Peculiar Ventures

mDL Meets the WebPKI Ecosystem

What Ballot SMC015v2 means for
Certificate Authorities.

CA/Browser Forum Face-to-Face — SSL.com, Houston
March 2026
Ryan Hurst, CEO

What Just Happened

Ballot SMC015v2 passed. Mobile Driver's Licenses are now valid proof of identity for publicly-trusted S/MIME certificates.

17

Certificate Issuers
voted YES

3

Major Consumers
Apple, Microsoft, Mozilla

0

Votes against
the ballot

> Proposed by Stephen Davidson (DigiCert), endorsed by Ben Wilson (Mozilla) and Scott Rea (eMudhra). Immediate context is S/MIME, but the credential recognition extends to client auth, mTLS, and document signing.

How We Got Here

2021	2022	2023	Nov '24	Sep '25	Jan '26
ISO 18013-5 published	TSA begins accepting mDLs	ISO 18013-7 published	TSA final rule REAL ID waiver	Apple and Android ship 18013-7 support	SMC015v2 passes

What's next

2026-2028 More states start to shift to wallets with 18013-7 support

Dec 2026 EU EUDI Wallet deadline — 27 member states

2026-2027 CAs start to add support for MDL based issuance.

> Five years from standard to CA ballot. The next 12-24 months are when CAs build the verification infrastructure.

01

The Problem

Why This Matters Now

The Threat

- Deepfake fraud up 2,137% in three years[1]
- 42.5% of financial fraud now AI-driven[1]
- Gen AI produces convincing fake IDs at scale
- Liveness detection defeated by real-time video manipulation
- Gen AI fraud losses projected $40B by 2027[2]

The mDL Answer

- Government-issued, cryptographically signed
- Bound to device you physically hold
- ISO 18013-5 defines the credential structure
- ISO 18013-7 enables online presentment with challenge-response
- Resistant to replay, deepfakes, and document forgery

[1] Signicat/Consult Hyperion, "The Battle Against AI-Driven Identity Fraud" (Feb 2025), 1,200 respondents across 7 EU countries
[2] Deloitte Center for Financial Services, gen AI fraud loss projections (2024)

mDL State of the Nation

24	**250+**	**45%**	**33%**
TSA Recognized authorities	TSA Checkpoints accepting mDL	US Population eligible	Online Presentment coverage

- TSA final rule (Nov 2024) established REAL ID waiver framework — goal is all airports nationwide.
- NIST NCCoE building reference implementation (SP 1800-42) for mDL in financial KYC with 800-63-4 assurance mapping.
- Part 5 (in-person) is mature. Part 7 (online presentment) adoption still limited — the gap CAs need to close.
- 54% of mDL programs have a discoverable root CA — the rest need work before CAs can verify them.
- States must report mDL cybersecurity incidents to TSA within 72 hours.

What SMC015v2 Changes

Before

S/MIME individual identity validation relied on physical document inspection or video-based methods.

After

CAs can now accept mDL presented via ISO 18013-7 online presentment from a legally authorized issuer.

Requirements

CA/RA must verify issuing authority is legally authorized. mDL must be presented via cryptographic protocol.

Immediate context is S/MIME, but these are user identity certificates. **The credential recognition extends to client auth, mTLS, and document signing.**

02

The Standards

The Standards Stack

ISO/IEC 18013-5

In-person presentation. Defines credential structure, data model, proximity protocols (NFC/BLE). Powers TSA checkpoints at 250+ airports. Nearly all wallets support Part 5.

ISO/IEC TS 18013-7

Online presentment. The piece CAs need. Enables remote cryptographic verification with challenge-response resistant to replay and deepfakes. Adoption still limited — this is the frontier.

S/MIME BRs v1.0.13

Permits mDL as valid identity evidence under Section 3.2.4.2

AAMVA VICAL

Signed trust anchor for mDL issuer root certificates, ECDSA verified

NIST NCCoE SP 1800-42

Reference implementation for mDL in financial KYC/CIP

TSA Final Rule (Nov 2024)

REAL ID waiver framework. 72-hour incident reporting. Goal: all airports.

