

Mobile Driver's License Pilot Program

In Accordance with Vehicle Code §13020



Gavin Newsom
Governor

Toks Omishakin, Secretary
California State Transportation Agency

Steve Gordon, Director
Department of Motor Vehicles



TABLE OF CONTENTS

Executive Summary	3
Pilot Program Guidelines	4-6
CA DMVs' Unique Approach	7-12
Product Review	13
CA DMV Wallet	13-19
Native Industry Wallets	20-22
Lessons Learned	23-24
Fiscal Impact	25-27
Recommendations	28-29
Outreach Material	30
Vehicle Code §13020	31-33

Executive Summary

[Vehicle Code \(VC\) §13020](#) authorizes the California Department of Motor Vehicles (CA DMV) to conduct a pilot program to evaluate the use of optional mobile or digital alternatives to driver's license and identification (DL/ID) cards. As part of conducting the pilot, CA DMV is required to submit a report on the mobile driver's license (mDL) pilot program to the California Legislature, no later than July 1, 2026, to include, but not be limited to, the following:

1. A review of the products developed and evaluated during the lifecycle of the pilot program. Additionally, this report includes details of the security and privacy features that are currently installed and designed to protect against unauthorized access to account data, personal information and to mitigate surveillance risks.
2. An overview of the lessons learned regarding the risks and solutions related to implementation and/or production viability and utility of the pilot program.
3. Recommendations for subsequent actions that should be taken regarding the products developed and evaluated during the lifecycle of the mDL pilot program.
4. An estimate of the fiscal impact of the deployment of the mDL pilot program, including the estimated impact to the Motor Vehicle Account, pursuant to [VC §42271](#).

CA DMV built a custom digital wallet ([CA DMV Wallet](#)) that can be used to digitally store and access essential documents from anywhere, at any time. It provides fast, convenient, and secure access to CA DMV's online services including applications for a Disabled Person Parking Placard (DPPP) or to a customer's "My DMV" account mDL holders are able to provision their mDL on popular native industry wallets such as the Apple Wallet, the Google Wallet, and the Samsung Wallet.

CA DMV's mDL pilot has demonstrated that this technology benefits Californians. CA DMV's mDL will reduce fraud, improve the customer experience, lower the demand for in-person service at DMV field offices, and create cross-agency efficiencies.

CA DMV recommends continued investments in this technology and its multitude of uses for Californians. CA DMV continues to evaluate the integration of the mDL into additional online services to provide the public with a secure and convenient way to prove their identity when conducting CA DMV business transactions online.

Pilot Program Guidelines

[Assembly Bill \(AB\) 149 \(Chapter 81, Statutes of 2021\)](#) authorized CA DMV to establish a pilot program to evaluate the use of optional mobile or digital alternatives to DL/ID cards, including, but not limited to, the voluntary participation of persons in the program and a limitation on the percentage of people that can participate in the program. AB 149 also required CA DMV, in developing and implementing the use of digital DL/ID cards, to ensure the protection of personal information and include specified security features that protect against unauthorized access to information.

AB 149 established the following parameters for the administration of the pilot:

- Any pilot program established shall be limited to both of the following:
 - ▶ Persons who have voluntarily chosen to participate in the pilot program.
 - ▶ No more than 0.5 percent of licensed drivers for the purpose of evaluation.
- A participant in any pilot program may terminate their participation in the pilot program at any time, and may, upon termination, request the deletion of any data associated with their participation in the program. Within 10 days of any such request, the department and all entities contracted with the department for the purpose of effectuating the pilot program shall delete all data collected or maintained pursuant to the participant's participation in the program.
- All participants shall receive both a physical and, if requested, an immutable and unique driver's license or identification card.
- In developing and implementing the use of digital driver's licenses and identification cards, the department shall ensure the protection of personal information and include security features that protect against unauthorized access to information, including, but not limited to, all the following:
 - ▶ Ensuring that any remote access to the digital driver's license or identification card shall require the express, affirmative, real-time consent of the person whose digital driver's license or identification card is being requested for each piece of information being requested, and shall be limited to only that information, which is provided on a physical driver's license or identification card.
 - ▶ Ensuring that the digital driver's license or identification card, as well as any mobile application required for the digital driver's license or identification card, shall not contain or collect any information not strictly necessary for the functioning of the digital driver's license, identification card, or mobile application, including, but not limited to, any information relating to movement or location.

- ▶ Ensuring that the information transmitted to the digital driver's license or identification card, as well as any mobile application required for the digital driver's license or identification card, is encrypted and protected to the highest reasonable security standards broadly available, including ISO-18013-5, FIPS 140-3, and NIST 800-53 Moderate, and cannot be intercepted while being transmitted from the department.
- In the conduct of any pilot program pursuant to this section, any data exchanged between the department and any electronic device, between the department and the provider of any electronic device, and between any electronic device and the provider of that electronic device, shall be limited to those data necessary to display the information necessary for a driver's license or identification card.
- An entity contracted with the department for this purpose shall not use, share, sell, or disclose any information obtained as part of this contract, including, but not limited to, any information about the holder of a digital driver's license or identification card, except as is necessary to satisfy the terms of the contract. Upon termination or expiration of any contract entered for this purpose, the contracting entity shall delete any data collected or generated in the course of activities pursuant to that contract within 30 days.
- The holder of a digital driver's license or identification card shall not be required to turn over their electronic device to any other person or entity in order to use the digital driver's license or identification card for identity verification.
- The holder of a digital driver's license or identification card showing or turning over their electronic device to any other person or entity in order to use the digital driver's license or identification card for identity verification shall not constitute consent to a search, nor shall it constitute consent for access to any information other than that which is immediately available on the digital driver's license or identification card. Information incidentally obtained in the process of viewing a digital driver's license or identification card in order to verify the identity of the holder shall not be used to establish probable cause for a warrant to search the electronic device.
- Any request for remote access to their digital driver's license or identification card for identity verification shall require the express consent of the holder of the digital driver's license or identification card, shall be limited to the content of the digital driver's license or identification card specified in the request for remote access, and shall not exceed the information available on a physical driver's license or identification card.

- Consent to remote access to a digital driver's license or identification card by the holder shall not constitute consent to a search, nor shall it constitute consent for access to any information other than that which is immediately available on the digital driver's license or identification card. Information incidentally obtained in the process of remotely accessing a digital driver's license or identification card shall not be used to establish probable cause for a warrant to search the electronic device.

A participant in any pilot program established by the department pursuant to this section shall not be required to use a digital driver's license or identification card rather than a physical driver's license or identification card for the purpose of identity verification, nor shall their participation in the pilot program preclude their use of a physical driver's license or identification card under any circumstances. A person or entity shall not provide preferential service based on a person's use of a digital driver's license or identification card rather than a physical driver's license or identification card. The pilot program may include the issuance of mobile or digital Real ID driver's license or identification cards upon authorization of the United States Secretary of Homeland Security.

Subsequent to the start of the pilot, [Senate Bill \(SB\) 125 \(Chapter 54, Statutes of 2023\)](#) expanded the maximum number of participants from 0.5 percent of the licensing population to 5 percent of the licensing population.

[SB 153, \(Chapter 109, Statutes of 2025\)](#) further expanded the percentage of licensed drivers who can participate in the mDL pilot program from 5 percent to 15 percent.

