. 201(1) and (2).

[9] 6 CFR 37.5(b).

[10] *Id.*

[11] REAL ID Act of 2005 sec. 201(1) and (2). On December 21, 2020, Congress passed the REAL ID Modernization Act, which (among other things) would amend the definitions of ''driver's license'' and ''identification card'' to specifically include mobile or digital driver's licenses that have been issued in accordance with regulations prescribed by the Secretary. Sec. 1001 of the REAL ID Modernization Act, Title X of Division U of the Consolidated Appropriations Act, 2021, *available at*

Continued

mDL is issued for use as identification or to convey driving privileges, an mDL, therefore, must meet applicable REAL ID security requirements in order for federal agencies to accept them for official purposes.[12] Examples of such security requirements applicable to physical cards include ''common machine-readable technology'' and ''security features designed to prevent tampering, counterfeiting, or duplication . . . for fraudulent purposes.'' [13]

On January 29, 2008, DHS published a final rule implementing the Act's requirements.[14] The regulation prescribes requirements for the issuance and production of DL/ID in order for Federal agencies to accept those documents for official purposes. Because these regulatory requirements were developed for a physical document world, long before the advent of mDLs, some of the requirements may not be fully applicable to mDLs. For example, the regulation requires compliant DL/ID media, such as ''easily identifiable visual or tactile [security] features'' on the surface of a card to enable physical detection of fraudulent DL/ID,[15] ''[m]achine-readable technology on the back of the card,'' [16] and State plans for the security of ''[s]torage areas for card stock and other materials used in card production.''.'' [17] Such surface-level and/or physical security features do not apply to mDLs, which rely primarily on electronic security features and other measures that are not addressed in the regulation.[18] In addition to some requirements that are not applicable to mDLs, the regulation does not address the technological and functional considerations specific to mDLs, and appropriate to protect data as well as individual privacy.

Accordingly, receipt of information from this RFI will help inform any potential updates to the regulation to account for this new technology, including security standards for states to incorporate into their issuance and production processes to enable federal agencies to accept mDLs as REAL ID-compliant identification for official purposes.

C. Industry Standards and Guidelines for mDLs

Two international standards-setting organizations, the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC),[19] are jointly drafting standards relevant to mDLs. DHS understands that at least one such standard under development, ISO/IEC 18013–5, will set forth requirements concerning communication protocols, data structures, methods for identity verification, data integrity and protection mechanisms for authentication, and enable interoperability with a wide range of mobile devices and readers. The Department has participated in the development of this standard as a member of the United States national body member of the Joint Technical Committee developing the standard.[20] Through its involvement, DHS understands that the final standard may be published by early 2021.

Because the draft ISO/IEC 18013–5 standard is being developed for worldwide application, it may not meet all requirements necessary for use within the United States. The American Association of Motor Vehicle Administrators (AAMVA) has published Implementation Guidelines recommending extensions to the draft standard that would adapt it for DMVs in the United States.[21]

In addition to standard ISO/IEC 18013–5, DHS understands that ISO/IEC subcommittees are drafting additional standards that may set forth further requirements for mDLs. For example, ISO/IEC 23220–3 would set requirements that govern the step of ''provisioning'' (*see* Part D, below). This project, however, is in early stages of development; final drafts are not anticipated in the near term, and may not publish at all if the subcommittees cannot achieve consensus.

D. Relevant Terminology

For purposes of this RFI only, the following description of key terms is provided to ensure a consistent understanding of terminology in this RFI.

- *Authenticate* means establishing that a certain thing (*e.g., mDL Data*) belongs to its purported owner (*e.g., mDL Holder*) and has not been altered.
- A *Certificate Authority* issues *Digital Certificates* that are used to certify the identity of parties in a digital transaction.
- *Data Freshness* refers to the synchronization of *mDL Data* stored on a mobile device to data in a *DMV's* database, within a specified time period.
- *Department of Motor Vehicles (DMV)* refers to the state agency or its authorized agent responsible for issuing an mDL and for maintaining mDL data in its database.
- *Digital Certificates* establish the identities of parties in an electronic transaction, such as recipients or digital signatories of encrypted data.
- *Digital Signatures* are mathematical algorithms routinely used to validate the authenticity and integrity of a message.
- *Identity Proofing* refers to a series of steps that a *DMV* executes to prove the identity of a person.
- *Identity Verification* is the confirmation that identity data belongs to its purported holder.
- *Issuance* includes the various processes of a *DMV* to approve an individual's application for a REAL ID driver's license or identification card.
- An *mDL* is a digital representation of the information on a state-issued physical DL/ID, and is stored on, or accessed via, a mobile device.
- *mDL Data* is an individual's identity and DL/ID data that is stored

https://docs.house.gov/billsthisweek/20201221/BILLS-116HR133SA-RCP-116-68.pdf.

