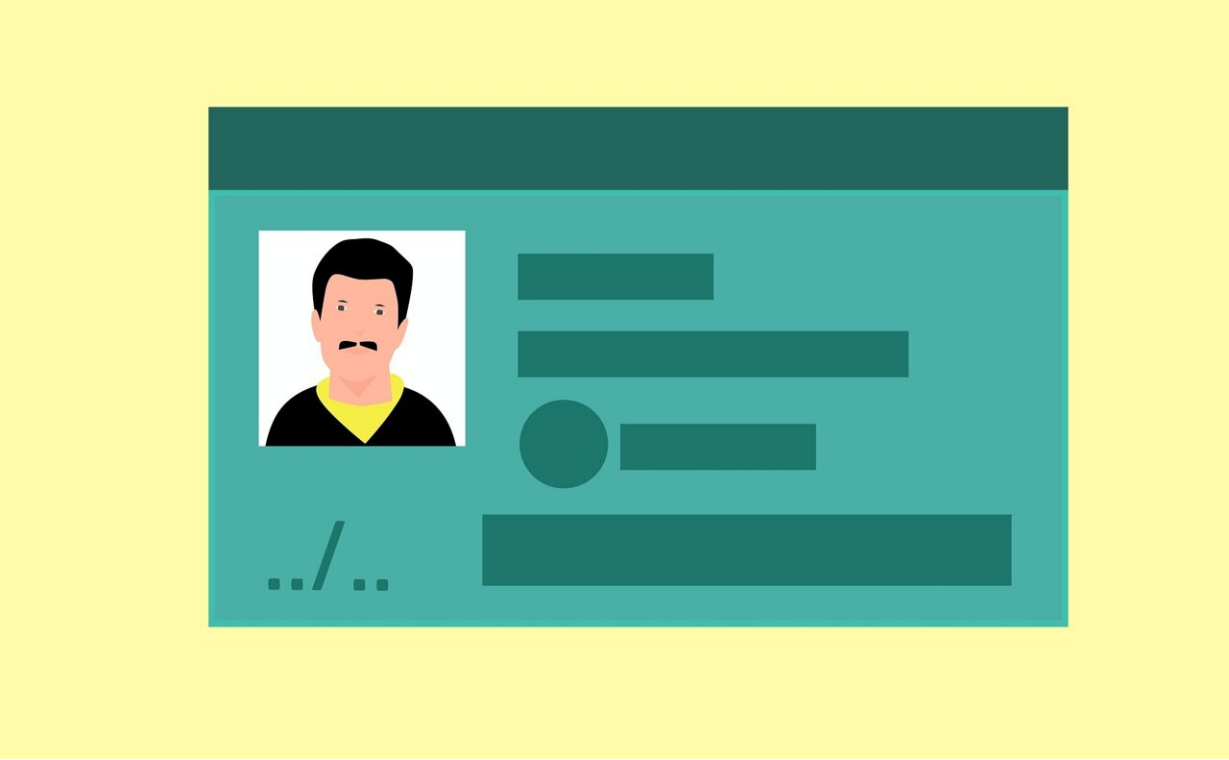
California will test digital driver's licenses. Is personal info at risk?

May 25 2022, by Jon Healey, Los Angeles Times



Credit: Pixabay/CC0 Public Domain

Are Californians ready for yet another new version of the driver's license?

The last one—called "Real ID"—went over about as well as CNN+. As

of April, less than half of the state's drivers had obtained one, even though Californians will need a Real ID or a passport to get on a plane or enter a federal building in a year. The tepid reaction may stem from the fact that these IDs offer no new benefits to drivers, just another time-consuming obligation.

Now the state's Department of Motor Vehicles is planning to test a version called a mobile driver's license or digital ID—an identity-verifying credential stored on your smartphone. And unlike Real ID, a mobile license could give you more control over your personal information, although critics say a poorly designed system would threaten your privacy.

Louisiana, Colorado and Arizona already have rolled out mobile licenses, and Utah is testing them. Other countries, including Germany and New Zealand, are also creating digital identity systems. Yet the technology is still in its early days, experts say, with some key pieces unfinished.