How Online Presentment Works

ISO 18013-7 defines two models for remote mDL verification. Both produce the same cryptographic proof.

Cross-Device (QR Code)

1. Verifier displays QR code on website
2. User scans with wallet app on phone
3. Wallet prompts for consent + biometric
4. Wallet sends signed response over HTTPS
5. Verifier validates against issuer root

Same-Device (App / Browser)

1. Website invokes wallet via browser API
2. OS switches to wallet app on same device
3. Wallet prompts for consent + biometric
4. Wallet returns signed response to browser
5. Verifier validates against issuer root

The exchange: Verifier sends nonce + requested attributes → Wallet signs response with device key → Response includes issuer signature chain back to root. **No document images. No liveness video. Cryptographic proof.**

Mandate vs. Utility

More credentials in hands without a mandate than with one.

United States — No Mandate

5M+

mDLs issued and in people's hands

- California: 2.65M issued (Aug 2025)
- Arizona: 1.1M enrolled (23% of drivers)
- New York: 246K in first year
- TSA anchor tenant drove adoption
- Utility first, mandate never

European Union — Mandated

0

production EUDI Wallets live*

- 27 states must offer wallet by Dec 2026
- Netherlands, Bulgaria already behind
- 550 orgs in pilots — pilots ≠ issuance
- Cross-border interop just proven Dec 2025
- Mandate first, utility TBD

> Utility drives adoption, mandates don't. Both build on ISO 18013-5/7. CAs building verification now are positioned for both.
>
> * Several EU countries have successful national digital ID (Sweden BankID ~95%, Estonia eID, Denmark 2.1M digital DLs) — but non-interoperable national schemes, not eIDAS 2.0 EUDI Wallets.

03

Building It

What CAs Need To Build

1 mDL Verification Pipeline

Integrate ISO 18013-7 online presentment into your identity vetting workflow. Replaces or supplements document upload + liveness check.

2 Issuer Trust Store

Consume AAMVA VICAL and web-discovered roots. Validate issuer is legally authorized. Build for 50-state coverage plus territories.

3 Derived Credential Issuance

Convert verified mDL attributes into X.509 certificate subject fields. Bind legal identity to signing key with cryptographic audit trail.

4 Ongoing Governance

Root certificates rotate. States add programs. Trust lists update. Budget for continuous monitoring — not a one-time integration.

Hancock: mDL to X.509

1 Sender requires mDL verification → **2** Recipient presents mDL via 18013-7 → **3** mDL authenticated against issuer root → **4** Derived X.509 certificate issued → **5** Document signed + timestamped

- Standards-based: output is a standard X.509 certificate verifiable in Adobe, Office, any PDF reader.
- Cryptographically verifiable audit trail links signer's government-verified identity to the document.
- Eliminates in-person notarization for high-stakes contracts, KYC/AML, benefit distributions.
- Peculiar Ventures' Hancock mDL-based remote vetting ships H1 2026.
- Over 3-5 billion electronic signatures annually — massive addressable market.

Live Demo: Hancock mDL Verification

mDL presentment → identity verification → derived X.509 → document signature

04

Why It Matters

What These Certs Actually Do

mDL-verified X.509 certificates solve specific, expensive problems.

Stop Benefit Fraud at Scale

30M unemployment claims hit at once in 2020. A cryptographic identity check — not a web form — would have caught the prison WiFi rings.

KYC Without Scanned Documents

Banks accept photos of IDs that Gen AI forges in seconds. An mDL-derived cert gives them cryptographic proof from the issuing state.

Stop Email and Wire Fraud

CEO impersonation, mortgage wire fraud, vendor invoice scams. S/MIME with mDL-verified identity means the sender is provably who they claim to be. Not a display name — a cryptographic fact.

Contract Signing With Legal Identity

3-5B electronic signatures annually. Most have no verified identity behind them. Derived certs bind government-verified identity to the signature.

When There's No System

$56B

Nationwide identity fraud losses (2020)

$647M

Washington State alone

$1B+

Clawed back through recovery

Washington State's unemployment system was a web form. No authentication. No identity verification. Because there was nothing to plug in.