[12] This interpretation is also consistent with the Act's primary purpose, which was to raise the security bar for state-issued drivers' licenses and identification. The REAL ID Act sec. 202(b). Security features must ''prevent tampering, counterfeiting, or duplication of the document for fraudulent purposes.'' Cong. Rec.—House H453 (Feb. 9, 2005) (''Certainly all of us who board planes want to know that there is some integrity to our ID system in this country and that terrorists are not boarding planes by the use of a state-issued identification card.''); Cong. Rec.—House H453 at H463 (Feb. 9, 2005) (''sources of identity are the last opportunity to ensure that people are who they say they are'').

[13] REAL ID Act sec. 202(b)(8) and (9).

[14] Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes; Final Rule, 73 FR 5272 (January 29, 2008); codified at 6 CFR part 37. Currently, the regulation provides that beginning October 1, 2021, Federal agencies may only accept REAL ID-compliant DL/ID for official purposes, including boarding federally regulated commercial aircraft.

[15] 6 CFR 37.15(c) & 37.17(h).

[16] 6 CFR 37.17(i) & 37.19.

[17] 6 CFR 37.41(b)(1)(ii).

[18] These mDL-specific security features must be readable by DHS security technologies, such as Credential Authentication Technology (CAT).

[19] ISO is an independent, non-governmental international organization with a membership of 164 national standards bodies. ISO creates documents that provide requirements, specifications, guidelines or characteristics that can be used consistently to ensure that materials, products, processes and services are fit for their purpose. The IEC publishes consensus-based International Standards and manages conformity assessment systems for electric and electronic products, systems and services, collectively known as ''electrotechnology.'' ISO and IEC standards are voluntary and do not include contractual, legal or statutory obligations. ISO and IEC standards contain both mandatory requirements and optional recommendations, and are implemented by adopting mandatory requirements.

[20] A member of the Transportation Security Administration serves as DHS's representative to the Working Group.

[21] AAMVA Mobile Driver License (mDL) Implementation Guidelines, April 2019.

and maintained in a database controlled by a *DMV* and may also be stored and maintained on an individual's mDL.

- *mDL Holder* refers to the owner of a mobile device.
- *mDL Reader* refers to an electronic device that ingests *mDL Data* from a mobile device.
- *Offline* means no live connection to the internet.
- *Online* means a live connection to the internet.
- An mDL *Public Key Distributor* is a trusted entity responsible for compiling and distributing *Digital Certificates* issued by *DMVs.*
- *Public Key Infrastructure (PKI)* means a structure where a *Certificate Authority* uses *Digital Certificates* for *Identity Proofing* and for issuing, renewing, and revoking digital credentials.
- *Provisioning* refers to the various steps required for a DMV to securely place an *mDL* onto a mobile device.
- *Token* means a cryptographic key used to authenticate a person's identity.

III. Model for mDL Acceptance by Federal Agencies for Official Purposes

For Federal agencies to accept mDLs for official purposes, an mDL ecosystem must allow for trusted and secure communications between a DMV, a mobile device, and a federal agency.[22] Fundamentally, such a system would provide functionality analogous to the physical security features required under 6 CFR 37.15 that are designed to deter forgery and counterfeiting, promote confidence in the authenticity of the DL/ID, and facilitate detection of fraud.

DHS is exploring various technological solutions to determine how to implement such a secure system across the full range of federal agency use cases. Preliminarily, DHS believes that federally-accepted mDLs should address, as a baseline capability, the security, privacy, integrity, and trust features that are set forth in draft standard ISO/IEC 18013–5, and possibly the AAMVA Implementation Guidelines. However, those normative references should be viewed as a starting point, pending publication of the final documents, resolution of potential gaps in those documents, future technical developments and emerging technologies, and other implementation considerations. For illustrative purposes, and to develop issues and questions that are applicable to mDL implementation at all federal agencies, this section discusses the requirements being considered in the context of DHS's envisioned reference implementation and interoperability model. DHS believes that the following description of the reference implementation will help focus public comment on this RFI. DHS invites comments that address the near- and long-term considerations relevant to DHS's model and welcomes comments regarding other models that could be deployed at federal agencies.