Here's a rundown of how mobile licenses would work, the benefits they could provide and the potential drawbacks.

What's the point?

Eric Jorgensen, director of Arizona's Motor Vehicle Division, said in a recent interview that the goal is to improve security, privacy and convenience. "It's not about balancing one against the other," he said. "It's an attempt to make all three of those better."

The easiest way to understand the push for change, though, is to consider the problems with conventional driver's licenses.

The 9/11 terrorists used fraudulently obtained state IDs to board the planes they hijacked, putting an exclamation point on the vulnerabilities

of physical ID cards. That day's events prompted the federal government to pass the Real ID Act in 2005, which set higher standards for how licenses were designed and issued. The goal was to deter the cards from being counterfeited or obtained by people who were not legal residents.

Real ID was no panacea, however. While the watermarks and other design features were hard to copy, they were also hard for the untrained eye to recognize. You almost have to be a security expert to detect them, Jorgensen said.

And like all physical IDs, conventional licenses are not much help when it comes to verifying your identity on the internet. They're not useless—see, for example, how ID.me uses licenses and smartphone cameras to verify identities online. But you have to jump through a lot of hoops on the web to prove that the ID card you're using actually belongs to you, and the process is still vulnerable to scamming.

Another problem with physical ID cards is that they can share too much information. When that creepy bouncer at the nightclub door demands proof that you're old enough to enter, you can't just show him the birthdate on your license. You have to show him the whole thing, revealing your name and address in the process. Ugh. (And as Jorgensen points out, nothing stops the bouncer from taking pictures of every license shown at the door.)

In addition, the information laminated into permanence on a physical ID is not, itself, permanently accurate. And nothing on the card will signal that it has incorrect information; the only way to verify details like your current name and address is to access the DMV's database.

And finally, even a counterfeit-proof, updated ID card can't confirm that the hand holding it belongs to the person who obtained it. There's information on the card that a cashier or clerk can check against a

person's physical appearance, but that's hardly a foolproof system of verification.

How would a mobile license be different?

The shortcomings of driver's licenses are part of a larger problem with how people go about answering the question "Who are you?" It's an even bigger challenge online, where identity theft has risen sharply over the past decade. The need for something more secure than ID cards and the ubiquitous login-password combo has inspired numerous companies and inter-industry groups, such as the Better Identity Coalition and the Fast Identity Online Alliance, to promote more reliable ways to verify identity.

In response, the tech world is steadily shifting toward solutions based on "multi-factor authentication." A password is one factor—something only you know. An ID card is a single factor too—something you have. Multi-factor authentication is some combination of something you know, something you have and something you are, such as a fingerprint or facial scan.

That's the approach taken by a mobile driver's license app. It uses the biometric capabilities of your smartphone (something you are) to tie your mobile driver's license or ID to your device (something you have). For certain uses, you could even require a passcode (something you know).

Proponents of mobile driver's licenses say a system built around the technical standard published last year by the International Organization for Standardization addresses all of the shortcomings of a physical license. One caveat is that the ISO standard just covers in-person use at the moment; the standards for online use are still in development.

Imagine, just for example, you're trying to enter that nightclub with the creepy bouncer:

—You can decide whether to let him check your mobile license—he can't do so without your permission. And you don't have to hand the bouncer your phone to display your ID; your license app will exchange information wirelessly with his device.

—You control which pieces of information from your license to share and which to keep concealed. Also, the license app is able to answer some yes/no questions, so it can reveal whether you are old enough to enter without telling the bouncer your birthdate.

—The way the system is designed, none of the information you disclose will be stored by the bouncer's device.

—The mobile license is easier for the bouncer to check too. Instead of him scrutinizing your physical license for watermarks or other anti-counterfeiting features, his device will use cryptographic techniques to confirm that your license is authentic.

—Leave your phone at the bar after overindulging? The mobile license is more theft-resistant than its physical counterpart, thanks to the biometric controls on your phone. Plus, if your phone is lost, you can tell the DMV to revoke your mobile license, rendering it inoperable—in sharp contrast to a revoked physical license, which looks no different than a valid one.

