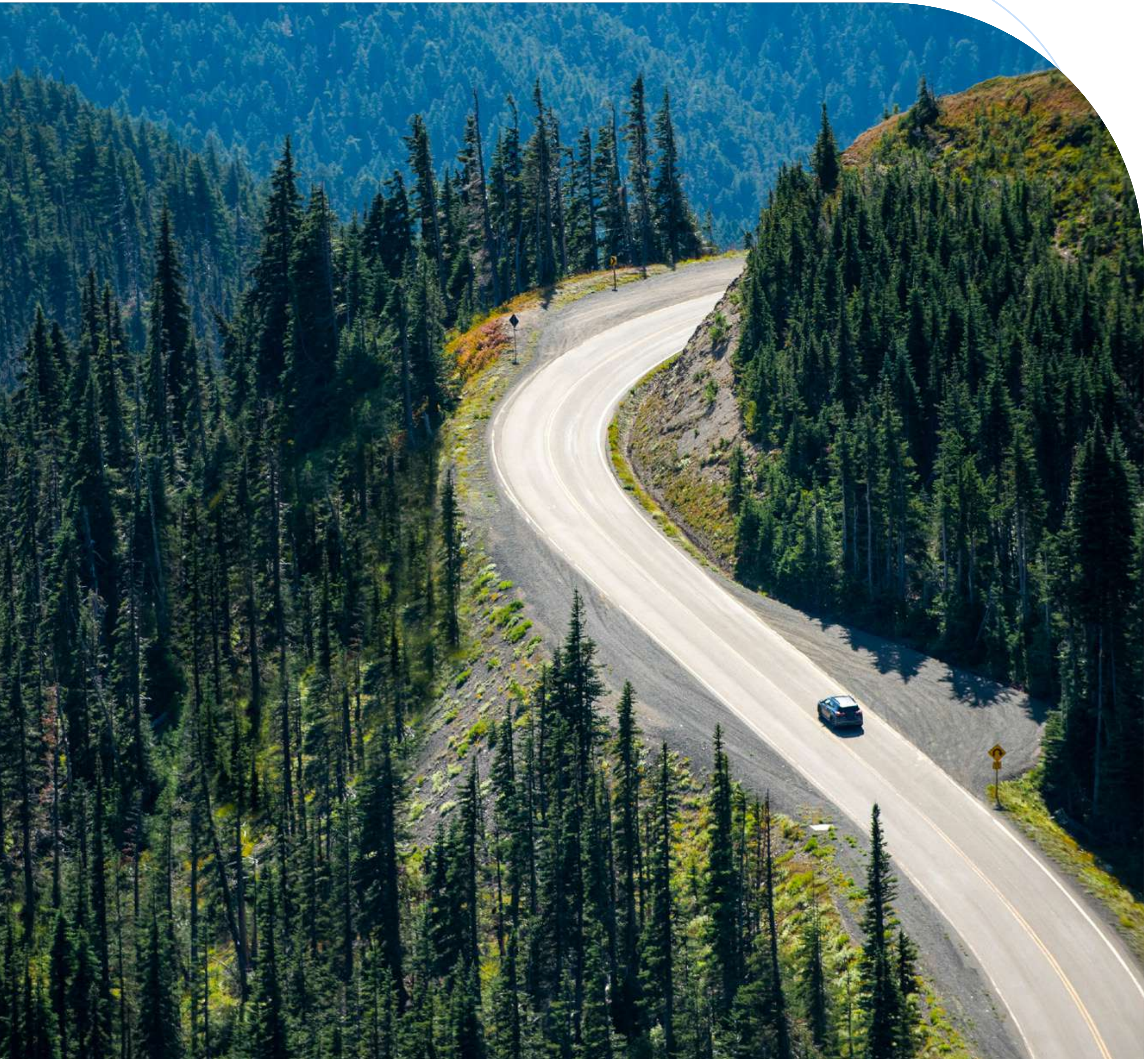
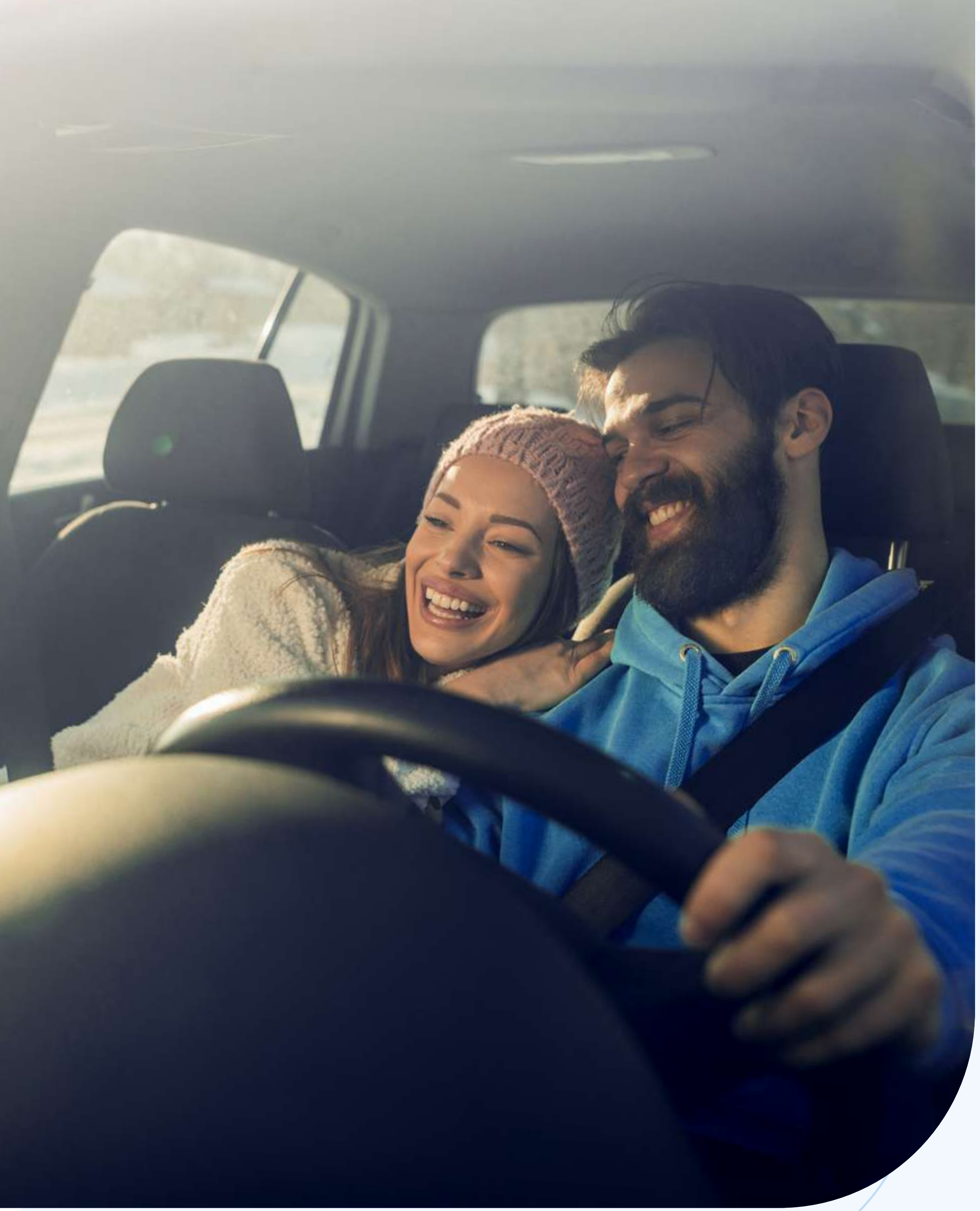