A. Generally

Consistent with draft standard ISO/IEC 18013–5, DHS envisions a process in which a DMV would be responsible for issuing an mDL and enabling a user's mobile device to store and/or access mDL data. A Federal agency would use an mDL Reader to retrieve from a mobile device or from the DMV only the mDL Data needed for the purpose of the transaction. An individual's mDL Device would transmit mDL Data, or a digital ''token,'' to the reader via wireless or secure optical communication protocols (but not, for example, a static image of the driver's license or identification card, or any aspect of the physical card, reproduced from a physical driver's license). The reader should be capable of, and have necessary permissions for, transacting with mDLs issued by any DMV, and be agnostic to mobile devices, operating systems, and mDL apps. Such interoperability would require DMVs, app developers, and device manufacturers to conform to criteria established by ISO/IEC 18013–5 and applicable Federal regulations. Both the reader and mobile device would require the capability to communicate and authenticate the mDL data in at least offline (no internet connection) mode. The system would require digital security protocols to protect the confidentiality, privacy, security, and integrity of the mDL data, through its full lifecycle.

B. Physical DL/ID Issuance and mDL Provisioning

''Issuance'' is the process where a DMV processes an application for a REAL ID compliant DL/ID and issues the physical card to the individual. Provisioning (*see* Part C.1., below), which follows issuance sequentially, is a process used to establish that an mDL applicant is the rightful owner of identity data, approve an individual's application to receive an mDL, and securely place the mDL on an individual's mobile device. The issuance process for a REAL ID DL/ID is fundamentally different from the mDL provisioning process, which involves unique steps not applicable to physical DL/ID. DMVs will continue to be required to meet existing identity and lawful status documentation and verification requirements required under the REAL ID Act and implementing regulation for REAL ID compliant DL/ID, both physical and mDLs.

C. Communication Interfaces

Generally, mDL-based identity verification involves a series of transactions between an issuing authority (here, a DMV), a mobile device, and a verifying entity (here, federal agencies). Specifically, the DMV would provision mDL Data onto a mobile device, and an mDL Holder would authorize release of relevant mDL Data from the device to a federal agency, which would confirm data authenticity and choose whether to accept the mDL for its purpose. These transactions would require an architecture consisting of communication interfaces among a (1) DMV and mobile device, (2) mobile device and federal agency, and (3) federal agency and DMV (or an aggregator, such as a Public Key Distributor, or a centralized bridge to connect DMVs to a common infrastructure). Draft standard ISO/IEC 18013–5 establishes requirements governing the latter two interfaces. The communication interfaces enable the parties to exchange information and assess if the mDL Data (1) was provisioned by a trusted source (the DMV), (2) belongs to the individual asserting it, and (3) was transmitted to and received by an agency unaltered.

1. DMV and mDL Device: Provisioning

This communication interface enables the step of ''provisioning.'' Generally, ''provisioning,'' which follows issuance, is the process where a DMV would authorize the secure storage of mDL Data onto a mobile device, enable the device to receive the data from a DMV, and transmit the data to the device. The initial step of provisioning requires proving that the target mobile device belongs to the mDL applicant. Next, a trusted connection would be established between the DMV and the target mobile device. Finally, the DMV would use this connection to securely transmit and update mDL Data on the device (or enable the device to access the data).

Generally, mDLs can be provisioned in-person or remotely based on individual DMV preference. ''In-person'' provisioning requires an individual to bring a mobile device and identity documents to a physical DMV location,

[22] Whether a state law enforcement entity refuses to accept mDLs as driver's licenses is not relevant to DHS's determination of whether an mDL falls within the REAL ID Act's definition of ''driver's license.''

which would then confirm the individual's identity and provision mDL Data onto the target mobile device. ''Remote'' provisioning, in contrast, does not require an individual to be physically present at a DMV location. Instead, individuals would electronically send identity verification information to the DMV to establish their identities and ownership of the target device. The Department is not aware of any mature industry standards [23] defining standardized communication protocols to assure comparable levels of trust between the in-person and remote methods of provisioning. Accordingly, DHS seeks comment (*see* Part IV) on the security and privacy risks, as well as mitigating solutions, concerning provisioning to ensure that federal agencies can trust mDLs provisioned either in-person or remotely. DHS also seeks comments concerning which methods of provisioning provide the security, privacy, and trust appropriate for acceptance by federal agencies.

