



Reimagining the DMV Customer Experience: From Transactions to Digital Trust

SPONSORED BY



As identity verification becomes the key to accessing government and commercial services, departments of motor vehicles are taking on a broader role as providers of trusted digital identity.

Threats such as synthetic identities and AI-enabled document fraud have increased the need to strengthen identity assurance. As issuers of foundational credentials, DMVs are uniquely positioned to meet these challenges.

This moment represents a meaningful shift for DMVs: from completing paper-based, in-person transactions to enabling trusted, digital-first experiences that foster confidence in government. The federal REAL ID mandate reinforced this evolution, placing DMVs at the center of how residents establish and verify who they are. At the same time, some states have begun rolling out digital credentials: More than 5 million U.S. residents already have a digital driver's license,¹ a number projected to reach 143 million by 2030.²

"Some states are further along in their journey, while others are still finding their way," says Richard Grape, head of identity and transformational solutions at LexisNexis® Risk Solutions. "There is a tremendous opportunity to simplify the process of obtaining trusted credentials while improving convenience for residents and operational efficiency for agencies."

As DMVs modernize identity services, the challenge extends beyond adopting new technology — it requires delivering experiences that are both trusted and easier for residents to navigate.

Aligning Identity Tech with Resident Expectations

The implementation of REAL ID in 2025 increased documentation requirements for state-issued driver's licenses. In many cases, residents may have trouble finding or accessing these records, which include things like birth certificates or physical Social Security cards. That adds time and complexity for both customers and DMV staff.

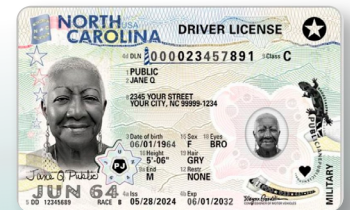
Meanwhile, resident expectations have evolved. People want government services to resemble the simple, secure digital experiences they receive from banks, retailers and technology providers. In fact, 65% of residents in Canada and the U.S. say they are interested in digital IDs.³

"Constituents expect convenient, trusted digital experiences," says Katie James, head of DMV solutions at LexisNexis® Risk Solutions. "Agencies are working to meet those expectations while balancing modernization priorities, security requirements and evolving service demands."

DMVs must also combat increasingly sophisticated fraud tactics. Identity theft reports now exceed 1.1 million annually,⁴ while synthetic identity fraud alone accounts for tens of billions in losses each year.⁵ Digital vital records provide a powerful foundation for addressing these threats.

Beyond operational improvements, trusted digital identity helps strengthen resident confidence that government services are secure, accessible and easy to use.

DMVs are uniquely positioned to strengthen identity assurance and push government services forward.



Elevating the DMV Experience

Recent audits and operational reviews across several states highlight the growing demand placed on DMVs and their systems. Increased transaction volumes, expanded identity requirements, older systems and resource constraints make it harder to deliver exceptional customer service.

Many of these challenges stem from the DMV's evolving mission. "DMVs weren't originally created to serve as the primary authority for identity verification," James says. "Their role has expanded significantly over time, particularly as digital services and identity assurance have become increasingly important."

Agencies that modernize service delivery are seeing measurable results. According to the Boston Consulting Group, one state reduced DMV wait times by up to 70%, while another can now process 10% more daily transactions after streamlining in-person interactions.⁶ In California, the time it takes to apply for a REAL ID has dropped from 35 minutes to 7 minutes thanks to digital workflows and automation.⁷

DMVs can improve customer experiences even more by creating a system that provides digital vital records to residents at DMV offices. This type of initiative streamlines identity verification and reduces operational burden.

Less frustrated residents

Few experiences create more frustration than showing up to complete an important DMV transaction only to learn that a required document is missing. Historically, resolving missing documentation could require multiple trips, mail requests or visits to another government office.

Digital vital records eliminate those steps by enabling residents to securely retrieve and present required documents during the transaction itself.

"Show up without a birth certificate? Now you can order that while you're in line at the DMV and have the digital credential sent directly to your phone," James says. "They can accept it, and you can continue your transaction."



How One State Leveled-Up Its DMV

A recent state pilot demonstrates how digital credentials can simplify identity verification while improving experiences for both residents and agencies.

A state DMV sought to enable residents to access trusted digital credentials through their mobile devices. To support that vision, the agency partnered with LexisNexis® Risk Solutions to implement identity assurance, digital credential issuance and secure delivery capabilities powered by VitalChek®, the nation's largest vital records ordering network.

The result was a streamlined process that enabled residents to obtain, verify and present trusted digital credentials

while helping the agency strengthen identity assurance and improve operational efficiency.

"On the back end, it's organized to provide a single, integrated experience," James says. "It takes you from that initial ordering and identity verification, all the way to the credential that lives on your device and is accepted by the agency."