Mobile Driver's License (mDL) Must Haves

Ten Requirements for Selecting the Right Vendor

EBOOK



About This Guide

Mobile driver's licenses (mDLs) are quickly moving from promise to reality in many states across the U.S. Yet with approaches diverging — and technical standards still a work-in-progress — much remains uncertain.

HID has provided secure, convenient and efficient identity solutions to governments across the globe for over 15 years. We are also actively contributing to a wide range of international identity document standards and recommendations, including the ISO 18013-5 mDL standard, ISO 23220 and the work of the American Association of Motor Vehicle Administrators (AAMVA) Card Design Standard committee.

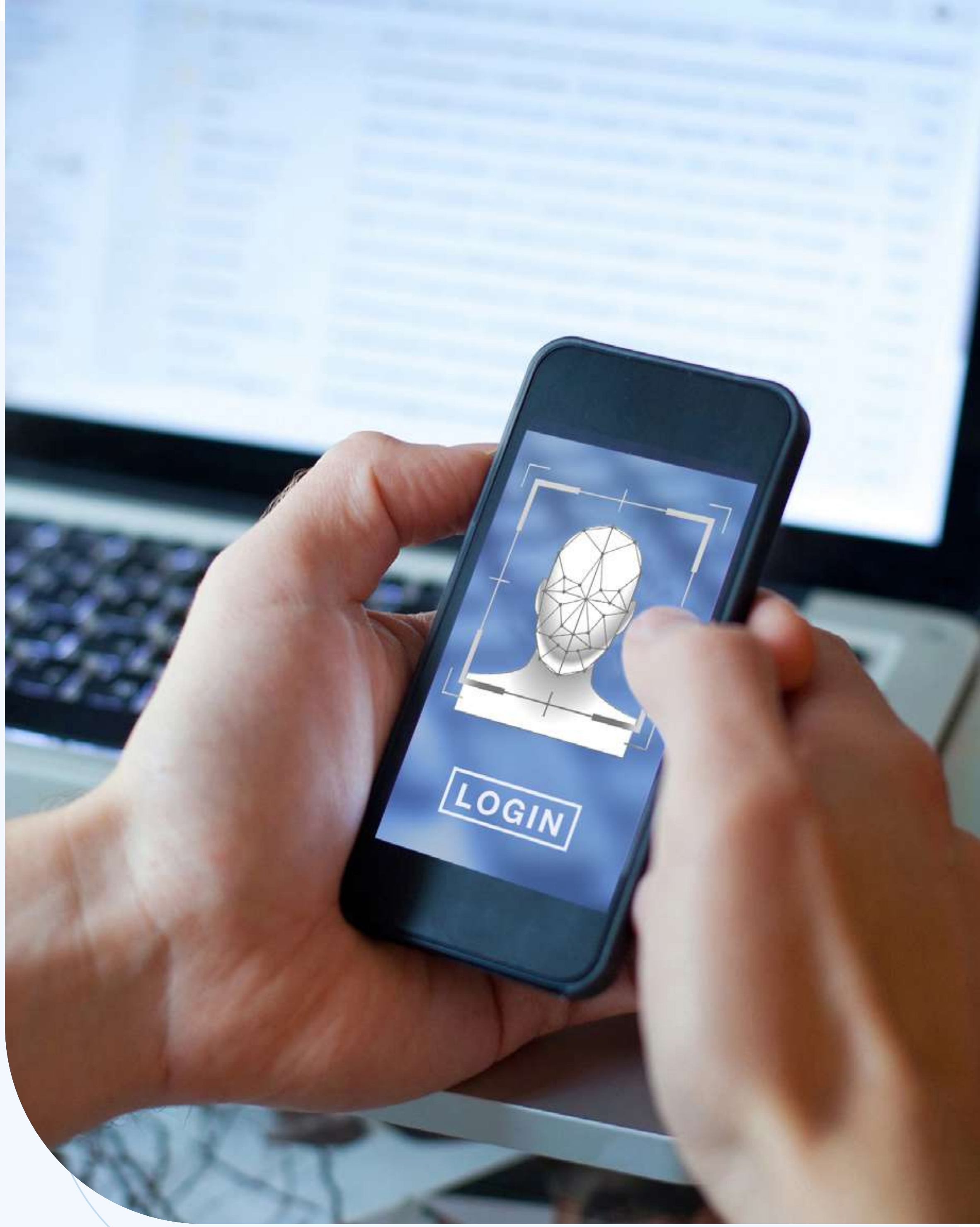
We created this guide to help officials who are planning to deploy an mDL solution understand best practices and make successful decisions in a changing landscape.