Regarding the storage and protection of mDL data on a mobile device (known as ''data at rest''), DHS is aware of at least two notional types of solutions: (1) A hardware-based option, where the mobile device private key and/or mDL Data would be stored in and/or secured by a mobile device's secure hardware, and (2) a software-based option, where the private key and/or data would reside within a third-party app installed on a mobile device, secured by the device's key chain management interface. Preliminarily, DHS believes that both solutions offer advantages and disadvantages. Given the absence of mature industry standards for storing and securing mDL data on a device, however, the Department seeks comment (*see* Part IV) on preferred solutions for these considerations.

2. mDL Device and Federal Agency: Offline Data Transfer

Draft standard ISO/IEC 18013–5 sets forth requirements that govern communication between a mobile device and a federal agency. This communication interface serves two functions: (1) Establishing a secure communication channel between a mobile device and a federal agency, and (2) transmitting mDL Data to an agency in an ''offline'' transaction (where an agency's mDL Reader or user's mDL Device are not connected to the internet).

Under draft standard ISO/IEC 18013–5, a secure communication channel could be established via NFC or QR Codes, and data transmission could occur using a higher bandwidth channel, such as Bluetooth Low Energy, WiFi Aware, or NFC. DHS may reference pertinent requirements of the draft standard in a future rulemaking and seeks comments (*see* Part IV) on this approach.

In an offline data transfer mode, an mDL Holder initiates the transaction and authorizes release of mDL data to a federal agency's mDL Reader.[24] Draft standard ISO/IEC 18013–5 would allow an mDL Holder to release only the data necessary for the purpose of the transaction (*e.g.,* identity verification), while blocking the Agency's ability to view any other mDL data (*e.g.,* organ donor status). The mDL data would then be transferred directly from a mobile device to the federal agency, which would need to authenticate the data and verify that it originated with a DMV and was not altered. This is known as ''offline authentication,'' and is discussed below.

3. Federal Agency and DMV: Online Data Transfer and Offline Authentication

Draft standard ISO/IEC 18013–5 sets forth requirements governing the communication interface between a federal agency and a DMV, which enables (1) online data transfer, and (2) offline authentication.

In an online transaction, a federal agency would receive mDL Data directly from a DMV instead of from a mobile device. In this step, a mobile device would first pass a token to a Federal agency, which would use the token to retrieve mDL Data from the DMV. Draft standard ISO/IEC 18013–5 governs communication protocols and methods for online verification functionality. This interface can also be used for offline authentication, although development of infrastructure and additional related procedures are required.

An ISO/IEC 18013–5 compliant mDL must include both online and offline functionality. DHS is considering referencing pertinent parts of ISO/IEC 18013–5 in a future rulemaking and seeks commenters' views (*see* Part IV) on the appropriateness of this approach. In particular, DHS seeks comments concerning the security and privacy risks, as well as mitigating solutions, concerning both offline and online data transfer modes.

D. Other Considerations

1. Data Trust and Security Features

Fundamentally, Federal agencies cannot accept an mDL unless the agency can authenticate the identity information. This means confidence that the mDL Data came from a trusted source (the DMV), and the mDL Data was transmitted to the agency unaltered. The current regulation establishes such ''trust'' by requiring physical DL/IDs to include physical security features on the surface of a card that are designed to deter and detect forgery and counterfeiting. As mDLs lack a physical form they cannot overtly display physical security features. Therefore, regulatory requirements for physical security features on a physical substrate need to be updated to establish comparable mDL-specific security features.

