NIST SP 1800-42 explained: using mobile driver's licenses for secure online identity

23 November 2026 · 6 min read · blogs.iictp.org/nist-sp-1800-42-mobile-drivers-license-online-explained

Short answer: NIST SP 1800-42 is a draft report from NIST's National Cybersecurity Center of Excellence, announced on 19 November 2026, that shows how organisations can accept mobile driver's licenses (mDLs) online. It documents a reference architecture built from commercial off-the-shelf parts and is open for public comment until 20 December 2026. It matters because very few online services accept mDLs today, even though the credential is cryptographically protected.

TL;DR The short version

- NIST SP 1800-42 is a draft that shows how organisations can accept mobile driver's licences online, open for comment until 20 December 2026.
- It documents a reference architecture from commercial parts, built with technology firms, agencies and five of the ten largest US banks.
- The pattern to note is using the strong credential once to bind identity, then relying on phishing-resistant passkeys day to day.

Read online, listen to it, or change the text size: https://blogs.iictp.org/nist-sp-1800-42-mobile-drivers-license-online-explained

What is an mDL?

A mobile driver's license is a digital form of a driver's licence held on a phone. NIST says its information is cryptographically protected, which makes it hard to steal or fake, and that it can be used in person or online. It can replace uploading photos of a physical ID card.

The adoption problem

NIST engineer Bill Fisher calls it a chicken-and-egg problem: consumers will not adopt mDLs unless they work in everyday, high-value cases, and companies hesitate to integrate without demand. NIST says 22 US states and territories have active programmes, with at least 5 million mDLs in use and about 47% of the population having access.

How the reference architecture works

- The project involved technology companies, government agencies and five of the ten largest US banks.
- It demonstrates three capabilities: presenting an mDL to verify identity in an online transaction; requesting one in higher-risk moments, such as high-value transactions or account recovery, to re-establish trust; and issuing a

phishing-resistant authenticator, that is, a passkey, to the user.
- It was built with commercially available technology and standards, and the report lists threats to an mDL ecosystem with mitigations, pointing to the NIST Privacy Framework and SP 800-53 Rev. 5.

What NIST says it found

The draft includes seven usability best practices from testing with volunteers. Fisher says the limit on adoption is not the technology but the maturity of the surrounding ecosystem: issuers, technology providers and relying organisations must coordinate.

Limitations and open questions

- It is a draft. Content may change after the comment period.
- We read NIST's news release, not the 1800-42 report itself, so technical details such as the exact protocols used are not covered here.
- Coverage is US-specific; other jurisdictions run different wallets and trust frameworks.

How to evaluate it for your service

1. List where you now accept a physical ID, such as account opening or recovery.
2. Decide which steps need identity proofing and which only need a passkey.
3. Read the draft and send comments before 20 December 2026.
4. Pilot with a low-risk journey and measure completion and fraud outcomes.

What it means for security and identity engineers

The pairing of a verified credential with a passkey is the pattern to note: use the strong credential once to bind identity, then rely on phishing-resistant authentication day to day. See what is OAuth and OpenID Connect and digital badges and verifiable credentials explained.

Frequently asked questions

- **Is SP 1800-42 final?** No. NIST describes it as a draft for public comment.
- **Who can comment?** Anyone; comments go by email or through the project resource hub until 20 December 2026.
- **Does it need special hardware?** NIST says the demonstration uses commercially available technology and standards.
- **Does it replace passkeys?** No. The architecture includes issuing a passkey after an mDL is presented.

Related reading

- What is OAuth and OpenID Connect?
- Digital badges and verifiable credentials explained
- What is zero trust?

- Certified Technical Practitioner

Sources and currency

Sources were read on 23 November 2026. Products, rules and standards change, so check the linked originals before you rely on any detail.

> Related credential: Certified Technical Practitioner. Explore the exam facts and syllabus.

Sources and further reading

1. NIST. NIST Project Aims to Accelerate Mobile Driver's License Adoption. 19 November 2026. nist.gov/news-events/news/2026/11/nist-project-aims-accelerate-mobile-drivers-license-adoption.

Published by IICTP, an independent technical credential body, on 23 November 2026. The current version of this post is at https://blogs.iictp.org/nist-sp-1800-42-mobile-drivers-license-online-explained. More guides: blogs.iictp.org.