The mDL Revolution

It’s not hard to imagine the convenience of being able to store your driver’s license on a device that’s always with you. What if you could verify your age or get through airport security with a simple tap of your phone? What if you never had to wait in line at the DMV again?

There are benefits to security, as well. The biometric security features built into mDLs make them difficult to spoof or fake. Personal data can be wiped out remotely if someone loses their phone and — with it — their digital driver’s license. In many ways, mDLs are more secure than physical cards that are vulnerable to theft, loss, alteration and other forms of exploitation.

But the landscape is changing rapidly. In this guide, we’ll assess different options for developing mDL solutions — and outline ten key requirements to help jurisdictions select the right vendor and position their projects for success.



Getting Started with **mDLs**

A mobile driver's license is a secure digital ID that enables people to store and access the information on their physical driver's license on a smartphone or smart device.

Yet realizing the technology's full potential requires a careful evaluation of your state's needs and capabilities. An mDL must be easy for DMVs to issue and manage, convenient for citizens to use and safe for law enforcement to verify. It should be secure, scalable and compatible with other states' solutions. And it should give jurisdictions the flexibility to add and adapt features as this dynamic market continues to evolve.

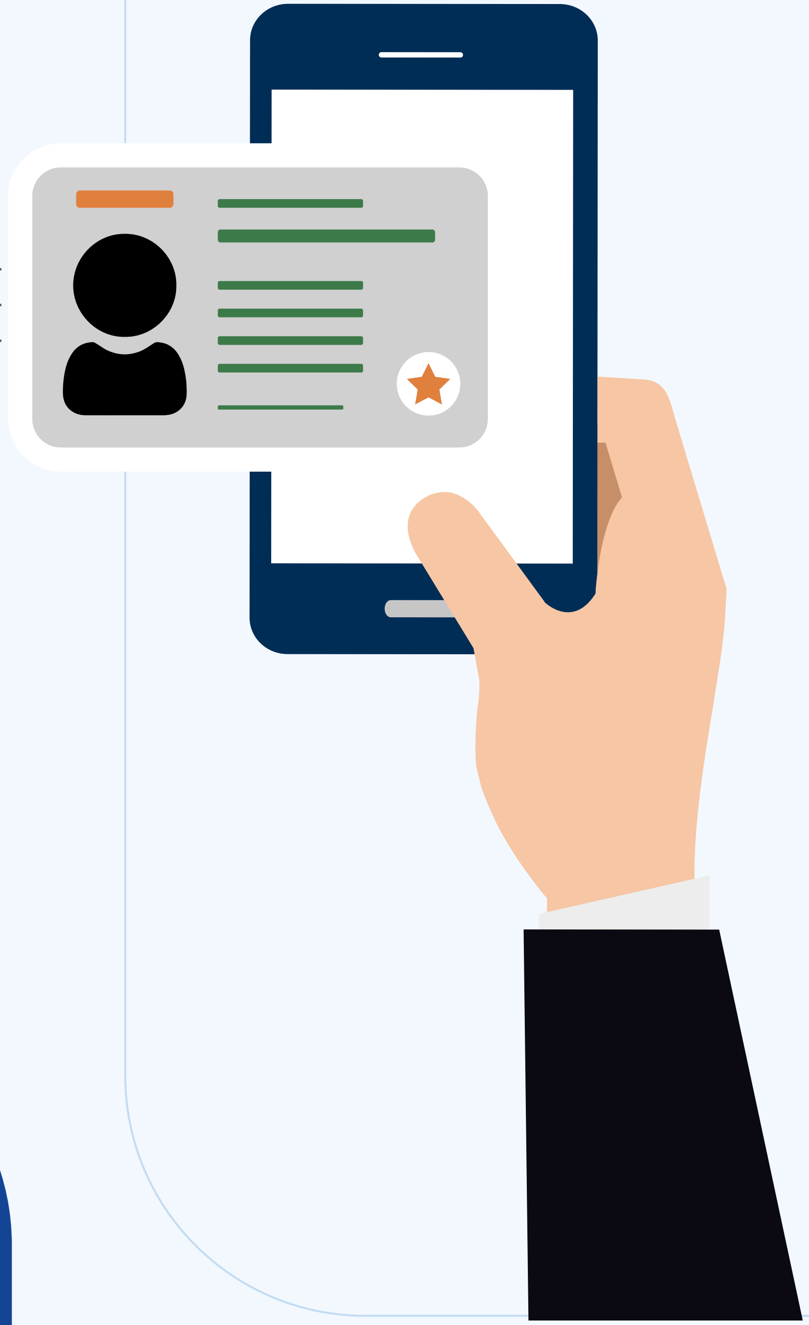
What does that mean for the development process? Jurisdictions should look for vendors and solutions that **deliver expertise while enabling them to customize the features that suit their state's specific needs.**

Understanding the mDL Development Process

End-to-End — The vendor delivers a comprehensive mDL solution that reduces risk but gives issuing authorities few choices when it comes to features, functionality or future developments

Cutomizable Mobile ID Ecosystem — The vendor supplies a set of tools and resources that enable municipalities to assemble — and control — the end result while benefitting from deep knowledge about best practices

DIY — Jurisdictions assemble a team that can design and deliver an mDL, assuming full responsibility for the outcome



Deciding what's best for your state — and which vendors to select as your partner — means evaluating how you'll meet **ten essential requirements for mDL development.** In the following pages, we'll unpack these requirements and help you understand why they're so critical to the success of your solution.