DHS is aware of at least two means of extending security features to the digital medium: (1) For offline transactions, asymmetric cryptography/public key infrastructure (PKI), and (2) for online transactions, establishing a secure communication channel with a trusted Issuing Authority. With respect to offline transactions, ''asymmetric cryptography'' generates a pair of encryption ''keys'' to decrypt protected data. One key, a ''public key,'' is distributed publicly, while the other key, the ''private key,'' is held by the DMV. When a DMV issues an mDL, the DMV uses its private key to digitally ''sign'' the mDL data. A Federal agency confirms the integrity of the mDL data by obtaining the DMV's public key to verify the digital signature. With the potential for 56 U.S. states [25] to issue mDLs, however, an aggregator, such as a master list holder, or a public key distributor, or a centralized repository of trusted public certificates, may be necessary for assuring that verifying entities have updated digitally signed certificates/public keys.

Online transactions would require establishing a secure network connection between a Federal agency and a DMV. This may take the form of an encrypted communication channel

[23] As discussed in Part II.C., above, DHS understands that the ISO and IEC are developing standard ISO/IEC 23220–3, which may set forth requirements for provisioning. However, publication of a final draft is not anticipated in the near-term.

[24] Federal agencies may choose to implement an mDL Reader using different technology. For example, one embodiment could be a device integrated into an agency's Credential Authentication Technology to receive mDL data.

[25] The REAL ID Act defines ''state'' to mean ''a State of the United States, the District of Columbia, Puerto Rico, the Virgin Islands, Guam, American Samoa, the Northern Mariana Islands, the Trust Territory of the Pacific Islands, and any other territory or possession of the United States.'' REAL ID Act of 2005 sec. 201(5), as amended by sec. 2(a) of Public Law 115–323 (Dec. 17, 2018).

using a DHS-approved encryption algorithm.

For all transactions (offline and online), DHS preliminarily believes mDL Data requires protection, both during transmission (known as ''data-in-transit'') and during storage on a mobile device (known as ''data-at-rest''). Draft standard ISO/IEC 18013–5 requires encryption of data-in-transit, but not data-at-rest. The AAMVA Implementation Guidelines, however, seek to address this gap by affirmatively recommending such encryption.[26] Accordingly, DHS is considering requiring, in a future rulemaking, mandatory encryption of both data-in-transit and data-at-rest. DHS seeks comments (*see* Part IV) concerning proposed and alternative solutions to provide the requisite levels of security to establish the trust required for Federal agencies to accept mDLs for official purposes.

2. Data Freshness

Unlike physical DL/ID, mDLs have the potential to provide verification of the ''freshness,'' of identity data. For offline transactions, this enhancement arises from the ability of an mDL to communicate the last date on which identity data was synchronized with the DMV's database (*i.e.,* the most recent time and date when the DMV confirmed that the identity data remained valid), a concept known as ''data freshness.'' Data freshness verification enables a Federal agency to trust that the identity data is still current and valid. This concept does not apply to online transactions, where a Federal agency receives data directly from the DMV (which potentially offers even greater security, because the agency would receive data updated from the DMV in real-time). In contrast to mDLs, physical DL/ID are static and do not instill any trust of data validity or ''freshness'' beyond the expiration date printed on the face of the DL/ID at the time of issuance.

Preliminarily, DHS believes that shorter data freshness periods may bring security benefits, and is exploring the benefits and costs of requiring specific data freshness periods in the regulation. Although draft standard ISO/IEC 18013–5 specifies various data fields that reflect when mDL data was last refreshed, it does not require any specific freshness period. In addition, DHS understands that DMVs independently establish mDL data validity periods. Because of the absence of industry standards and common practices among DMVs, DHS seeks comment (*see* Part IV) concerning whether, and on what basis, DHS should require specific data freshness periods for offline transactions, as well as appropriate periods for data freshness.

3. Verification

Generally, an mDL can be verified via two methods: Attended and unattended. Attended verification requires the physical presence of an attendant to supervise the mDL transaction, whereas unattended verification is performed algorithmically without the presence of an attendant. Draft standard 18013–5 sets forth requirements specifically for attended verification, but does not address the unattended online model (but DHS understands this may be the subject of a future ISO/IEC project). Accordingly, additional standards and requirements would need to be established to enable Federal agencies to implement unattended online verification. DHS seeks comments (*see* Part IV) concerning technical requirements necessary to enable unattended online verification by Federal agencies. DHS also seeks comments concerning the security and privacy risks, and mitigation solutions, concerning unattended online verification.