—But let's say a thief somehow manages to unlock your phone and your mobile license, then tries to rent a car with the license before you revoke it. When the thief shares the mobile license data with an agent at the counter, the picture stored with it will be transmitted electronically to the agent's device so he or she can compare it with the person pretending to

be you.

—One other benefit: When you change your address, you can update your information immediately. Similarly, if your driving privileges are suspended or revoked, the digital license would immediately reflect that, yet it would continue to function as an ID.

The two states first out of the gate with mobile license apps—Louisiana and Colorado—acted before the ISO standard was complete, limiting their licenses' interoperability. At this point, Colorado's app is accepted by that state's agencies and police officers, and Louisiana's works with government agencies, state liquor stores and other app users.

To enable broader use of mobile licenses, the American Assn. of Motor Vehicle Administrators, a trade group of DMV officials from across the country, has issued guidelines for mobile driver's licenses built around the ISO standard. And in keeping with a 2020 law, the U.S. Department of Homeland Security is working on ways to verify IDs electronically, using the same standard.

The Transportation Security Administration has started supporting standards-based mobile licenses in Apple's wallet app. At selected airports, Arizona residents with a mobile license from the state can pass through a TSA screening with a single tap of their device, Jorgensen said.

State agencies in Arizona are also starting to accept its mobile driver's license to verify applicants for other state licenses and services, Jorgensen said, adding that retailers and banks have also expressed interest in how they can implement the technology. In the program's first year, he said, about 320,000 Arizona residents had downloaded the mobile license app, and since March about 60,000 had put their mobile ID into an Apple wallet. (The state has more than 5.3 million licensed

drivers.)

Vittorio Bertocci of Okta, whose technology helps businesses verify identities, said that after two decades working on identity issues, "probably for the first time, I see that the standards and the technology are mature enough to give a good base, a good foundation" for mobile ID. "And I see the desire, the investment, from governments," said Bertocci, who is a principal architect at the company.

So what could go wrong?

The fact that there is an international standard doesn't mean every country is using it. Although the U.S. is building around the standard, Bertocci said that European countries are taking a different approach. Companies like Okta can provide ways to bridge the differences so digital ID systems can interoperate, he said, but that sort of arrangement may not be universally accepted.

Nor does everyone have a smartphone or tablet. That's why every mobile license rolled out in the U.S. so far has been a complement to a physical ID, not a replacement for it.

More fundamentally, the notion of shifting IDs from physical to digital is troubling to some privacy advocates. Among other things, they're worried that companies and governments will find a way to use digital licenses to track your movements and learn something about your personal life.

Granted, you leave a digital trail when you use your credit card or smartphone to pay for things away from home. But with a driver's license on a card and a bunch of cash in your wallet, you can go about your business in relative anonymity.

Bill Lamoreaux, a spokesman for Arizona's Motor Vehicle Division, said those concerns are being addressed by the people developing and implementing mobile licenses.

"Mobile ID, as implemented, is device to device," Lamoreaux said. In other words, the device checking your ID doesn't connect to the DMV, so it can't track you. "As the issuing authority, we do not know when or where these are used, as is the case with a physical, plastic license or ID."

Still, Alexis Hancock, director of engineering for the Electronic Frontier Foundation, said the standard for digital licenses includes a way for the app to stay in touch with the agency that issued it, and "it doesn't really effectively address how to limit this."

Jeremy Grant, coordinator of the Better Identity Coalition, said some government officials, especially those in law enforcement, would love to use digital licenses for tracking. And the consequences could be severe: Imagine, Grant said, if licenses could report when a woman went to an out-of-state abortion clinic.

But that kind of tracking can't happen in a properly designed system, he said. Each mobile license will come with the state's encrypted digital signature. When you share information from your license, the verifying device only checks to see whether the digital signature is valid—if so, your ID and the data on it are valid. "They can get a yes/no answer without the state knowing it was you," Grant said.