CALIFORNIA'S UNIQUE APPROACH

In conducting the mDL pilot program, CA DMV took a unique approach. In contrast to other states, which relied primarily or heavily on large technology companies' proprietary software and hardware, CA DMV pioneered a privacy-first, open sourced, multi-use case architected digital identity platform, which allows mDL holders to control their personal “digital” data. By creating an mDL that serves as a user-controlled identity, mDL holders are able to prove who they are to various public vendors, service providers, government agencies, websites, and applications, rather than relying on a website or tech company to verify their identity.

CA DMV built a custom digital wallet ([CA DMV Wallet](#)) and designed the mDL to be platform agnostic, which improves accessibility by affording additional choices in what mobile devices are used and how online identities are stored and managed. To maximize the utility of the new identification format, CA DMV executed two key strategies:

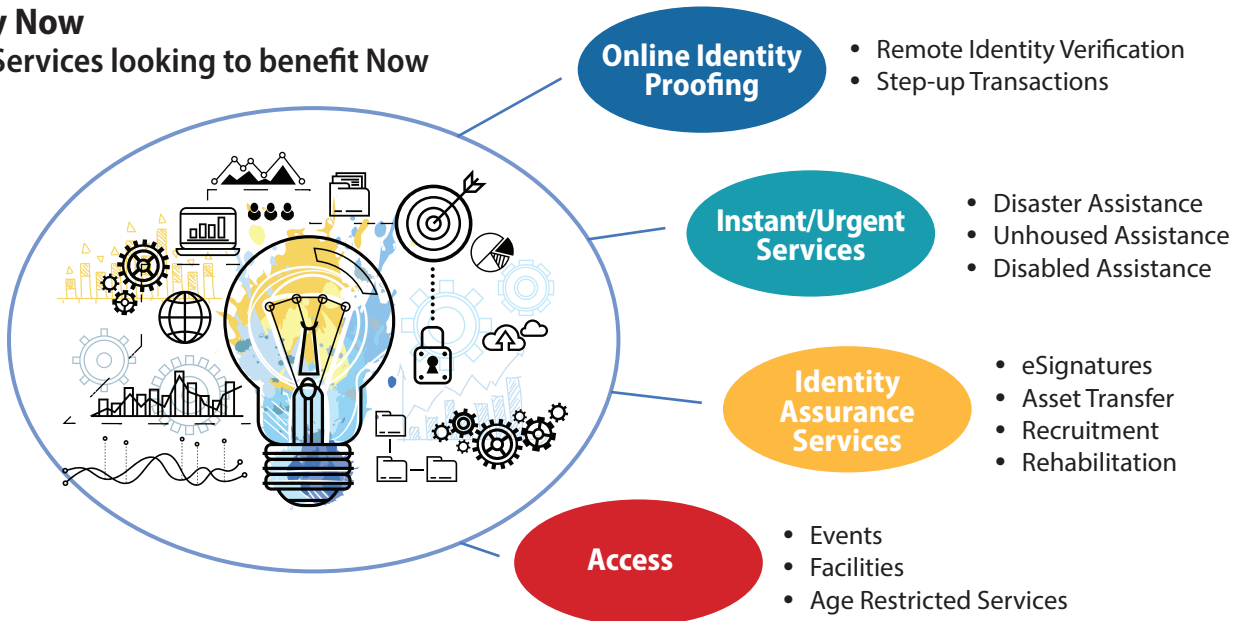
- Designed the mDL to conform with the emerging global standards and guidelines from the International Organization for Standardization ([ISO](#)), the World Wide Web Consortium ([W3C](#)), and the National Institute for Standards and Technology ([NIST](#)).
- Partnered with agencies, organizations and retailers who require identity and/or age verification, including:
 - ▶ **Transportation Security Administration (TSA):** During the mDL pilot program concept and planning phase, CA DMV envisioned the utility of a Federally accepted mobile credential, diligently ventured forward, in collaboration with TSA, to realize that vision and develop it to viable production. Consequently, for mDL holders who also hold a corresponding REAL ID compliant CA DL/ID card, the mDL is currently recognized as a Federally compliant credential and accepted at over 250 select [United States airport checkpoints](#).
 - ▶ **The National Association of Convenience Stores' TruAge system:** Integrated into CA DMV Wallet and activated upon pilot program sign up and mDL provisioning, TruAge may be used for age-verified product purchases at 78 participating convenience stores statewide.
 - ▶ **California Community Colleges:** California Community Colleges accept the DMV Wallet as a form of high assurance identity verification to reduce financial aid fraud and also to reduce identity verification.
 - ▶ **DMV Services:** DMV online and in person services have been modified to accept mDL to verify identity and prefill data saving operational costs of manual document verification and data entry errors in the submission process of select services.

Benefits to Government Services

California's unique approach to an aggressive market adoption strategy has started to find traction within State, local, federal and cross border public sector use cases focused on cost and fraud reduction, accessibility, process optimization and convenience as illustrated below.

Ready Now

State Services looking to benefit Now



EDD, FTB, CoveredCal, DMV, CCCO, SSA, SCO

- Cost elimination for third party identity proofing (TransUnion, Socure)/Service Augmentation for low success rates with third parties (fraud and ID Maps/Tableau Public)
- Reduced fraud, user friction and abandonment in proofing and authentication steps
- Additional no-cost identity reverification for sensitive online transactions

County of LA, City of SF, SAC, Local Assistance Centers, EMSA

- Expedited services needing verified identity
- Reduced DMV onsite need
- Disaster area access/logistics management for volunteers and first responders

CDCR, Caltrans, UCOP

- Integrated Background checks
- HR Onboarding
- Interim verifiable Identity proof for delays in identity card issuance

City of LA (Olympics), ABC, Cannabis, CHP, DOJ

- Age verification for purchases
- Sports events special entry
- Reduced duration roadside stop
- Firearms and ammunition (Ral ID) purchase

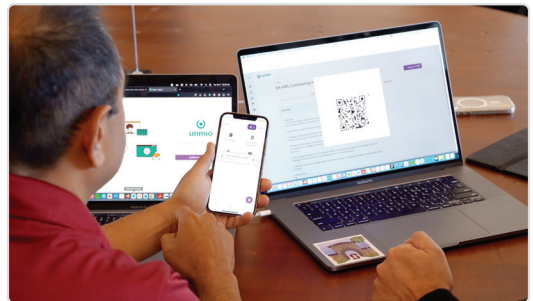
Hackathons

CA DMV, in partnership with the non-profit open standards body OpenID Foundation, hosted [two hackathons](#), which showcased the utility and potential of mDLs and set a precedent for future collaborations between public and private sectors for exploring real-world use cases and to achieve widespread adoption of digital identity.

The first hackathon was held October 1, 2024, in Mountain View, California, brought together 15 selected teams that include over 50 participants from over 20 leading private sector companies and start-ups. These teams explored practical and privacy-focused applications for the mDL, demonstrating their value in industries like financial services, retail, healthcare, and entertainment.

Several teams at this first event were recognized for their outstanding contributions:

- **Most Compelling and Most Socially Impactful:** Team Entidad. Integrating mDL for nonprofits to reach and enroll underserved community members into social benefits programs.
- **Most Promising:** Team Cisco VC Verifiers. Using mDL as a root digital identity to enable password less authentication.
- **Best Privacy and Security Design:** Team Block (the parent company of Square). Leveraging mDL for point-of-sale age verification of age-restricted products sold by Square merchants.
- **Most Scalable:** Team US Bank. Implementing mDL for in-person identity verification at bank branches, specifically for high-risk transactions.
- **Best User Experience:** Team UltraPass. mDL, combined with encrypted biometric authentication, to streamline account creation for new users and helps businesses prevent users from creating duplicate accounts.
- **Best Presentation:** Team MATTR (MATTR, Samsung, Treez, Nuvei). mDL for identity and age verification in cannabis dispensary and delivery services.
- **Best Independent Submission:** Team UFI. Integrating mDL into existing Identity and Access Management (IAM) systems.