At a Glance: Your Checklist for mDLs Development Success

Your mDL vendor must be able to meet these ten essential requirements:

1 A secure provisioning platform for issuing and managing drivers' mDL

2 Deep experience in electronic and mobile identity solutions

3 A device-agnostic mDL platform that enables you to integrate your mDL into any app of your choosing

4 Full compliance with the technical standards set forth in ISO18013-5

5 Offline data retrieval to increase convenience and decrease security risks

6 A cloud demo and proof-of-concept so you can see how the solution aligns with your needs

7 A safe, convenient solution for law enforcement stops

8 A flexible development platform that enables you to add and adapt mDL features

9 On-device security to protect mDL data across a wide range of driver devices

10 End-to-end encryption to keep drivers' data safe from unauthorized entities

Requirement #1
A Secure Provisioning Platform

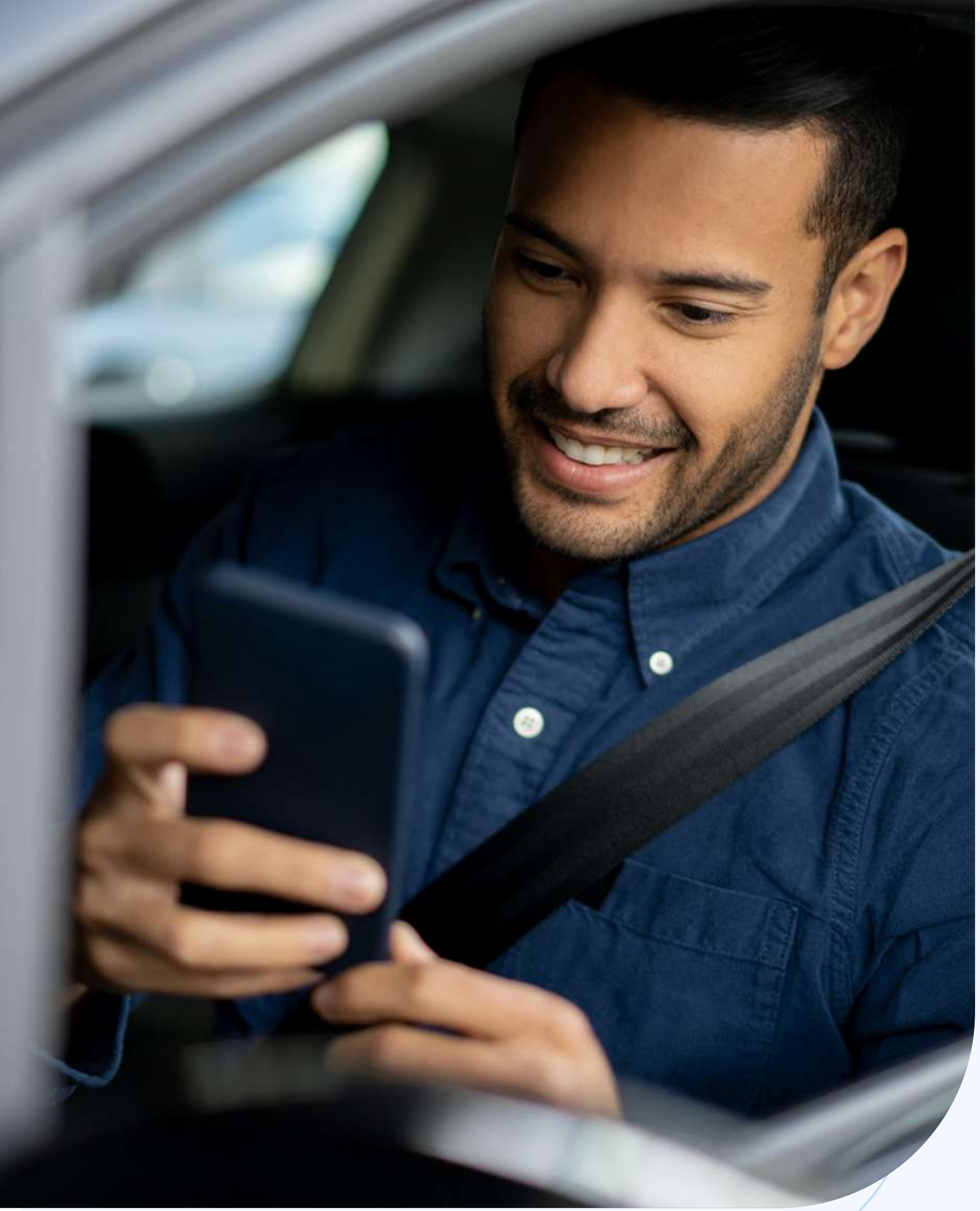
What it is: A provisioning platform enables your state to manage drivers' identities and issue an mDL to their mobile devices. It is imperative to keep this platform secure and safe from attack.

Why it's important: The architecture of your provisioning platform is key to ensuring its security, performance and scalability.

MINIMUM REQUIREMENTS

Vendor provisioning platforms should include:

- **An on-premise provisioning system** — To comply with ISO standards, you must sign every mDL using data from your driver database. These signatures are handled by your provisioning system's data preparation module — using a private key that is easier to secure when it is stored on-premise, behind the government firewall.
- **A provisioning gateway service** — Your provisioning gateway ensures secure, scalable communication between your internal network and your drivers' mobile devices. It will be easier to scale — and more secure — if it is hosted by a vendor with a strong commitment to efficient, secure communication.
- **Secure information storage** — Your solution should be able to securely store each driver's mDL independently of any SIM or Secure Element. Interactions with mDL readers should be managed according to ISO18013-5 standards.