- Organized crime filed claims from prison WiFi using stolen identities.
- 30 million claims hit at once — no system to verify any of them.
- States sent money and hoped. That was the entire verification strategy.
- AI now generates perfect birth certificates and fake IDs on demand.
- The question isn't whether the next crisis hits. It's whether you have infrastructure when it does.

18013-7 Unlocks the Utility

7 out of 10 digital identity efforts fail. The #1 reason? No utility. ISO 18013-7 fixes that.

Without Online Presentment

mDL only works at airport gates and liquor stores. No remote use. CAs can't verify. Banks can't onboard. Benefits systems stay broken. Infrastructure hoping for use.

With Online Presentment

Every CA becomes a verifier. Banks do KYC remotely. Benefits check identity at scale. Account recovery has cryptographic backing. Utility from day one.

The systems that succeed still need all four:

Utility

Online presentment creates it. CAs, banks, benefits, account recovery.

Anchor Tenant

TSA proved it. Now CAs + financial sector extend it online.

Institutional Trust

DMV authority already exists. Don't build new trust — leverage it.

Governance

10-15% annually. Roots rotate, states join, algorithms age.

Momentum: Utah SB275

Utah Senate unanimously passed SB275

- Digital Identity Bill of Rights — foundational individual protections
- Authorizes State-Endorsed Digital Identity (SEDI) program
- First comprehensive consumer protection framework for digital ID issuers, wallets, verifiers, and relying parties
- First-in-nation Duty of Loyalty — entities must act in individuals' best interests
- ACLU supports it, calling Utah the only state asking the right questions

Why CAs Should Pay Attention

- This is the governance layer the mDL ecosystem has been missing
- State-endorsed, not state-controlled — individual retains the core identifier
- Establishes clear rules for verifiers and relying parties (that includes CAs)
- Identity belongs to the person, not the government — privacy by statute
- Building a multi-state coalition — critical mass for a national framework

Open Challenges for This Room

Root Store Fragmentation

Only 54% of mDL programs have discoverable roots. How do CAs reliably build a trust store? Do we need a centralized VICAL equivalent managed by this community?

Interoperability Testing

Standards without conformance testing fragment. We learned this from e-passports and eIDAS. Who runs the test suite? Who funds it? What does CABF's role look like?

Ongoing Cost Model

Root certs rotate. States join. Algorithms age.

These are governance questions disguised as technical ones.

The WebPKI ecosystem just recognized mDL.

Now we need to build the verification infrastructure worthy of it.

- Participate in interop testing — validate your mDL verification against real state infrastructure.
- Contribute to open-source tooling for the mDL-to-X.509 pipeline.
- Budget for continuous root store maintenance — this is operational, not project-based.

Ryan Hurst · ryan@peculiarventures.com · unmitigatedrisk.com

Utah SEDI Summit Coverage

techbuzz
utah tech news

Search

Utah’s SEDI Summit Charts a Path for State-Endorsed Digital Identity

Utah’s SEDI Summit (UVU - Orem, UT) explored state-endorsed digital identity, emphasizing governance, privacy, and security. Leaders and legislators discussed technical frameworks, policy strategies, and human impacts, charting a roadmap for safe, equitable digital identity systems.

Mark Tullis
Oct 22, 2025 - 5 min read

Orem, Utah — October 22, 2025

In a rapidly digitizing world, identity is no longer just a piece of paper; it is a living, evolving credential that carries the weight of personal

TechBuzz News · October 2025

Coverage of the SEDI Summit at Utah Valley University. Discusses digital identity governance, failure rates, and the framework Utah is building.

The Failure Modes: 30 Years of Lessons

UNMITIGATED RISK

un.mit.i.gat.ed: Adj. Not diminished or moderated in intensity or severity; unrelieved. risk: N. The possibility of suffering harm or loss; danger.