In addition to deploying the solution, LexisNexis® Risk Solutions worked with the DMV to ensure effective service implementation. That meant training workers on the new systems and troubleshooting any problems.

"We met with them on several different occasions. When they had learning days, when they had team meetings, we would provide that training," James says, adding that there wasn't a major learning curve for staff. "It's just a couple of clicks. The process is intuitive and easy for staff to adopt."

The pilot project started with birth credentials for adults. The DMV plans to expand this initiative soon to enable credentials for minors. The solution will eventually incorporate marriage certificates for name changes. "That is a big use case for DMVs," Grape says.



The experience is designed to be simple and accessible, even for residents with limited technical proficiency. “This isn’t designed just for younger users and tech adopters,” Grape says. “I watched one 95-year-old grandmother go through the digital credential process who hadn’t seen her physical birth certificate in 40 years.”

Reduced staff burden

When residents arrive without the required documentation, it also impacts DMV employees. Staff must explain the issue, restart the process and manage longer queues — all while trying to maintain a positive customer experience.

Digital vital records offer a better alternative by giving staff a faster, more reliable way to help customers retrieve and present the documents they need. That means fewer repeat visits, fewer manual document checks and less time spent resolving paperwork problems.

It also gives staff greater confidence in the authenticity of the records they receive, allowing them to move transactions forward instead of trying to determine whether a paper document is valid, complete or current. In advanced environments, with fewer routine problems consuming their time, DMV staff can focus more attention on customers who need additional support.

Strengthening Trust and Identity Assurance

For DMVs, the challenge extends beyond obtaining a document. Agencies must be confident that the document is authentic, untampered with and being presented by the individual entitled to use it.

Digital vital records strengthen confidence by creating a secure, verifiable chain of trust from issuance through presentation. Unlike paper documents, which can be lost, altered or difficult to validate, digital credentials are issued directly from trusted sources and verified using modern identity assurance processes. This approach helps agencies strengthen security while creating a more convenient experience for residents.

This interaction happens with a strong sense of assurance for the DMV. Identities are validated according to National Institute of Standards and Technology (NIST) standards, and residents authenticate requests on their own devices. Credentials are stored in secure mobile wallets and bound to the individual through identity verification and biometric protection.

“You have confidence it’s the right person, and that everything has been facilitated accurately,” Grape says. “This helps reduce both immediate and long-term fraud risk.”

That combination of verified identity, trusted issuance and secure presentation significantly reduces opportunities for fraud while simplifying the customer experience.

“Digitization increases the accessibility, usability and portability of that key foundational document,” Grape says. “It increases its relevance in the modern era, allowing all parties to have greater trust that it is coming from a legitimate, authorized source, and is being presented by a party that is entitled to have it.”

To maximize the security of digital birth certificates, DMVs should leverage ISO mDocs (Mobile Documents), the global standard for digital identity credentials.

“ISO mDocs has identity-binding components that keep identity attached to the entity that was entitled to receive it,” Grape says. “ISO mDocs leverage the industry-leading, best-of-breed identity assurance journeys that come from NIST.”



Modernizing identity services does not require agencies to transform everything at once. The following practices can help organizations prioritize investments while building a trusted digital identity foundation for the future.

A Roadmap for Trusted Digital Identity

1. Prioritize High-Impact Service Experiences

Not every DMV transaction needs to be transformed at the same time. Focus first on the interactions that create the most friction for residents and staff, such as REAL ID applications, first-time licenses, name changes and credential renewals that require multiple identity documents.

These use cases often generate repeat visits, long wait times and manual document reviews, making them ideal candidates for digital records.

✓ **What to do now:** Review transaction data and identify the three most common reasons residents are turned away or asked to return with additional documentation. Those pain points should become your initial priorities.

2. Create a Shared Vision for Digital Identity

Digital vital records sit at the intersection of multiple organizations, including the DMV, the state vital records office, public health agencies and technology partners. The most successful efforts begin with agreement on a common vision for identity verification and data sharing.

Rather than viewing digital records as a DMV project, treat them as a statewide digital identity initiative.

✓ **What to do now:** Convene a working group with representatives from the DMV, vital records office and other relevant agencies to map the current identity verification process and identify opportunities to eliminate paper-based handoffs.

3. Build Trust Through Secure, Resident-Centric Experiences

Convenience is often the most visible benefit of digital records, but trust is what drives adoption. Staff, agency leaders and residents need confidence that digital credentials are secure, authentic and resistant to fraud.

A strong emphasis on identity assurance, privacy protections and standards-based verification will help overcome skepticism and accelerate buy-in.

Digital vital records sit at the intersection of multiple organizations, including the DMV, the state vital records office, public health agencies and technology partners.