Requirement #2
Experience in Electronic and Mobile Identity Solutions

What it is: Few companies have direct, immediate experience developing mDLs. That doesn't mean it's impossible to vet potential vendors.

Why it's important: Mobile and electronic identities converge in mDLs. Vendors should be able to provide references in electronic identity and data preparation — and point to other mobile identity applications they've developed, like student, employee, residential, hospitality or government IDs. They must also be able to point to an established process and training plan that supports clients during the development process.

MINIMUM REQUIREMENTS

Vendor references should include experience with:

- **Private sector mobile IDs** — Multiple private-sector projects that involve an ID stored on mobile phones
- **Public sector mobile IDs** — Government-issued mobile IDs with the relevant quantity of issuances for a jurisdiction or country with at least the amount of inhabitants in the jurisdiction
- **ID gateways** — Many of provisioning gateway operations for electronic or mobile IDs
- **ID data preparation** — Multiple programs that involve data preparation for government-issued electronic identity documents
- **The U.S. government** — U.S. government-issued identity document with large issuances in the past few years

Requirement #3
A Device-Agnostic Platform

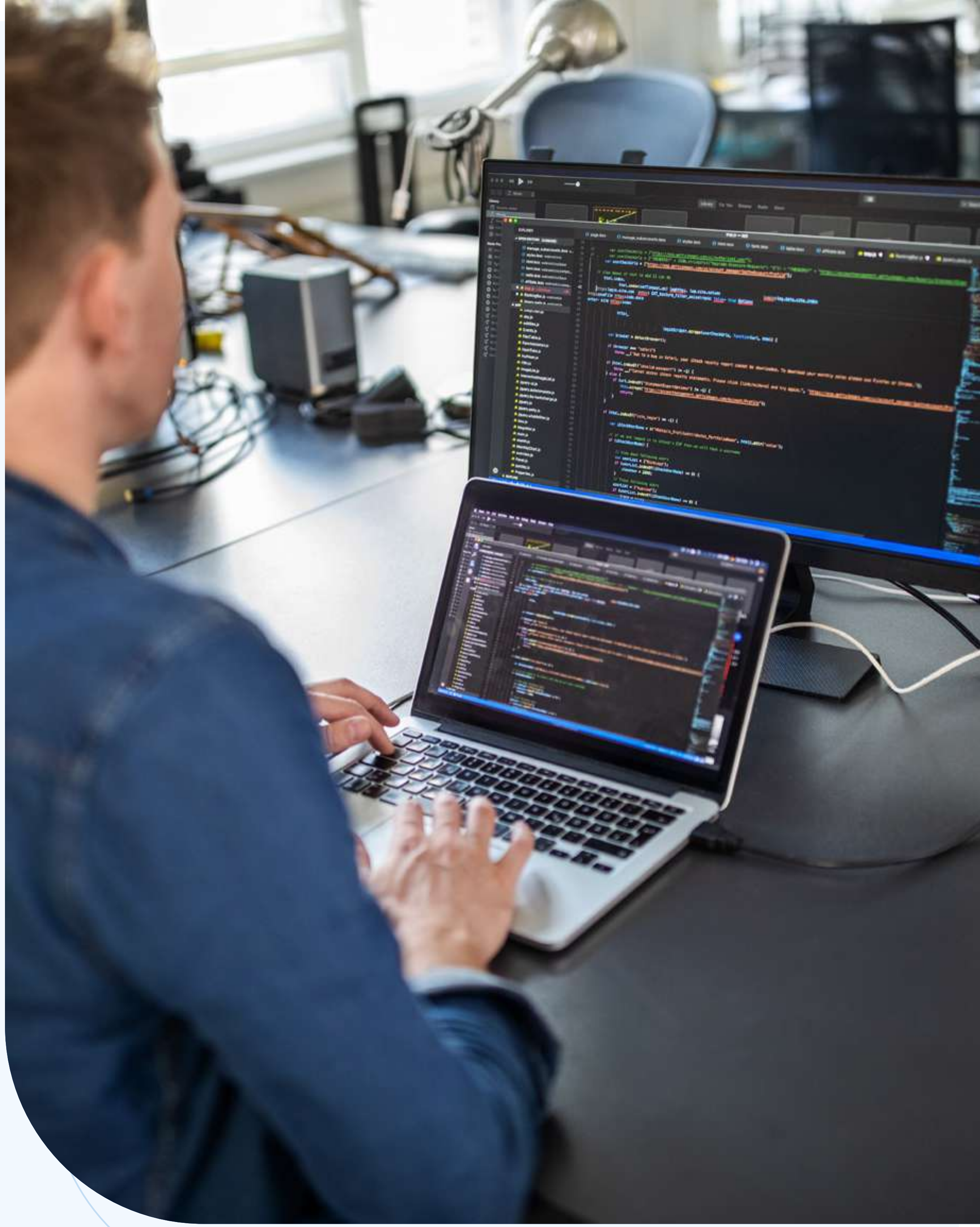
What it is: A device-agnostic mDL platform enables you to integrate your mDL into any app of your choosing, rather than binding you to the vendor's platform.

Why it's important: In a changing landscape, it's important to maintain flexibility. Some jurisidictions may choose to develop standalone mDL apps, while others prefer to package them together with other government features and functionalities. To protect your investment, you must build a solution that adapts easily to either scenario.

MINIMUM REQUIREMENTS

Vendor platforms should offer municipalities the ability to:

- **Integrate into any app** — Your mDL solution should be able to be integrated into a wide range of applications, including an existing state app or a native wallet.
- **Select a new app in the future** — Vendors should document how to adapt your mDL solution to a different application, should you later choose to.



Requirement #4
ISO Compliance

What it is: ISO18013-5 lays out standards that help issuing authorities develop a common, trusted approach to mDLs.

