



Reimagining the DMV Customer Experience: From Inconvenience to Digital Trust

SPONSORED BY



Since their inception, state DMVs have primarily been responsible for facilitating safe motor vehicle use.

That time is over. Now that U.S. residents need a Real ID for boarding domestic commercial flights, DMVs have become the front door for verifying identity.

This profound change introduces significant new complexities. “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 lot of pressure on them to facilitate the additional information needed to obtain Real IDs.”

Residents may struggle to provide proof of age, identity and residency — all requirements for Real ID. Someone’s birth certificate and other core documents might be locked away in a forgotten cabinet. Or maybe in a box in their parents’ attic. Some people may not have a copy of anything.

At the same time, constituents today want a better customer service experience at the DMV.

“Constituents expect to see the same seamless services as with any big retailer that deals with secure identities,” says Katie James, LexisNexis Risk Solutions’ head of DMV solutions. “But some states are still on COBOL mainframes and other outdated systems that don’t allow for that.”

DMVs must also account for a growing number of document forgeries, AI deepfakes and other fraud tactics.

The solution to all these challenges is digital vital records, which empower DMVs to lead the future of constituent services. “People don’t have to stand in a line that wraps around the building,” Grape says. “With the right combination of digital tools, it’s possible for residents to finish everything in a single smooth interaction.”

Why Residents Hate the DMV

The DMV has long been one of the most maligned aspects of state government.

In a [recent Reddit thread](#),¹ one user said the DMV experience “made me question my entire existence,” while another advised to “just bring your sleeping bag.” In a March [Washington Post op-ed](#),² former Indiana Gov. Mitch Daniels called state DMVs a “laughingstock” that’s “often atrocious.” As Daniels argued, poor DMV experiences directly affect public trust in government competence.

A 2025 state [audit in North Carolina](#)³ illustrates just how bad the problem can be. The audit revealed average DMV wait times of an hour and 15 minutes, an *increase* of 15.5% since 2019. Nearly 14% of visits exceeded two hours and 30 minutes, a whopping 79% increase since 2019. That takes a toll on employees as well: In the same audit, 43% of DMV workers expressed negative views of leadership.

Many of these issues can be traced to the DMV’s evolving role in recent years. “DMVs weren’t created to verify your identity,” James says. “They were created to verify that you can drive a vehicle safely, that you can be on the road and follow all the rules. Pictures on a credential didn’t come about until the 1960s.”

Many of residents’ issues with the DMV can be traced to the department’s evolution toward identity verification.



The introduction of REAL ID, which took effect in May 2025, brought the underlying problems with DMV customer service into stark relief. “The front door is where those operational problems occur,” James says. “And when the Real ID Act happened, all of those things — fraud, bottlenecks and resident frustration — spiked.”

A Real ID requires more substantiating documents, usually in the form of paper records, which already come with risks and costs. Paper documents are easy to lose or misplace, and paper-based workflows mean headaches for DMV employees.

Digital vital records offer a smoother alternative. These are secure, verifiable and digitized electronic versions of offline certificates, including birth, death, marriage and divorce records.

For DMVs looking to elevate user experience and take pressure off their staff, digital records can form the foundation for trusted identity.

Benefits on Both Sides of the Counter

A seamless consumer experience. Imagine a resident who has already taken time off work to come to a DMV office to obtain or renew his license. Now imagine he failed to bring all the necessary documents to verify his identity.

In the past, he would have been sent home and forced to come back another time. But with digital vital records, he can retrieve the missing document almost instantly.

“Show up without a birth certificate? Now you can order that while you’re in the DMV, and get that digital credential on your phone,” James says. “They can accept it, and you can continue your transaction.”

Paper-based workflows mean headaches for DMV employees.



How One State Leveled-Up Its DMV

A recent state pilot demonstrates the art of the possible.

A state DMV was looking to create digital credentials that residents could keep on their phones or other handheld devices. To accomplish this, the department partnered with LexisNexis, implemented new tools and applications, and relied on VitalChek, the nation’s largest vital records ordering system. With that three-pronged approach, the DMV office created a verifiable credential that the consumer can present as digital proof of identity.