Beyond that, a standards-based mobile license doesn't transmit a unique identifier when it shares its data. So again, there are no electronic footprints to connect the mobile ID used at nightclub X or brewery Y to the person to whom it belonged.

Before moving forward with mobile licenses, Hancock said, governments need to work through a number of issues that could be raised by putting IDs on smartphones filled with sensitive personal information. For example, she said, what happens if a traffic cop or TSA agent demands that you hand over your unlocked phone for an ID check, even though they can get the information they need from your mobile license without you doing so? What safeguards are there against your phone being unlawfully searched?

Some privacy advocates want to spread out the storage of ID data online, using blockchain or other distributed ledger technology, rather than having it centralized in one state database. Each piece of a person's identity information—name, birthdate, address, picture, etc.—would be stored separately so it could be checked independently of the others. That would reduce the risk of a massive data leak while also ensuring that the government keeps no record of where and when the digital IDs are used.

The decentralized approach, known as verifiable credentials, is being explored by the Canadian province of British Columbia and a coalition of groups across Canada. A bill by state Sen. Bob Hertzberg (D-Van Nuys), SB 1190, would require California by Jan. 1, 2024, to "provide industry standards and best practices" regarding the issuance of verifiable credentials for individuals and businesses.

Grant said his group doesn't have a position on the technical question of how ID credentials are stored, just that the arrangement needs to preserve privacy and be secure. But his personal view, he said, is that the blockchain approaches "introduce some very complicated ways to manage identity and privacy that will overwhelm the average consumer," such as requiring people to "manage a different private [cryptographic] key for every data point about them."

He added, "You can preserve privacy and avoid tracking with technologies that do not require blockchain, and that are easier to implement, easier for people to use, and that scale better."

Some of the most libertarian advocates of the verified credentials approach want to remove the government completely from the identity business. They would have people certify themselves, albeit in some verifiable way. The steep challenge for this group, Grant said, is persuading banks, government agencies and others to accept "self-sovereign" claims, rather than those backed by a DMV or other government agency.

What is California doing?

State lawmakers authorized the DMV last year to do a trial run with mobile driver's licenses and ID cards, giving the department a year to come up with a timeline and cost estimate for the pilot project. At this point, the department is still talking to multiple vendors about possible approaches, with no date set for the launch of any pilots, the department said in an email.

The department declined to say how it would respond to the concerns expressed by privacy advocates. But the authorizing legislation, which lawmakers tucked into a 2021-22 budget trailer bill, laid out a number of mandatory protections for people taking part in the trial, including:

—No forced participation. Only volunteers will be included in the trial, which is limited to 0.5% of the state's licensed drivers, or about 135,000 people.

—No tracking or data mining by your app. Your digital license or ID card and the corresponding mobile app are barred from collecting or holding any information beyond what's needed to perform their stated

functions, "including, but not limited to, any information related to movement or location."

—No sneaky license checks. Before your mobile ID app responds to any request for information, you would have to approve the release of any amount of information.

—No warrantless searches. You cannot be forced to hand over your device in order to verify your ID, nor do you consent to having your device searched if you use it to verify your ID.

—No extra data provided. The information that can be released by the app is limited to what's on your physical driver's license or ID card.

Ultimately, the success of a mobile license will depend on how widely it's adopted—not just by drivers, but by anyone who asks for your ID. There's a bit of a chicken-and-egg problem, Jorgensen said, because there's not much incentive for companies to build apps that support mobile IDs if few people are using them, and states and their residents won't have much incentive to adopt mobile IDs if there aren't many places that accept them.

Yet there are plenty of other factors driving interest in digital IDs among state governments and businesses, particularly national ones. And millions of Americans have already gotten a taste of how their smartphones can be used to verify personal details—they've been using them over the past year to prove their vaccination status.

There's a long way still to go on mobile driver's licenses, though, with basic questions still to be answered about where identity credentials will be stored and how identity will be verified online. At the current pace, Grant said, it will take 10 to 15 years for mobile IDs to get to critical mass.

Californians is likely to have access to one well before that. But the DMV is the agency in charge of this effort, so a long wait time would be on brand.