The second hackathon held November 1, 2024, in Sacramento, California, shifted the focus to public sector use cases. With over 40 participants from a range of government entities, teams tackled diverse applications, such as from assisting people apply for government jobs, streamlining access to government services, and streamlining access to emergency and disaster assistance.

The teams recognized for their outstanding contribution to this second hackathon, included:

- California Office of Data and Innovation for 'Best Overall Solution and Most User-Friendly Design'.
- California Governor's Office of Emergency Services for 'Best Value to the Residents'.
- California Highway Patrol with their hackathon partner Credence ID for 'Most Viable Implementation'.

The two hackathons respectively welcomed more than 50 observers from a wide range of private and public sector entities that were interested in implementing mDLs and eager to learn from the participating teams. Many of these entities continued to engage with the CA DMV.

By collaborating with the OpenID Foundation, which develops identity and security specifications that are serving billions of consumers across millions of applications, the CA DMV was able to leverage the open standard body's extensive member network, funding to support real-world implementations, members' expertise and insights, and tooling and technical support.

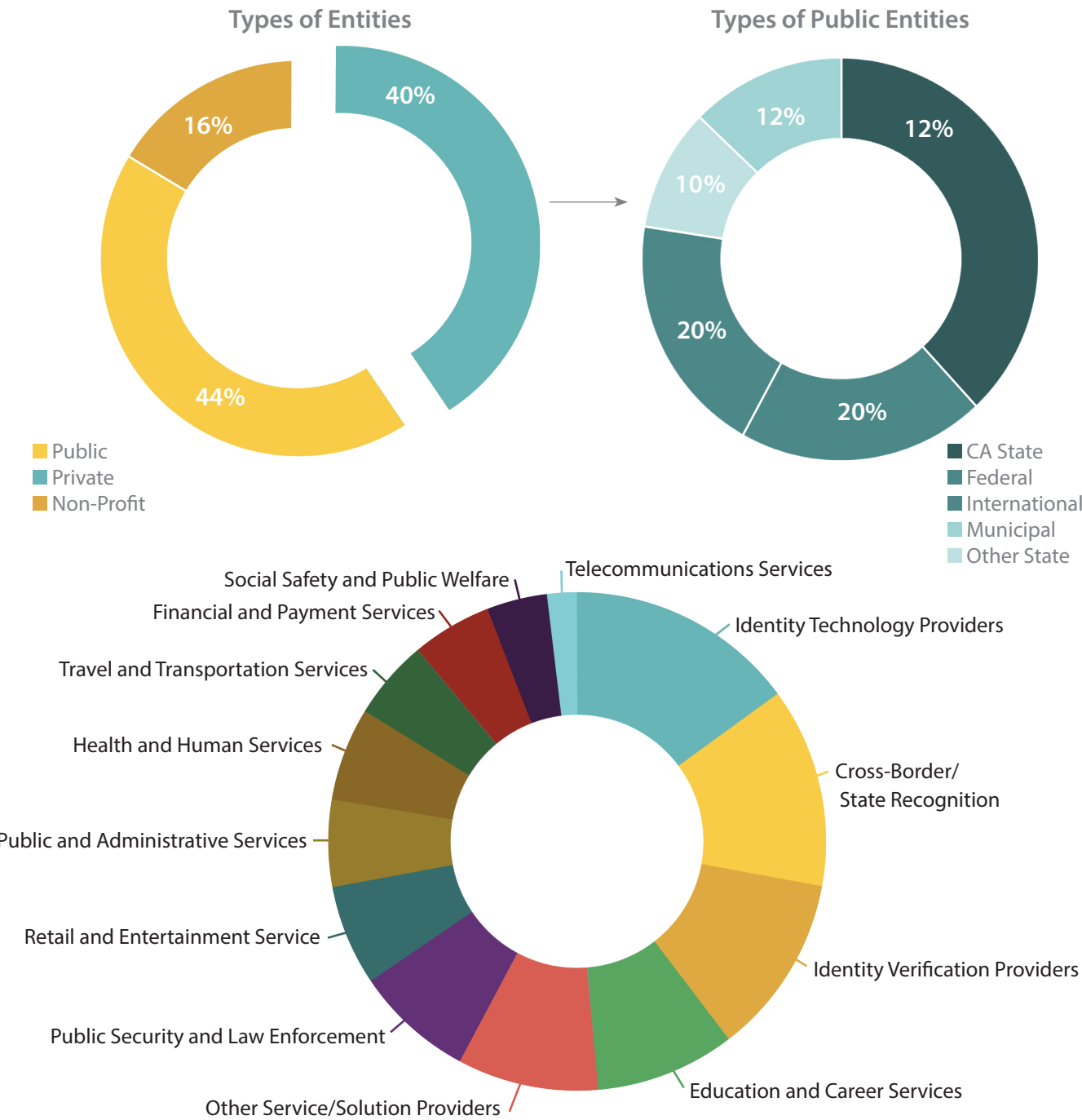
The success of both events was the result of meticulous planning and a targeted outreach strategy from both the CA DMV and the OpenID Foundation. By ensuring each team that participated represented a real-world challenge that a private entity or public agency is attempting to address, the hackathons provided relevant, practical, and valuable information.

Test Credential Program and Ecosystem Development

To sustain the momentum of mDL implementations after the hackathons, the CA DMV launched the mDL Test Credential Program in summer 2025. Building on the hackathon tooling and support, the Program gives organizations access to a DMV test environment, including a test DMV Wallet app and an mDL with dummy data, for development in non-production settings. This allows organizations to design and test mDL use cases without needing the production DMV Wallet or a real California mDL, while following best practices by avoiding the use of Personally Identifiable Information (PII).

Following a successful beta test in fall 2025, the Program was opened to interested organizations—including the California Highway Patrol, New Zealand’s Ministry of Internal Affairs, and Okta—at the end of the year. Within the first month of this controlled rollout, more than 15 organizations had enrolled.

The CA DMV also maintains a growing list of nearly 180 implementers and ecosystem partners, about half of which are public entities implementing or expressing interest in mDLs. The DMV has engaged with these organizations over the past 2.5 years through use-case development and broader ecosystem collaboration.



Participant Volumes

Since launch on August 15, 2023, CA DMV has provisioned approximately 1.9 million unique mDLs to date, which includes:

- 934,000 in the CA DMV Wallet (launch date: 08/15/2023)
- 1,000,000 in Apple Wallet (launch date: 08/23/2024)
- 139,000 in Google Wallet (launch date: 09/19/2024)
- 7,000 in Samsung Wallet (launch date: 04/27/2026)

Awards

CA DMV received the [2023 Gartner Eye on Innovation for Government Award](#), in the category of provisional, state, or regional and nominated for the [2025 Gartner Eye on Innovation for Government award](#), in the category of disaster relief and unhoused.