IV. Questions for Commenters

DHS requests comments in response to the following questions. We do not intend these questions to restrict the issues that commenters may address. Commenters are encouraged to address issues that may not be discussed below based upon their knowledge of the issues and implications. In providing your comments, please follow the instructions in the Commenter Instructions section above.

1. *Security Generally.* Provide comments on what security risks, including data interception, alteration, and reproduction, may arise from the use of mDLs by Federal agencies for official purposes, which includes accessing Federal facilities, boarding federally-regulated commercial aircraft, and entering nuclear power plants.

a. Explain what digital security functions or features are available to detect, deter, and mitigate the security risks from mDL transactions, including the advantages and disadvantages of each security feature.

b. Provide comments on how mDL transactions could introduce new cybersecurity threat vectors into the IT systems of Federal agencies by, for example, transmitting malicious code along with the mDL Data.

c. Sections 37.15 and 37.17 of 6 CFR part 37 set forth specific requirements for physical security features for DL/ID and other requirements for the surface of DL/ID. Provide comments on what requirements are necessary to provide comparable security assurances for mDLs.

2. *Privacy Generally.* Provide comments on what privacy concerns or benefits may arise from mDL transactions, and how DHS should or should not address those concerns and benefits in the REAL ID context. Explain what digital security functions or features are available to protect the privacy of any personally identifiable information submitted in mDL transactions, including the advantages and disadvantages of each security feature.

3. *Industry Standards.* Executive Order 12866 directs Federal agencies to use performance-based standards whenever feasible. DHS is considering including technical standards for mDL transactions in its proposed rule, drawing heavily on standards under development by the industry, to support compatibility and technical interoperability across all interested Federal agencies nationwide. If commenters believe an industry standard should be chosen, provide comments on how DHS should choose the correct standard(s) for mDLs, and on the appropriate baseline standard(s) that DHS should impose.

4. *Industry Standard ISO/IEC 18013–5: Communication Interfaces Between mDL Device and Federal Agency, and Federal Agency and DMV.* DHS may adopt certain requirements that may be established in forthcoming international industry standards that specify digital security mechanisms and protocols with respect to the communication interface between a mobile device and a Federal agency, and the communication interface between a Federal agency and a DMV.

a. Provide comments on what concerns commenters have regarding such standards and DHS's adoption of their requirements. In particular, explain whether commenters believe the current drafts of industry standard ISO/IEC 18013–5 are mature enough to support secure and widespread deployment of mDLs.

b. Explain the impact on stakeholders and mDL issuance if such standards are not approved in a timely manner.

c. Quantify the initial and ongoing costs to a stakeholder to implement these standards.

d. Provide comments on what, if any, key areas related to mDLs are not covered in these standards that DHS should consider addressing by regulation.

e. Identity what, if any, alternative standards or requirements DHS should consider.

5. *Industry Standard ISO/IEC 23220–3: Communication Interface Between DMV and mDL Device.* DHS understands that forthcoming international industry standard ISO/IEC 23220–3 may specify digital security mechanisms and protocols with respect to the communication interface between a DMV and a mobile device, specifically concerning provisioning methods, data storage, and related actions. Although DHS may seek to adopt certain requirements anticipated to appear in this standard, the Department understands that this standard may not be finalized for several years.

a. Explain whether commenters believe the current drafts of standard ISO/IEC 23220–3 are mature enough to support secure and widespread deployment of mDLs.

b. With the ongoing development of ISO/IEC 23220–3, provide comments on what, if any, alternative standards or requirements DHS should consider before the standard is finalized.

6. *Provisioning.* DHS understands that provisioning may be conducted in-person, remotely, or via other methods.

a. Explain the security and privacy risks, from the perspective of any stakeholder, presented by in-person, remote, or other provisioning methods.

b. Provide comments on the security protocols that would be required for DMVs to mitigate security and privacy risks presented by in-person, remote, or other provisioning methods, and to ensure at a high level of certainty that a REAL ID compliant mDL is securely provisioned to the rightful owner of the identity and the target mDL device, for in-person or remote applications.

c. Provide comments on whether mDL Data should include data fields populated with information concerning the method of provisioning used.

d. Provide estimated costs for a DMV to implement in-person or remote provisioning. Costs may include IT contracts, hiring full or part-time IT staff, as well as software and hardware.