“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 also worked with the DMV to ensure effective 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. It’s super easy for them.”

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. “When someone gets married or divorced and they’re changing their name, they have to authenticate that. And their birth certificate doesn’t have that information. That use case will further improve the experience and reduce in-office time.”



“They don’t have to go home to find it in a filing cabinet, or trek to the nearest vital record office to order it, or request it by mail,” Grape says. “They can get it in minutes.”

The solution is simple even for those with little or no technical proficiency. “This isn’t designed just for younger users and tech adopters, Grape says. “I had one 95-year-old grandmother going through the process who hadn’t seen her birth certificate in 40 years.”

A better employee experience. When residents arrive without the right documents, DMV staff are often left to explain the problem, turn people away and help them restart a process that may already have required time off work, travel and long waits.

Digital vital records reduce those frustrating interactions by giving employees 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.

With a lower number of routine problems consuming their time, DMV employees can focus more attention on customers who need additional support. The result is a smoother workflow, less friction at the counter and a better experience for both residents and staff.

Combating Fraud

For DMVs, the challenge isn’t simply obtaining a document — it’s knowing that the document is authentic and that it is being presented by the person who is legally entitled to use it.

Digital vital records provide a higher level of assurance than traditional paper documents. A paper birth certificate can be lost, damaged, altered or forged, and DMV employees often have limited ways to verify its authenticity.

Digital credentials, by contrast, are issued directly from trusted sources and validated against rigorous identity standards, creating a secure chain of trust from issuance through presentation.

This interaction happens with a strong sense of assurance for the DMV. Identities are validated according to 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 protections.

“You have confidence it’s the right person, and that everything has been facilitated accurately,” Grape says. “It’s the right party that’s asking to obtain the information.”

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.”



Best Practices for Digital Vital Records Adoption

1. Start with the highest-friction customer journeys.

Not every DMV transaction needs to be transformed at once. Focus first on the interactions that create the most frustration for residents and employees, 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 modernization priorities.

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

2. Build a shared identity strategy across agencies.

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. Focus on trust before convenience.

Convenience is often the most visible benefit of digital records, but trust is what drives adoption. Employees, 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.

✓ **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. Design for the employee experience.

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

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

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

5. Measure what matters.

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. Think beyond the DMV.

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.