Why it's important: An mDL's utility is limited if it cannot be used in other jurisdictions and countries. Compliance with ISO18013-5 is the best way of ensuring interoperability.

MINIMUM REQUIREMENTS

Vendor offerings should ensure:

- **ISO compliance** — The vendor must provide a solution that fully complies with ISO18013-5's standards for interacting with and verifying the data from an mDL.
- **Flexibility** — The American Association of Motor Vehicle Administrators (AAMVA) and others have issued their own guidelines for the features that mDLs should support — including several items that go beyond ISO. To maximize flexibility, mDL solutions should not preclude or limit the deployment of these functionalities.

Requirement #5
Device Retrieval (Offline Mode)

What it is: Though mDLs and the readers that government officials use to authenticate them may not always be online, they must still be able to communicate. That's why ISO requests that mDL solutions rely on device data retrieval (a.k.a. offline).

Why it's important: In most cases, both mDL and reader will be online. However, because the two devices do not require an Internet connection to communicate, there is no need for mDL solutions to be capable of retrieving data from an online server. In fact, server retrieval would force issuing authorities to open their driver database to the Internet and exposed information about their drivers' whereabouts, greatly increasing the risk to both security and privacy.

MINIMUM REQUIREMENTS

Vendor offerings should include:

- **Device retrieval mode** — An mDL solution must comply with the mandatory device retrieval mode that's outlined in the ISO 18013-5 standard.
- **No additional options for server retrieval** — Because of the risks to privacy and security, vendors should not propose an optional server retrieval mode.

Requirement #6
A Demo and Proof-of-Concept

What it is: Demos provide a general overview of how an mDL solution works, while a more formal proof-of-concept in your environment helps you see how it might serve your state's specific needs.

Why it's important: Demos are the simplest way for jurisdictions to get a quick overview of a vendor's solution. An early-stage proof-of-concept, meanwhile, accelerates the development process by enabling you to see how the solution's capabilities align with your needs.

MINIMUM REQUIREMENTS

The vendor should be able to demonstrate:

- **How the provisioning platform operates** — You can evaluate the architecture of an mDL solution's provisioning platform and its verification mechanisms.
- **How basic features will work in your environment** — Request a proof-of-concept to test basic features and understand how well the solution will integrate with your systems.

Requirement #7
A Safe, Convenient Solution for Law Enforcement Stops

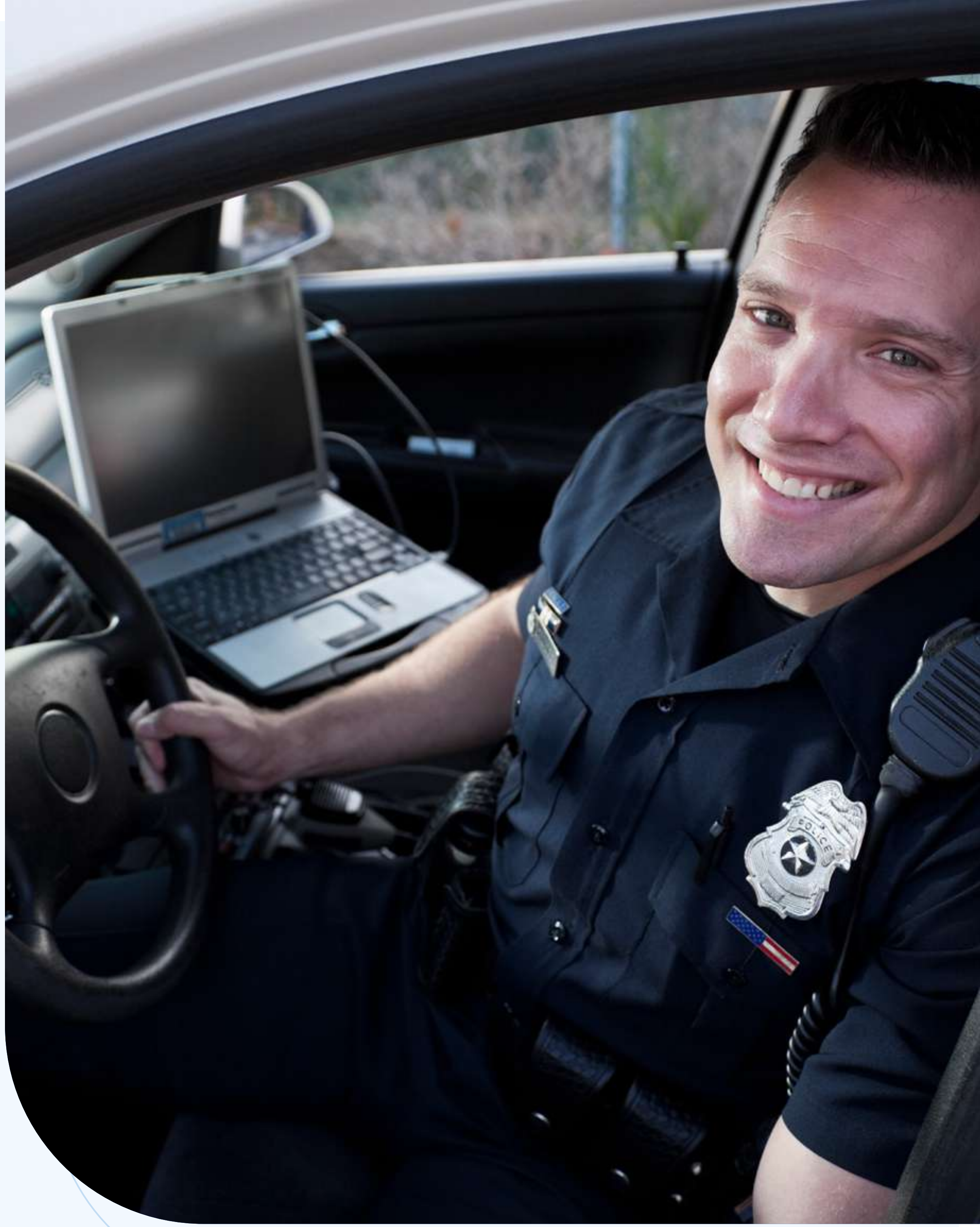
What it is: Law enforcement officials must be confident that your mDL will meet their needs — and maintain their security during roadside stops.