PRODUCT REVIEW

CA DMV Wallet

The CA DMV Wallet is a digital solution designed to provide a fast and reliable identity/age verification process and a more convenient way to manage CA DMV related needs. This digital wallet allows mDL holders to store and access their DL/ID cards, vehicle registration, and other vital documents electronically, all while enabling mDL holders to manage their motor vehicle related business, such as renewing their DL/ID cards and/or vehicle registration. The transition from a physical DL/ID card format to digital management is a significantly crucial step towards modernization and efficiency. The CA DMV Wallet can be used to digitally store and access essential documents from anywhere, at any time, and thus mitigate risks of fraud/identity theft, loss or damage. It also provides fast, convenient, and secure access to CA DMV's online services including applications for a Disabled Person Parking Placard (DPPP) or accessing their "My DMV" account with automatic login using mDL identity verification. CA DMV continues to integrate mDL into additional online services to provide the public with a secure and convenient way to prove their identity when conducting CA DMV business transactions online.



Privacy and Security Features

The privacy of an mDL holder has been paramount in the mDL design process from the start. Great care has been taken to ensure that methods and means are available to protect mDL holder privacy.

Based on an independent evaluation by a third-party privacy and security firm, the mDL in the CA DMV Wallet is compliant to all the technical and operational privacy and security criteria's and guidelines as outlined by the American Civil Liberties Union (ACLU), Electronic Frontier Foundation (EFF), and Electronic Privacy Information Center (EPIC) together and as in the public comments related to the U.S. Department of Homeland Security's (DHS) mDL program ([2021-07-29 - ACLU EFF EPIC comments re DHS's mDL](#)).

CA DMV's mDL program follows the American Association of Motor Vehicle Administrators' (AAMVA) Implementation Guidelines, which closely adhere to the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 18013-5 mDL specification. It is flexible enough to accommodate the W3C's Verifiable Credential Standard. The CA mDL platform meets the majority of the AAMVA Implementation Guideline requirements.

CA DMV Wallet mDL holders' account data and personal information is protected with advanced encryption technologies. Additionally, biometric authentication on the mobile device with the mDL ensures that only the intended DL holder person can access and share mDL account data and personal information. Accessing the mDL requires biometric authentication or pin code to unlock the CA DMV Wallet and access encrypted personal data. CA DMV prohibits the use of the mDL and requires the mDL holder to re-enroll if biometrics are deleted or altered on their mobile device, or the device is replaced.

Data minimization and selective data disclosure are essential components of the mDL ecosystem, which enables the capability of sharing the appropriate portion of Personally Identifiable Information (PII) and choosing with whom it is shared via a consent-based information sharing flow. For example, when sharing their mDL to a verifying party, mDL holders are prompted to share specific PII data elements. A notification appears on their mobile device, and they can accept or decline which data elements they wish to share with the verifying party. For example, in a transaction to verify that a customer's age is over a specific threshold, only a picture of the mDL holder and an indicator displaying they are over or under that age will be shared with the verifying party. For law enforcement stops, all PII that is currently shared on a physical DL/ID card can be shared if the mDL holder accepts the request. This gives the mDL holder full control of what data they wish to share or not and with whom. This has significant privacy and security benefits protecting Californians from misuse of personal data. California implementation also prevents knowing and tracking the use of mDL by CA DMV, adhering to the strict consumer privacy standards in the State.

A crucial function of the privacy and security features designed into the CA DMV Wallet is to restrict permanent retention of account data and personal information, other than the mDL holder's phone number and an encrypted digital image of their physical DL/ID card. The following are additional measures CA DMV took to protect mDL holder's PII:

- mDL information is stored in encrypted form upon rest and transit.
 - ▶ At rest, mDL info is encrypted using AES-256 and protected by hardware-backed key storage.
 - ▶ Data in transit is protected using TLS 1.2 or higher, utilizing AES-GCM encryption with elliptic curve key exchange.
- Private key material is protected in a hardware security module designed for the safekeeping of key material.
- The mDL holder must be authenticated when any mDL data is accessed or released, at a point in time that is sufficiently close to the time of access or release.

- The CA DMV Wallet does not track nor report locations where an mDL has been presented.
- mDL data is shared with ISO/IEC compliant verifiers, using 18013-5 Device Engagement over Quick Response (QR) code, Near Field Communication (NFC) and Device Retrieval using Bluetooth (BLE) for transmission of mDL data itself.
- “Device Engagement” and “Device Retrieval” are defined terms in the ISO/IEC 18013-5 specification, which inform how the mDL is shared in-person.
- ISO/IEC 18013-7 specification, utilizing an over-the-internet interface will be implemented for online presentment, once there are significant indications of increased demand for these use-cases.
- Both ISO/IEC 18013-5 and 18013-7 specifications:
 - ▶ Provide protection against engagement/request information being forwarded by an attacker to an mDoc (a document or application that resides on and/or requires a mobile device to access the document or application) by binding the presentment to the originating request channel.
 - ▶ Provide, or are used with, a data transfer protocol that allows the mDL verifier to convey information and delivers messages to the mDL Wallet application.
 - ▶ Have been approved by the AAMVA Identity Management Committee.
- To ensure mDL holders always possess a valid mDL, CA DMV implemented a required periodic refresh cycle, which forces mDLs in the CA DMV Wallet to refresh every (30) days or when a significant change is made to the driver license. This forced refresh performs a validation of the mDL holders motor vehicle record and ensures that their mDL reflects the real-time status of their physical DL/ID. This prevents mDL holders from presenting their mDL if they have any stop on their Motor Vehicle Record, such as their DL is expired, suspended, or revoked.
- CA DMV also purposely limits the amount of data that is displayed when the mDL holder views their mDL on their mobile device. This helps to avoid “flash pass” scenarios in which an mDL holder may try to just show the face of their mDL to a verifying party without it being electronically verified. mDLs must always be electronically verified to be trusted.
- CA DMV sends follow-up alternate communication via email to those who have been issued an mDL and have a registered and verified online account and email address with the CA DMV. The email notifies the registered CA DMV online recipient that an mDL has been issued in their name and enables them easy access via an online portal to either cancel the mDL or report fraud directly to CA DMVs’ Investigations Unit. In fact, in the case of stolen identity, this process identified a fraudster and stopped them from proceeding as well as generating evidence for further investigation by DMV investigations team.

- To maintain trust in the integrity of the mDL, CA DMV adheres to industry standards, best practices, and recognized security principles regarding public and private key management. Asymmetric cryptography is used to provide digital signatures and secure key exchange, ensuring the authenticity, integrity, and controlled access of mDL data. These cryptographic mechanisms define secure communication protocols and data structures that allow the mDL to be provisioned, stored, and verified using a mobile device while maintaining security and user privacy.
- Encryption at rest and in transit utilizes NIST-approved cryptographic algorithms, including AES-256 for data protection and elliptic curve cryptography for key exchange and digital signatures. Cryptographic keys are protected using hardware-backed secure storage mechanisms available on modern mobile devices. Where applicable, cryptographic modules used within the system are designed to align with Federal Information Processing Standard (FIPS) 140-3 security requirements for validated cryptographic modules.
 - ▶ A Public Key is a cryptographic code that encrypts data using cryptographic algorithms based on one-way mathematical functions. These functions are easy to compute in one direction but extremely difficult to reverse, ensuring the security of the cryptographic process. The trust model for mDL relies heavily on security in the public-private key relationship. This includes incorporating physical and technical security access controls to ensure that access to the key administration infrastructure is limited only to authorized individuals who have a direct need for this.
 - ▶ A Private Key is a crucial component that defines the secure communication protocols and data structure for an mDL and allows it to be provisioned, stored, and verified using a mobile device while maintaining security and user privacy. This key is generated using a well-defined key ceremony with three disparate owners to collaborate and change it and place it in a CA DMV cloud hardware security module accessible to only authorized DMV system administration staff (no contractors).

mDL Verify Feature

To enable a cost free and easy mDL verification process for relying parties such as government and law enforcement agencies, merchants, and service industry personnel, the CA DMV Wallet has integrated mDL verification functionality within the CA DMV Wallet app as a standalone verifier, which enables any relying party to use the CA DMV Wallet App to verify an mDL once the app is downloaded.