HOME WHO I AM

The Account Recovery Problem and How Government Standards Might Actually Fix It

Leave a reply

Account recovery is where authentication systems go to die. We build sophisticated authentication using FIDO2, WebAuthn, and passkeys, then use "click this email link to reset" when something goes wrong. Or if we are an enterprise, we spend millions staffing help desks to verify identity through caller ID and security questions that barely worked in 2005.

This contradiction runs deep in digital identity. Organizations that require hardware tokens and biometrics for login will happily reset accounts based on a hope and a prayer. These companies that spend fortunes on authentication will rely on "mother's maiden name" or a text message of a "magic number" for recovery. Increasingly we've got bank-vault front doors with screen-door back entrances.

The Government Solution

But there's an interesting solution emerging from an unexpected place: government identity standards. Not because governments are suddenly great at technology, but because they've been quietly solving something harder than technology – how to agree on how to verify identity across borders and jurisdictions.

RECENT POSTS

The Signal They Chose to Ignore
Duplicates Are Not the Problem
Teach to the Median, Punish the Variance
The Data Doesn't Support the Narrative
When Building Gets Cheap, Distribution Becomes Destiny

RECENT COMMENTS

rmhrisk on Agents Are More Like Humans Than Workloads. Here's Why That Matters for Identity.
Adam on Agents Are More Like Humans Than Workloads. Here's Why That Matters for Identity.
Adam on Agents Are More Like Humans Than Workloads. Here's Why That Matters for Identity.

unmitigatedrisk.com

Blog post on account recovery and how mDL standards address it. Companion to "Digital Identity: Learning from Three Decades of Success and Failure."

APPENDIX

mDL State of the Nation Dashboard

mdl.peculiarventures.com

Interactive dashboard tracking mDL deployment across all US jurisdictions.

24	10	54%	45%
TSA	VICAL	Roots	Pop.

- Root certificate discovery and lifetime analysis
- AAMVA VICAL signature verification (ECDSA)
- State-by-state coverage map with wallet support
- Adoption timeline with population curves
- Filter by wallet provider and CORS proxy

mdl.peculiarventures.com

Live dashboard with real-time data from TSA, AAMVA VICAL, and web-discovered roots. Updated daily.

APPENDIX

TSA REAL ID mDL Program

tsa.gov/realid/realid-mobile-drivers-license-mdls

The anchor tenant that made mDL adoption real.

24	250+	May '25
States	Airports	REAL ID

- Final rule (Nov 2024) established REAL ID waiver framework for mDL acceptance at federal facilities
- States apply for temporary waivers; TSA publishes approved list
- 72-hour cybersecurity incident reporting requirement
- Goal: accept mDLs at all airports nationwide
- REAL ID full enforcement began May 7, 2025

tsa.gov

TSA's official REAL ID mDL page. Lists participating states, waiver application process, and security requirements.

APPENDIX

NIST NCCoE mDL Project

SP 1800-42: Digital Identities — mDL

Reference implementation for real-world mDL deployment.

- Use Case 1: KYC/CIP onboarding for financial institutions — simulated bank accepting mDL
- Use Case 2: Federal credential service provider (CSP) and federation
- Use Case 3: Healthcare and electronic prescribe
- Published: mDL assurance mapping to NIST 800-63-4, interaction diagrams, privacy risk assessment (PRAM)
- Consortium includes AAMVA, Apple, Google, Spruce, and 12+ other partners
- Open-source reference implementation in progress

nccoe.nist.gov

NCCoE mDL project page. Includes draft publications, wireframes, consortium details, and community of interest.

APPENDIX

ISO/IEC 18013-5 & 18013-7

Part 5: In-Person (ISO/IEC 18013-5:2021)

mDL data model, credential structure, proximity presentation via NFC/BLE, device engagement, session encryption, selective disclosure. Powers all TSA checkpoint verification. Nearly all wallets support Part 5.

Part 7: Online (ISO/IEC TS 18013-7:2024)

Online/remote presentment protocol. Challenge-response for replay resistance. Browser-mediated and cross-device flows (QR code, link-based). The piece CAs need for remote identity vetting. Adoption still limited — this is the frontier.

iso.org/standard/69084.html