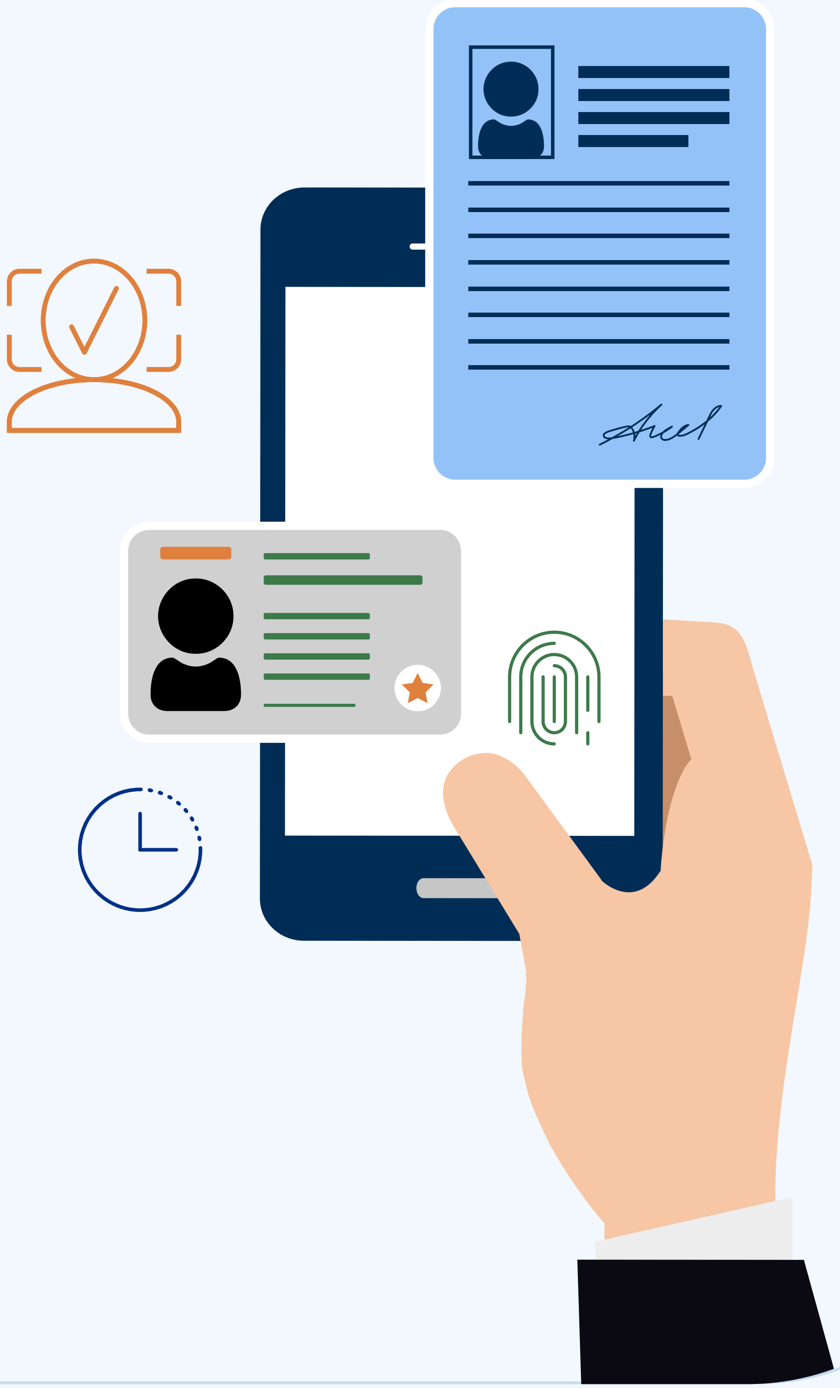
Why it's important: The support of your state's law enforcement community is critical to your mDL's success. The best way to accomplish this is by designing a solution that ensures a safe, efficient workflow in the line of duty.

MINIMUM REQUIREMENTS

Vendor offerings should include:

- **Hands-free verification** — Officers should be able to maintain their freedom of movement while authenticating an mDL.
- **Remote verification** — Officers should be able to authenticate mDLs without having to touch the driver's mobile device, using equipment that stays in the patrol car.





Requirement #8
A Flexible Development Platform

What it is: A flexible development platform enables issuing authorities to add and adapt mDL features as needs and requirements change.

Why it's important: The mDL market is dynamic and fast-moving. Today, you may be focused on digitizing your state's driver's license. In the future, you may want to store additional digital permits or even use your app to send emergency push notifications.

MINIMUM REQUIREMENTS

Vendor offerings should include:

- **Flexible document issuance** — The vendor's provisioning platform and data preparation module should enable drivers license bureaus to issue a broad range of documents and credentials, not just driver's licenses.
- **No additional restrictions on features or functionalities** — Your provisioning platform should not prohibit you from implementing beyond ISO functions within your mDL app.