The mDL Verify feature is a QR code scanner, included in the CA DMV Wallet, which provides real-time identity and/or age verification to multiple relying parties, such as government agencies and law enforcement agencies, merchants, and service industry personnel.

When the mDL QR code is scanned, encrypted data transmits directly into relying on parties' back-end identity and/or age verification systems. This is the same process currently utilized when the back of a physical DL/ID card is scanned.

When relying parties scan a unique QR code directly from a mDL holder's mDL, they'll access only relevant information as required for their specific use case. For example, the mDL verifier provides TSA or law enforcement with just the information attributes they seek to verify identity. Whereas retailers and service industry personnel will only have access to the mDL holder's photo and receive confirmation that the mDL holder is of legal age to complete the transaction.

CA DMV's verifier also has near-field communication (NFC) capabilities and can provide verification for both Apple and Google mDLs for relying parties. However, verification beyond confirming one's age is not currently a functionality for the CA DMV's verifier.

Emergency Use Case (EUC)

The emergency use case process has been implemented specifically for those with an existing, valid, and unexpired DL/ID card on record, but the physical card is not currently in their possession, due to an unforeseen circumstance. Before EUC enrollment can be approved, CA DMV must confirm if the customer can locate and obtain their physical DL/ID card after enrollment, or if a replacement DL/ID card is needed.

If the physical DL/ID card cannot be recovered, an application for a replacement DL/ID card is processed, with a fee waiver, per the proclamation of a state emergency and an mDL is provisioned if the customer decides to voluntarily opt-in. However, if the customer acknowledges that they can recover their physical DL/ID card, an mDL is provisioned if the customer decides to voluntarily opt-in.

Instant Identity Card (IIC)

For those affected by natural disasters, who cannot access their physical DL/ID card and their mobile device, may now request a verifiable paper based IIC that is cryptographically temper-evident via a digital signature on the paper document, valid 60 days from the date issued. This solution is intended to provide identification to the unhoused, upon visiting a disaster recovery center.



The IIC has been implemented specifically for existing California residents with a valid, unexpired DL/ID card on record, who need proof of identity immediately to receive benefits from entities such as Federal Emergency Management Assistance (FEMA), California Office of Emergency Services (CalOES), American Red Cross, California Housing and Homelessness Agency (CHHA), Los Angeles and San Francisco temporary housing and relocation services, etc.

An IIC cannot be accepted by just showing the paper document and must be electronically scanned/verified by accessing the [CA DMV Credential Verifier website](#) on a camera equipped mobile device.

When the QR code is scanned, the IIC holder's identity is checked in real time via an encrypted digital key transaction with the CA DMV to ensure the verified identity information is accurate and up to date. To assist those impacted by natural disasters, IICs can be obtained at a Disaster Recovery Center, when applying to replace a physical DL/ID card.

State Issued Documents as Verifiable Digital Credentials

The DMV Wallet technology has been extended to take advantage of the highly secure digital representation of the identity document (the driver's license) and allow for additional State Issued documents like Vehicle Title, Disabled Placard ID to be added to the DMV wallet. This has enabled digital/online verification of these documents and created a convenience and security that was not available prior to this innovation.

mDL Dashboard

The mDL dashboard is a transparent feature on CA DMV's website which displays current mDL adoption rates, locations where CA mDLs are accepted in CA, and which digital wallets CA residents can provision an mDL in. CA DMV continues to add metrics to the dashboard on monthly basis.

mDL Portal

The mDL Portal allows easy and convenient access for mDL holders to view and manage all of their mDL cases. Once logged into the portal via the mDL holder's "My DMV" account, they can opt in or opt out of the mDL pilot program. The opt out option will permanently hinder someone from provisioning an mDL until they opt back into the mDL pilot. The portal also enables mDL holders to cancel their mDL remotely. This feature helps those who may have lost their phone and want to take extra measures to prohibit others from potentially accessing their mDL.



CA DMV also provides a portal function for mDL holders to log complaints around suspected fraud associated with an mDL.

Transportation Security Administration Waiver Compliance

In October of 2024, DHS/TSA released the final proposed rulemaking which amended the REAL ID regulations to allow, on a state-to-state basis, States to issue mDLs to both REAL ID compliant and non-compliant cardholders and establishes the mDL waiver application process. DHS/TSA required states to submit an mDL waiver application to enable federal agencies to continue to accept REAL ID compliant mDLs from specified states post the REAL ID enforcement date (May 7, 2025). This temporary waiver waives the regulatory requirement that mDLs must be compliant with REAL ID requirements. The waiver is temporary, valid for (3) years and is granted by TSA on a state-by-state basis.

This is not the final regulatory action with respect to mDL. TSA intends this rule to be part of an incremental, multi-phased rulemaking that will culminate in the promulgation of comprehensive requirements that enable states to issue mDLs in more permanent compliance with REAL ID. To qualify for the waiver, the final rule requires that states:

- Be in full compliance with all applicable REAL ID requirements as defined.
- Submit an application demonstrating that they meet the requirements specified in the rule.
- States must submit evidence that shows they comply with all provisions set forth in section 37.10(a) & (b) which lists out the application criteria for the temporary waiver.
- Section 37.10(a) lists out provisioning, issuance, privacy, and interoperability requirements states must comply with.
- Section 37.10(b) references the requirement that States must get independently certified.

CA DMV received independent certification from auditors from the California Department of Technology (CDT) and the California Department of Tax and Fee Administration (CDTFA). CA DMV was the first in the nation to be deemed fully compliant and issued the mDL waiver by TSA on May 7, 2025, which is valid until May 1, 2028.

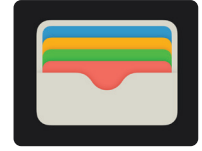
Native Industry Digital Wallets

In a strategic initiative towards enhancing accessibility, utility and convenience, CA DMV installed an innovative feature, which permits mDL holders to provision and present their mDLs not only on the CA DMV Wallet, but on popular native industry wallets such as Apple Wallet, Google Wallet, and Samsung Wallet as well.



Apple Wallet

Enabling iPhone and Apple Watch users, with a valid, unexpired physical DL/ID card, to seamlessly add and present their mDLs. Key Features include:



- **mDL provisioning requests within Apple Wallet**

Adding an mDL to Apple Wallet can be done in a few easy steps. Once in the Apple Wallet, iPhone users can tap the Add (+) button at the top, right of their screen, select "Driver's License or State ID," and follow the onscreen instructions to initiate the mDL provisioning process. Users will be prompted to scan their physical DL/ID card and take a selfie, which will be securely provided to CA DMV for verification. As an additional security step, iPhone users will then be required to complete a series of facial and head movements. Once verified, the mDL will be added to Apple Wallet.