☑ **What to do now:** *Develop clear messaging around how digital credentials are issued, verified and protected. Equip frontline staff with simple explanations they can use when residents have questions about security or privacy.*

4. Empower the Frontline Workforce

Many efforts focus exclusively on residents. But DMV staff ultimately determine whether a new process succeeds. The solution should reduce workload, simplify workflows and make it easier for staff to serve customers.

If staff view this technology as another layer of complexity, adoption will suffer.

☑ **What to do now:** *Identify a small group of frontline staff to participate in pilot testing and process design. Their feedback can help uncover workflow issues before statewide deployment.*

5. Measure Outcomes That Matter

The value of digital vital records extends far beyond technology modernization. Agencies should track outcomes that demonstrate improvements in service delivery, operational efficiency and fraud prevention.

Metrics such as repeat visits, transaction completion rates, average processing times and customer satisfaction scores can help leaders quantify impact and justify future investment.

☑ **What to do now:** *Establish baseline metrics before implementation begins. Measuring conditions before and after deployment will make it easier to demonstrate success and secure support for expansion.*

6. Plan for a Broader Digital Identity Ecosystem

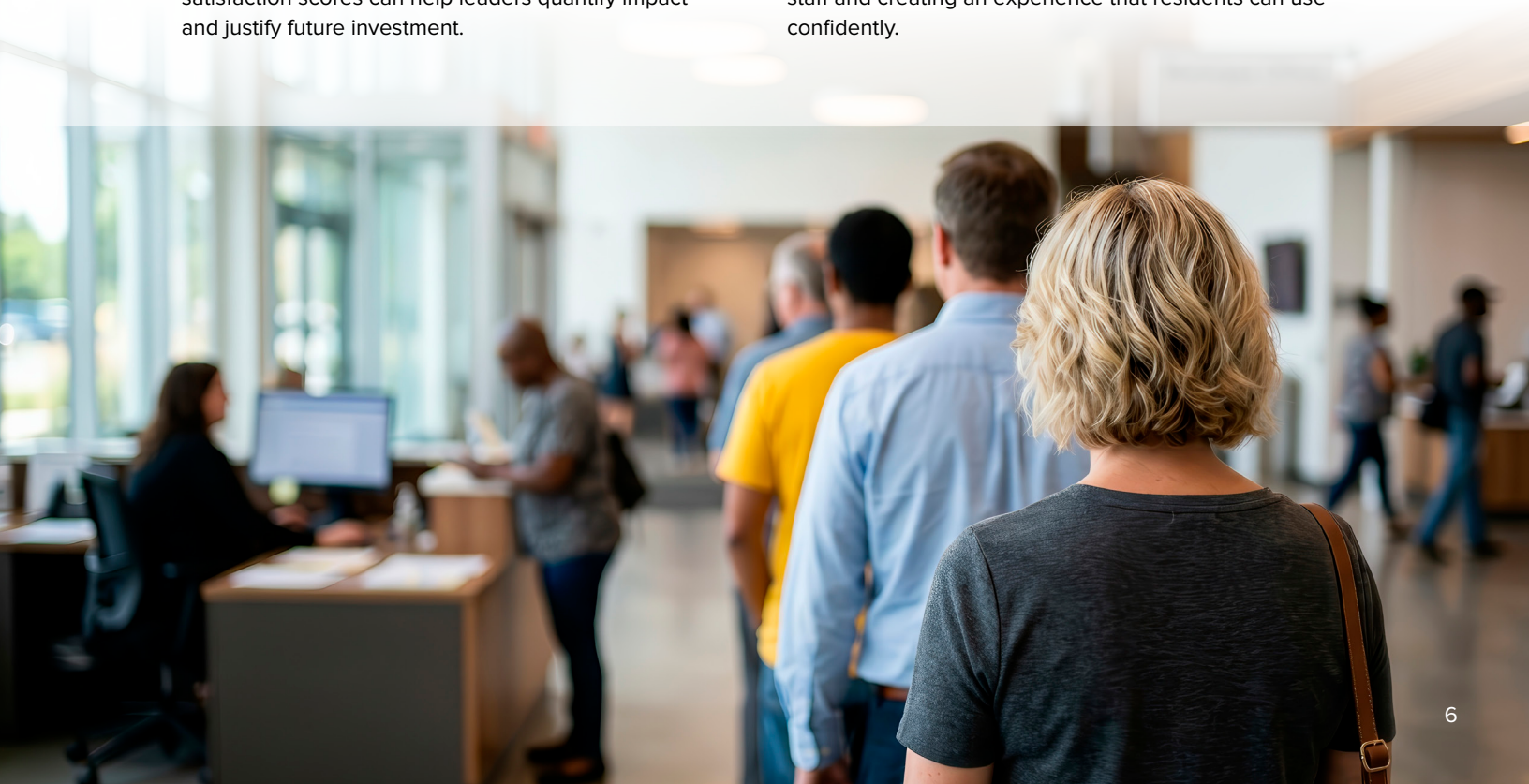
The DMV is often the logical starting point because of its central role in identity verification. But digital vital records create opportunities across government, from benefits administration and professional licensing to public health and social services.