Requirement #9
On-Device Security

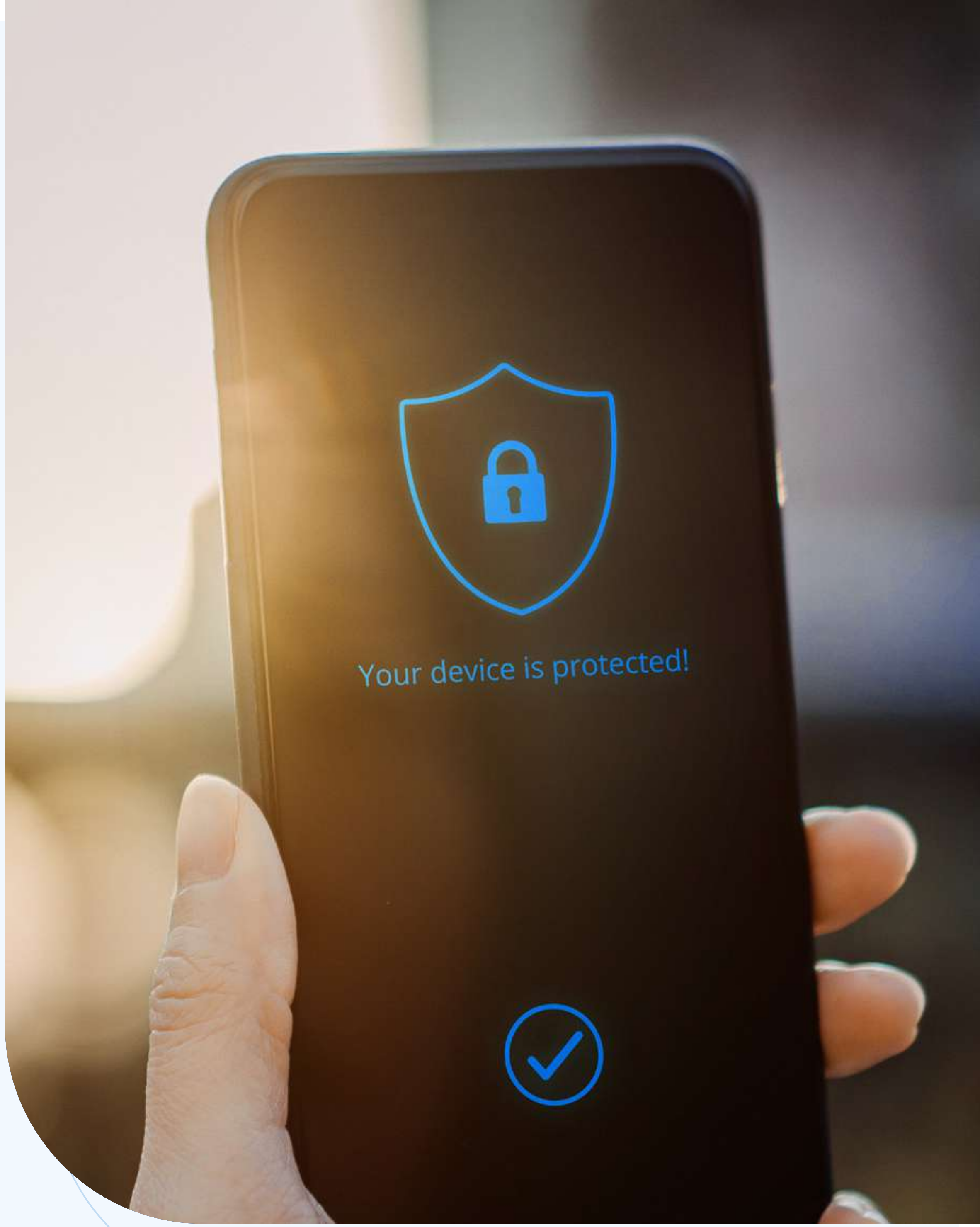
What it is: On-device security refers to a collection of tools and techniques that protect any sensitive information stored on a mobile device.

Why it's important: Jurisdictions will issue mDLs to millions of residents, each with a different device. Because security varies widely from device to device, it is imperative that your vendor follows best-in-class strategies for protecting mDL credentials regardless of where they are stored.

MINIMUM REQUIREMENTS

Vendor offerings should include:

- **Best-in-class security practices** — Your mDL solution should be protected by best-in-class practices like code obfuscation, tamper detection, reverse engineering protection and analysis protection. It must also offer a mechanism to protect against cloning.
- **OS updates** — Your vendor should provide as many updates as you need to keep up with different OS versions.



Requirement #10
End-to-End Encryption

What it is: End-to-end encryption will protect mDL data from being exposed to unauthorized entities.

Why it's important: Digital privacy advocates have already voiced concerns about mDLs, with apprehensions that range from police access to citizens' phones to the possibility that people will forced to download government apps. It's crucial that issuing authorities adhere to strict data privacy standards, which can only be ensured with an end-to-end encryption mechanism.

MINIMUM REQUIREMENTS

Vendor offerings should include:

- **End-to-end encryption** — There must be an end-to-end encryption mechanism between the mDL's on-premise platform and the mobile app on drivers' devices so that only encrypted data passes through the provisioning gateway that connects them. That way, even if the gateway is compromised, citizen data will be safe.
- **Encrypted provisioning and updates** — This end-to-end encryption mechanism should not interfere with the delivery of provisioned mobile identities and updates to drivers' devices.

Preparing for the Road Ahead

States across the country are looking forward to the innovation and convenience that mDLs will bring their citizens. As you prepare for this exciting future, it's important to make sure that the mDL vendors you work with design solutions that are customized, scalable and secure — so you can serve your citizens' needs no matter where the road takes you.

Learn more about the power of mDL:

- Visit our information hub about mDL
- Book time with one of our mDL specialists to discuss your business needs

hidglobal.com

North America: +1 512 776 9000
Toll Free: 1 800 237 7769
Europe, Middle East, Africa: +44 1440 714 850
Asia Pacific: +852 3160 9800
Latin America: +52 (55) 9171-1108

For more global phone numbers click here

2022-04-22-cid-mdl-guide-eb-en
PLT-06561

Part of ASSA ABLOY