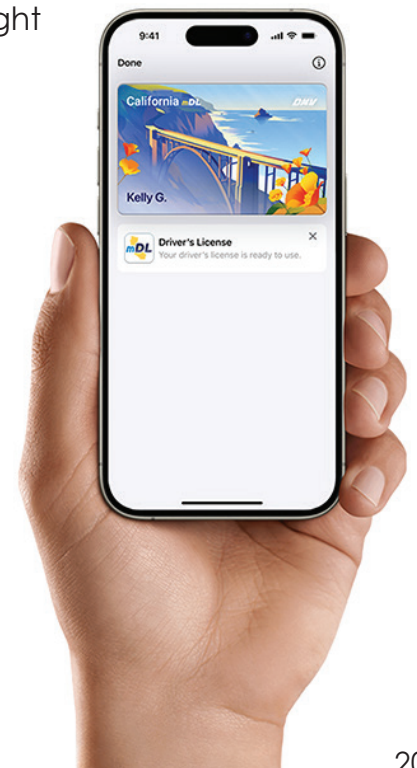
- **Presentment within Apple Wallet**

mDL holders can securely present their mDLs in Apple Wallet in person and in apps to provide proof of identity and/or age. For in-person presentment, mDL holders can select their mDL in Apple Wallet. Once they allow their iPhone or Apple Watch to be read by an mDL reader, they may review the specific information being requested and use Face ID or Touch ID to authenticate.

Currently, mDL holders can present their mDL in Apple Wallet at most airport TSA checkpoints, businesses, and venues, in addition to Apple Store locations across the U.S. for order pickup and Genius Bar appointments. They can also present their mDLs in Apple Wallet to businesses using apps such as Tap2iD Mobile, VeriScan, and Mobile ID Verify, for in-person age verification. These apps leverage Apple's ID Verifier API to securely and privately verify and accept mDLs right on iPhone, no additional hardware required.

To present an mDL in Apple Wallet in apps, mDL holders can select the "Verify with Apple Wallet" or "Continue with Apple Wallet" button. From there, they can review the specific information being requested and authenticate with Face ID or Touch ID before information is shared. Currently, mDL holders can present their mDL in Apple Wallet in select apps, including Turo and Uber, with additional partners such as CLEAR and MyChart coming soon.

When presenting an mDL in Apple Wallet, only the information needed for the transaction is presented, and the mDL holder has the opportunity to review and authorize the information being requested with secure Face ID or Touch ID before it is shared. mDL holders do not need to unlock, show, or hand over their mobile device to present their mDL.



Google Wallet

Google Wallet, in partnership with CA DMV, enables those with a valid California DL/ID card to add an mDL to Google Wallet. Key features include:



- **mDL provisioning requests within Google Wallet**

With a valid, unexpired physical DL/ID card, the process of adding an mDL may be completed within the Google Wallet on a camera equipped mobile device. When an mDL is requested, images of the valid, unexpired physical DL/ID card, along with a selfie-image are required. The Images are then uploaded as encrypted evidence vectors to CA DMV. The mDL will be added to Google Wallet, once CA DMV has approved the request and the mDL is provisioned. If additional review is needed, Google Wallet may send additional data points to assist CA DMV with resolving the request.

- **Presentment and storage within Google Wallet**

Once mDL holders have added their mDL to Google Wallet, the identity data on the mDL can only be viewed and shared with the mDL holder's authorization, via their mobile device access method (biometrics, passcode, PIN). mDL holders can choose what information will be shared with any relying party. Google Wallet follows the industry ISO 18013-5 standard for secure, interoperable presentation of digital credentials.

- **Remote deletion**

When mDL holders no longer have access to their mobile device containing their mDL, they can remotely delete their credentials in Google Wallet by visiting myaccount.google.com and triggering a remote deletion. mDL holders can also contact CA DMV, for assistance. Once the mDL holder's mobile device is connected to the internet, the mDL is deleted. If the mobile device is offline for a period longer than the provisioning set digital signature expiration, the mDL will also no longer be valid.



Samsung Wallet

CA DMV has partnered with a fourth digital wallet provider, Samsung. This allows CA residents to add their DL/ID to their Samsung digital wallet. Key Features include:



- **mDL Provisioning Requests into Samsung Wallet**

The mDL provisioning process is similar to other digital wallets which allows users to easily load their valid mDL by following a simple procedure. Users tap the "+" symbol on the Quick Access tab and select "Digital IDs" from the menu. The user can then select "Driver's license/state ID" to start the process. A list of supported states is displayed including California. The process continues by requesting the front and back of the physical DL/ID to be scanned along with a brief video of the user's face to prove that he or she is the lawful card holder. The user submits and the DL/ID is added to the wallet once approved by the CA DMV.

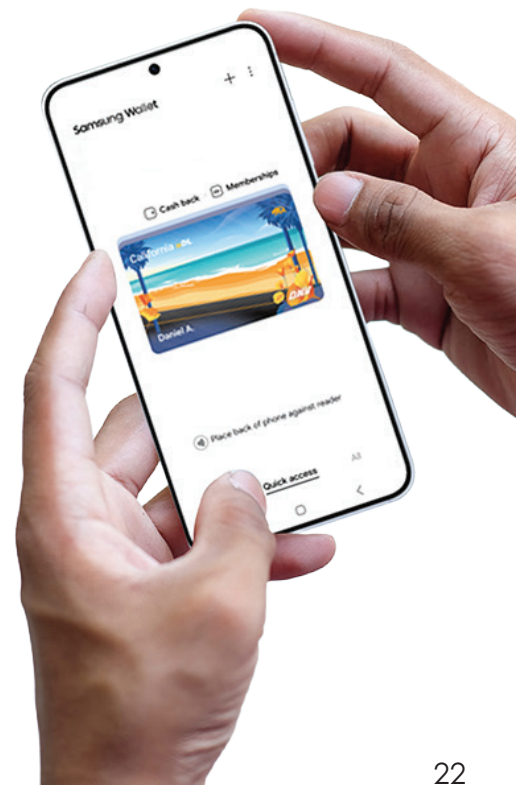
- **Presentment to Relying Parties**

The mDL can be transmitted in person to readers that support the ISO 18013-5 standard. The user simply holds their mobile device over the reader or shares the QR code visible on the mDL. Samsung Wallet will detect the request and display to the user the list of data fields that are requested from the relying party. Data from the mDL can only be transmitted by the lawful owner of the mDL. Users send the data by authenticating with their biometric fingerprint. Typical uses are to grant access through TSA security checkpoints and transactions that require proof of age for age restricted items. .

The mDL can also be shared through mobile apps and web sites. This transmission is similar to in person presentment but relies on the ISO 18013-7 standard for remote presentation. Apps and web sites can request an mDL which can be made available and passed via secure API to the relying party.

- **Secure Storage and Management**

The mDL is stored encrypted in the secure, trusted environment on the Samsung device. Key data is stored on the device embedded secure element separating it from other processing. Wallet contents including mDLs can be deleted remotely through a command on the Samsung user portal giving the user confidence that they can remove the mDL in the event the phone is lost.