The long-term value comes from building a trusted digital identity ecosystem that residents can use across agencies and life events.

☑ **What to do now:** *Identify one or two additional government services that could benefit from trusted digital credentials and begin conversations about future expansion. Early planning can help ensure today's investments support tomorrow's use cases.*

7. Select a Partner with Government Identity Expertise

Digital vital records initiatives require much more than software implementation. Success depends on integrating systems across agencies, navigating regulatory requirements, establishing trust frameworks, training staff and creating an experience that residents can use confidently.





The most effective partners bring deep expertise from both the public and private sectors. They understand the unique operational, legal and policy requirements of government agencies, while also drawing on lessons learned from industries such as financial services, health care and e-commerce, where secure digital identity and customer experience have been evolving for years.

Equally important, a trusted partner should support the entire transformation journey — from planning and implementation to staff training, change management and ongoing optimization. Technology adoption accelerates when frontline staff understand how the new process works, why it matters, and how it benefits both staff and residents.

☑ **What to do now:** *Evaluate potential partners based on both their technology capabilities and their experience supporting large-scale identity initiatives, integrating with government systems and training staff. Ask for examples of successful deployments and evidence that they can help agencies manage organizational changes, not just install software.*

Technology adoption accelerates when frontline staff understand how the new process works, why it matters and how it benefits both employees and residents.

From Modernization to a Trusted Digital Identity Ecosystem

For decades, DMVs have served as trusted stewards of mobility and public safety. Today, they are also becoming a cornerstone of trusted digital identity — helping residents securely access services in an increasingly digital world.

Digital vital records represent more than a technology modernization initiative. They provide a critical building block for trusted digital interactions that improve identity verification while enhancing security, efficiency and resident experience. The goal is not simply to digitize a document. It is to make government services easier to access, easier to trust and easier to navigate.

The implications extend far beyond the DMV. Trusted digital credentials can support a wide range of government services, from professional licensing and benefits administration to public health and workforce programs. Digital vital records may begin as a solution for REAL ID and identity verification, but their long-term value extends much further. They create the foundation for a trusted digital identity ecosystem that can support services across government throughout a resident's lifetime.

“Every successful implementation brings agencies one step closer to delivering trusted, secure and seamless identity experiences across government,” James says

The agencies that move first have an opportunity to do more than modernize a process. They can help shape a future where trusted digital identity makes government services easier to access, easier to trust and easier to navigate.

1. <https://mobileidworld.com/18-us-states-to-adopt-digital-drivers-licenses-by-2025-as-mobile-id-adoption-grows/>
2. <https://www.abiresearch.com/press/domestic-air-travel-and-digital-wallet-trends-drive-u.s.-mobile-drivers-license-install-base-to-143-million-by-2030>
3. <https://www.businesswire.com/news/home/20250910318632/en/Thales-Survey-Reveals-Growing-Interest-in-Mobile-IDs-Digital-Driver-Services-Across-US-Canada>
4. <https://app.stationx.net/articles/identity-theft-statistics>
5. <https://chargebacks911.com/ecommerce-fraud/synthetic-identity-theft/synthetic-identity-theft-statistics/>
6. <https://www.bcg.com/publications/2025/less-line-more-online-reimagining-dmv-experience>
7. <https://www.pedalmobility.com/en/insights/blogs/revolutionizing-dmv-services>

This piece was written and produced by the Government Technology Content Studio, with information and input from LexisNexis® Risk Solutions.



Produced by Government Technology

Government Technology is about solving problems in state and local government through the smart use of technology. Government Technology is a division of e.Republic, the nation's only media and research company focused exclusively on state and local government and education.

www.govtech.com



Sponsored by LexisNexis® Risk Solutions

LexisNexis® Risk Solutions helps DMVs modernize with confidence by enabling secure, seamless, constituent-first experiences across every service interaction. Through advanced data, analytics, and identity intelligence, we help agencies make trusted decisions, reduce friction, and strengthen identity assurance across digital and in-person channels.

Our solutions support the full DMV service journey — from identity verification and fraud prevention to digital credentials, payments, and vital records modernization. By helping agencies detect evolving threats, improve operational efficiency, and deliver faster, more trusted services, LexisNexis Risk Solutions empowers DMVs to transform the way constituents access essential services while protecting the integrity of every transaction.

Learn more at <https://risk.lexisnexis.com/government/departments-of-motor-vehicles-dmvs>.