7. *Storage.* DHS understands that mobile device hardware- and software-based security architectures can be used to secure mDL Data on a mobile device.

a. Provide comments on the advantages and disadvantages, with respect to security, functionality, and interoperability, of the different mobile security architectures for protecting, storing and assuring integrity of mDL Data.

b. Explain whether a hardware- or software-based solution, or both, would provide the requisite security in a competitively-neutral manner.

8. *Data Freshness.* Provide comments regarding whether and to what extent security risks concerning data validity and freshness can be mitigated by defining the frequency by which mDL Data should synchronize with its DMV database.

a. Provide comments regarding what data synchronization periods commenters believe are appropriate for mDL transactions. Explain the advantages and disadvantages of a longer or shorter periods.

b. Provide estimated costs to a stakeholder to implement the data synchronization periods stated above.

9. *IT Security Infrastructure.* Provide comments on whether IT security infrastructure, such as Public Key Infrastructure, would provide the level of privacy and security sufficient to implement a secure and trusted operating environment, for both offline and online use cases, and if not, explain what alternative approaches would be better.

a. Identify any what additional or alternative IT security infrastructure (*e.g.,* a public key distributor or aggregator such as a trusted public certificate list, Federal PKI) that would be required to facilitate trusted mDL transactions between mDL holders, verifying entities, and issuing authorities.

b. Provide estimated costs for a DMV or Federal agency to implement necessary IT security infrastructure. Costs may include IT contracts, hiring full or part-time IT staff, as well as software and hardware.

10. *Alternative IT Security Solutions.* Provide comments on whether DHS should consider privacy or security solutions adopted in other industries, such as finance (*e.g.,* mobile payments), automotive/telecommunications (*e.g.,* vehicle-to-vehicle or ''V2V''/''V2X'' communications), or medical (*e.g.,* electronic prescriptions for controlled substances), that rely on digital identity and/or secure device-to-device transactions. Explain what those solutions are and how they could be adapted or implemented for Federal mDL use cases.

11. *Offline and Online Data Transfer Modes.* DHS understands that mDL Data may be transferred to a Federal agency via offline and online modes.

a. Explain the security and privacy risks, from the perspective of any stakeholder, presented by both offline and online data transfer modes.

b. Provide comments on the security protocols that would be required to mitigate security and privacy risks presented by both offline and online data transfer modes.

12. *Unattended Online mDL Verification.* Provide comments on what capabilities or technologies are available to enable unattended online mDL verification by Federal agencies. Explain the possible advantages and disadvantages of each approach.

a. Explain the security and privacy risks, from the perspective of any stakeholder, presented by unattended online mDL verification.

b. Provide comments on the security protocols that would be required for DMVs to mitigate security and privacy risks presented by unattended online mDL verification.

13. *Costs to Individuals.* Provide comments on the estimated costs, including savings, to an individual to obtain an mDL, including:

a. Time and effort required to obtain the mDL.

b. Fees charged by DMVs.

c. Any charges for inclusion of additional information on an mDL, such as HAZMAT endorsements, hunting, fishing, or boating licenses.

14. *Considerations for mDL Devices Other than Smartphones.* Provide comments on whether provisioning an mDL on, or accessing an mDL from, a device other than a smartphone (*e.g.,* a smartwatch accessing mDL Data from a smartphone paired to it, or a mobile device authorized to access mDL Data stored remotely), poses security or privacy considerations different than provisioning an mDL on, or accessing an mDL from, a smartphone. Explain such security or privacy considerations and how they can be mitigated.

15. *Obstacles to mDL Acceptance.* Describe any obstacles to public or industry acceptance of mDLs that DHS should consider in developing its regulatory requirements. Provide comments on recommendations DHS should consider addressing such obstacles, including how to educate the public about security and privacy aspects of digital identity and mDLs.

The Department issues this RFI solely for information and program planning purposes, and to inform a future rulemaking. Responses to this RFI do not bind DHS to any further actions related to the response.

Kelli Ann Burriesci,

Acting Under Secretary, Office of Strategy, Policy, and Plans, United States Department of Homeland Security.

[FR Doc. 2021–07957 Filed 4–16–21; 8:45 am]

BILLING CODE 9110–9M–P