LESSONS LEARNED

Similar to the wide range of products and services currently offered, CA DMV utilizes a “lessons learned” strategy as an essential tool for continuous improvement, of not only mDL related products and services, but of the mDL pilot program as a whole. Throughout program development and implementation, documenting problems, analyzing their root causes, identifying areas for improvement and what works best are all considered as necessary components to ensure CA DMV will meet future mDL related goals. The following represents the key lessons learned, associated with mDL development and implementation:

- To achieve optimal interoperability and present lower fraud and security risks to mitigate, it was imperative that CA DMV adhered to all technical and business standards during development and implementation.
- To enable support for multiple use cases, it is/was important for architects to be familiarized with and aware of CA DMVs' digital plan for mDL.
- Remedy heightened provisioning periods (initial launch dates/news story releases) by constructing a robust queueing system to handle spike periods of increased traffic. (Apple had issues on their end and experienced difficulty with managing demand).
- To ensure that products achieve high key performance indicators (KPI) and adoption rates and promote prolonged use, it's important to properly plan mDL holder outreach.
- Law enforcement prefers not to be required to equip an additional, hand-operated, standalone mDL verification device, which could potentially increase the risk to officer safety. CA DMV is working to solve the remote or distance verification limitation, by enabling officers to verify an mDL from a further distance, using Bluetooth technology or something comparable.
- Law enforcement prefers an mDL verifier that would not require the use of the officer's own personal mDL. To accommodate, CA DMV built the mDL Verifier that anyone can download and use without needing to have provisioned an mDL.
- So that mDL holders can report potential issues or suspected fraud associated with their mDL case(s), CA DMV began sending those who have provisioned an mDL a “Congratulatory” email, which includes a dedicated link, which suspected mDL fraud can be directly reported to CA DMV's Investigations Unit.
- Housing agencies and non-profits require proof of identity for filing with the housing packet for unhoused. DMV developed a concept that generates a digitally signed pdf document proving the mDL presentation and also the Driver information.

- For Californians without a mobile phone in an emergency situation, an instant proof of identity would enable faster access to public assistance. DMV worked on an innovative concept to extend the mDL technology to work on a paper document called Instant Identity Card.
- For Californians planning air travel but stranded due to lost driver's license card, there was no option to get an mDL without a field office visit. CA DMV innovated again to design a remote identity verification flow (over video) and transmit the mDL without the need to access their physical driver license.
- Many State entities are reluctant to adding a new technology to their existing services. This remains an existing challenge with some encouraging developments using open-source code provided by CA DMV to short circuit the mDL use in their business flows.

FISCAL IMPACT

The DMV received an appropriation of \$10 million from the General Fund in the 2021 Budget Act to begin the development of an mDL Program. The funding was expended on the creation and release of the DMV Wallet Application for the pilot, launched on August 15, 2023. The costs included consultant, software, and service costs.

The DMV estimates that \$9.5 million is required to continue the mDL Pilot Program in 2026-27. The estimated costs include approximately \$1.8 million for state staff resources to support information technology, additional program workload, and policy. In addition, \$7.7 million is estimated for technology implementation and support services. The following table details the estimated costs needed to support an mDL Pilot Program in 2026-27 and annually while the department prepares for statewide implementation. Given the condition of the Motor Vehicle Account, the Department has requested \$5 million for technology support services including the mobile wallet build and support, photo and identity matching, AWS infrastructure, and program manager resources to continue the mDL Pilot Program in 2026-27.

Fiscal Impact	FY 2026-27
Additional Program Workload	\$549,000
Information Technology & Policy Support	\$1,244,000
Mobile Wallet Build & Support	\$1,000,000
Photo and Identity Matching	\$2,500,000
AWS Infrastructure	\$1,250,000
Product Managers	\$250,000
Salesforce Development/Support	\$1,450,000
MuleSoft Support/License	\$872,000
Marketing Support	\$350,000
SimpliGov Workflow	\$50,000
Total Fiscal Impact:	\$9,515,000

The technology and support service costs indicated in the table above include the following:

- **Additional Program Workload** – program staff resources are responsible for performing extended review of mDL applications and to provide assistance to mDL applicants
- **Information Technology & Policy Support** – staff resources for Cloud and Security Engineers, Business Analysts, Security Specialist, and policy subject matter experts
- **Mobile Wallet Build & Support** – consultant services to support the mDL application and continue development required to continue the expansion of the DMV Wallet
- **Photo and Identity Matching** – support services related to biometrics, validation of identity documents presented by applicants, and integration with existing departmental systems needed for identify verification
- **AWS Infrastructure Costs** – AWS cloud services that are applicable to all platforms of the mDL wallet(s)
- **Product Manager** – product management services for the development and implementation of the various products used for the mDL Pilot
- **Salesforce and MuleSoft Support/Licenses** – support and maintenance of the Salesforce platform and MuleSoft services utilized for the mDL Program IT solution
- **Marketing Support** – to continue outreach activities and provide information to the public related to the mDL program, its uses, and benefits
- **SimpliGov Workflow** – supports maintenance and development required for this workflow tool that allows efficient assignment of cases that require additional processing with a technician

The department will determine future cost estimates for the permanent mDL Program based on the pilot data and utilization trends through the Project Approval Lifecycle process with the California Department of Technology. DMV anticipates that the majority of the information technology resources to support the mDL technology solution are required on an ongoing basis with additional costs fluctuating based on the annual mDL applications received. The ongoing costs include information technology positions, additional program workload resources, mobile wallet support, photo and identity matching, AWS infrastructure, Salesforce/Mulesoft licenses and support, and SimpliGov workflow costs. Total ongoing workload and information technology costs are estimated at \$7.6 million annually.

In terms of return on investment, mDLs introduce advanced safety and security features, which surpass the capabilities of traditional physical credentials.

- The incorporation of selective disclosure empowers mDL holders to make informed decisions regarding the specific information they choose to share, thereby providing mDL holders with heightened control over interactions and information dissemination. This provides quantifiable privacy benefits by reducing the vulnerabilities associated, such as loss, theft, or fraud (over \$600 avoided per instance of fraud on average and over \$180,000-\$500,000 per convicted fraud case)
- Based on discussions with various law enforcement agencies, the technology also holds potential for noteworthy advancements in traffic enforcement and officer and driver road safety with reduced roadside stop time as this technology can help prepopulate data fields within the citation management tools
- Additionally, digital identity proofing enabled by mDL reduce identity proofing cost of operations (third party costs and manual work) while reducing online services fraud. There is also macroeconomic benefit of improved access to underserved and disabled population with the enablement of more online services via mDL.

RECOMMENDATIONS

CA DMV's mDL pilot has demonstrated that this technology benefits Californians. The continuously expanding participation rate confirms a desire by Californians for this offering. CA DMV's mDL will reduce fraud, improve the customer experience, lower the demand for in-person service at DMV field offices, and create cross-agency efficiencies.

CA DMV recommends continued investments in this technology and its multitude of uses for Californians. Full mDL implementation and general release beyond the pilot program would enable CA DMV to continue to:

- Collaborate with other state agencies on mDL integration efforts into their ecosystem thus providing them with a trusted and secure means to process and administer their product(s) expeditiously and reliably
- Integrate digital identification verification into state agencies' ecosystems which would heighten the online identity proofing process and curtail fraudulent attempts, thus potentially saving the state millions of dollars in identity proofing and fraud avoidance
- Expand the open-sourced principles to reduce technical implementation friction for State and Commercial entities interested in the technology
- Create live demonstrable features on how the mDL can be used by a variety of California State Agencies to verify identity, and and improve online/digital access
- Collaborate and solve for how mDL can be used on to enable and enhance the California Department of Technology's [Digital ID Framework](#)
- Prepare for the transition and scaling of the mDL from a pilot program to a statewide program and develop a clear and comprehensive plan for the rollout, communication, and support of the mDL
- Allocate funds to enable digital identity services and other new use cases for mDL holders, powered by the mDL (includes investments required for multiple third-party native wallets and other identity technologies and platforms)
- Continue to monitor and evaluate the performance and feedback of the expanded mDL program and use the data and insights to inform future improvements and decisions including mDL being accepted as an alternate form of identity by various relying parties

- Pursue additional collaborations, integrations and interoperability securely with other mDL and digital identity initiatives, across US states, federal government and international communities
- Engage in mDL use case expansion efforts, for both online and in-person presentment, which would include law enforcement agencies such as the California Highway Patrol, county and city police and sheriff's departments. The focus of this collaboration would be to assess and solve for the law enforcement accepting mDL as a valid form of identification in a safe manner
- Initiate the integration of mDLs into critical public and private sector business workflows to expand the network of relying parties and stimulate growth of the ecosystem with focus on accessibility, user-experience, fraud prevention, and macroeconomic cost savings. This would include enabling access to additional online services via a secure, privacy preserving and simplified means

OUTREACH MATERIAL

Your CA Driver's License on Your Phone

DMV Wallet & Mobile Driver's License Pilot Program



Opt-in at dmv.ca.gov/dmvswallet
Limited to 1.5 million participants.