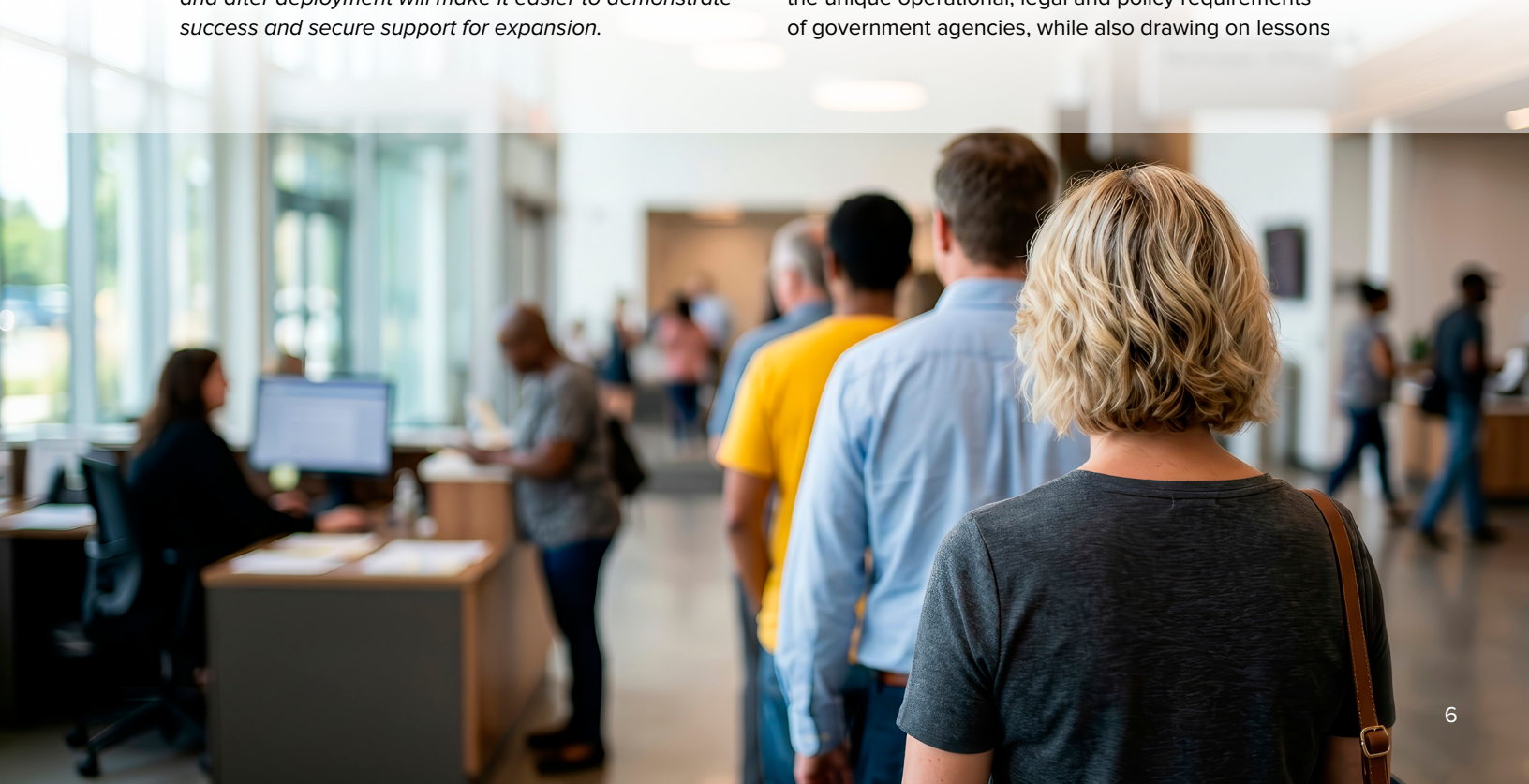
The long-term value comes from building a trusted digital identity ecosystem that residents can use across agencies and life events.

☑ **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. Choose a partner with experience in both government and consumer identity.

Digital vital records initiatives require much more than software implementation. Success depends on integrating systems across agencies, navigating regulatory requirements, establishing trust frameworks, training employees 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 employee 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 employees and residents.

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

Conclusion

For decades, DMVs have been defined by transactions: issuing licenses, renewing registrations and helping residents comply with the rules of the road. Today, their role is much larger. As the primary authority for identity verification in most states, DMVs are becoming a critical foundation for digital trust across government.

That responsibility arrives at a pivotal moment. Residents expect government services to be as seamless, secure and intuitive as the experiences

they receive from banks, retailers and technology companies. At the same time, agencies face mounting pressure to combat fraud, strengthen security and do more with limited resources.

Digital vital records help address all of these challenges at once. They reduce friction for residents, improve efficiency for DMV employees and provide a more secure, trustworthy alternative to paper-based identity verification. Most importantly, they create a stronger foundation for proving identity in an increasingly digital world.

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. Every successful implementation brings states one step closer to a future where residents can securely prove who they are without navigating a maze of paperwork, repeat visits and manual verification processes.

The agencies that move first have an opportunity to do more than modernize a process. They can help define the future of digital identity in government — creating a model that is more secure, more efficient and more responsive to the people it serves.

“You know that it’s the right party, that it’s accurate and that it comes from a trusted source,” Grape says. “That’s a big win for agencies, especially agencies that struggle to have line of sight into the party that might be presenting the documentation. Ultimately that’s what this is all about.”

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



1. https://www.reddit.com/r/AskReddit/comments/1s4qf1g/for_those_who've_lived_in_multiple_states_how
2. <https://www.washingtonpost.com/opinions/2026/03/31/dmv-department-motor-vehicles-government-efficiency/>
3. <https://www.auditor.nc.gov/news/press-releases/2025/08/04/dmv-audit-recommends-exploring-separation-dmv-and-dot-customer-experience-worsens>

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



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 Lexis Nexis

CTA to come

website.com