At security checkpoint:*
• Show digital card to TSA
• Scan QR Code
• Snap a photo
• Proceed to screening

* where available

Your CA Driver's License on Your Phone

DMV Wallet & Mobile Driver's License Pilot Program



Opt-in at dmv.ca.gov/dmvswallet
Limited to 1.5 million participants.



At security checkpoint:*
• Show digital card to TSA
• Scan QR Code
• Snap a photo
• Proceed to screening

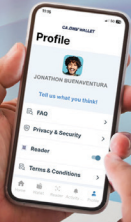
* where available

Airport Marketing Digital and Print

DIGITAL. SECURE. CONVENIENT.

mDL for Businesses and Government

GET STARTED




VERIFY AGE AND IDENTITY

USE THE mDL READER for Business and Government

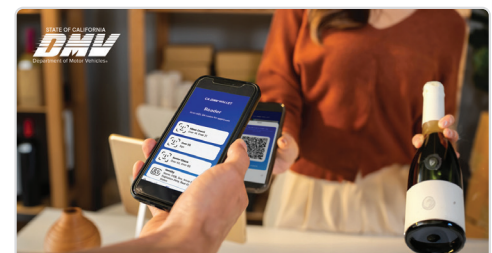
GET STARTED




DMV Website Banners



Social Media



VEHICLE CODE §13020

13020. (a) The department may establish a pilot program to evaluate the use of optional mobile or digital alternatives to driver's licenses and identification cards, subject to all of the following requirements:

(1) Any pilot program established by the department pursuant to this subdivision shall be limited to both of the following:

(A) Persons who have voluntarily chosen to participate in the pilot program.

(B) No more than 15 percent of licensed drivers for the purpose of evaluation.

(2) A participant in any pilot program established by the department pursuant to this subdivision may terminate their participation in the pilot program at any time, and may, upon termination, request the deletion of any data associated with their participation in the program. Within 10 days of any such request, the department and all entities contracted with the department for the purpose of effectuating the pilot program shall delete all data collected or maintained pursuant to the participant's participation in the program.

(3) All participants shall receive both a physical and, if requested, an immutable and unique driver's license or identification card.

(b) In developing and implementing the use of digital driver's licenses and identification cards, the department shall ensure the protection of personal information and include security features that protect against unauthorized access to information, including, but not limited to, all of the following:

(1) Ensuring that any remote access to the digital driver's license or identification card shall require the express, affirmative, real-time consent of the person whose digital driver's license or identification card is being requested for each piece of information being requested, and shall be limited to only that information which is provided on a physical driver's license or identification card.

(2) Ensuring that the digital driver's license or identification card, as well as any mobile application required for the digital driver's license or identification card, shall not contain or collect any information not strictly necessary for the functioning of the digital driver's license, identification card, or mobile application, including, but not limited to, any information relating to movement or location.

(3) Ensuring that the information transmitted to the digital driver's license or identification card, as well as any mobile application required for the digital driver's license or identification card, is encrypted and protected to the highest reasonable security standards broadly available, including ISO-18013-5, FIPS 140-3, and NIST 800-53 Moderate, and cannot be intercepted while being transmitted from the department.

(c) (1) In the conduct of any pilot program pursuant to this section, any data exchanged between the department and any electronic device, between the department and the provider of any electronic device, and between any electronic device and the provider of that electronic device, shall be limited to those data necessary to display the information necessary for a driver's license or identification card.

(2) An entity contracted with the department for this purpose shall not use, share, sell, or disclose any information obtained as part of this contract, including, but not limited to, any information about the holder of a digital driver's license or identification card, except as is necessary to satisfy the terms of the contract. Upon termination or expiration of any contract entered into for this purpose, the contracting entity shall delete any data collected or generated in the course of activities pursuant to that contract within 30 days.

(d) (1) The holder of a digital driver's license or identification card shall not be required to turn over their electronic device to any other person or entity in order to use the digital driver's license or identification card for identity verification.

(2) The holder of a digital driver's license or identification card showing or turning over their electronic device to any other person or entity in order to use the digital driver's license or identification card for identity verification shall not constitute consent to a search, nor shall it constitute consent for access to any information other than that which is immediately available on the digital driver's license or identification card. Information incidentally obtained in the process of viewing a digital driver's license or identification card in order to verify the identity of the holder shall not be used to establish probable cause for a warrant to search the electronic device.

(3) Any request for remote access to their digital driver's license or identification card for identity verification shall require the express consent of the holder of the digital driver's license or identification card, shall be limited to the content of the digital driver's license or identification card specified in the request for remote access, and shall not exceed the information available on a physical driver's license or identification card.

(4) Consent to remote access to a digital driver's license or identification card by the holder shall not constitute consent to a search, nor shall it constitute consent for access to any information other than that which is immediately available on the digital driver's license or identification card. Information incidentally obtained in the process of remotely accessing a digital driver's license or identification card shall not be used to establish probable cause for a warrant to search the electronic device.

(e) (1) A participant in any pilot program established by the department pursuant to this section shall not be required to use a digital driver's license or identification card rather than a physical driver's license or identification card for the purpose of identity verification, nor shall their participation in the pilot program preclude their use of a physical driver's license or identification card under any circumstances.

(2) A person or entity shall not provide preferential service based on a person's use of a digital driver's license or identification card rather than a physical driver's license or identification card.

(f) The pilot program may include the issuance of mobile or digital Real ID driver's license or identification cards upon authorization of the United States Secretary of Homeland Security.

(g) If the department conducts a pilot program authorized in subdivision (a), the department shall, no later than July 1, 2026, submit a report regarding the pilot program to the Legislature, in compliance with Section 9795 of the Government Code, to include, but not be limited to, all the following:

(1) A review of all products evaluated in the pilot program and of the features of those products. The report shall note any security features to protect against unauthorized access to information.

(2) Lessons learned from the pilot program with regards to the utility of a mobile driver's license program, or risks and solutions related to the implementation of a mobile driver's license program.

(3) Recommendations for subsequent actions, if any, that should be taken with regard to alternative options for digital driver's licenses or identification cards evaluated in the pilot program.

(4) An estimate of the fiscal impact of the deployment of a mobile driver's license program, including the estimated impact to the Motor Vehicle Account established pursuant to [VC §42271](#).

(h) As part of the 2022–23 budget, the department shall report to the Legislature on the status of the pilot program, including, but not limited to, all of the following:

(1) The scope of the pilot program, including pilot program goals and processes.

(2) The timeline for the pilot program.

(3) The fiscal impact of the pilot program.