THALES
Building a future we can all trust

Identity in the Digital Age: Lessons from Queensland Mobile Licence Implementation

A case study in citizen-centric, standards-based digital credentials

WHITEPAPER

Executive summary

Queensland has become one of the most closely watched examples of mobile identity in action. Since its statewide launch in late 2023, the Queensland Digital Licence app has been adopted by more than one million residents and is now recognised as one of the most successful mobile driver's licence (mDL) deployments globally. (Department of Transport and Main Roads)

Powered by Thales technology, the app operates as a distributed system, putting the citizen in control of their digital identity, allowing them to store and share secure digital versions of their core identity credentials on a smartphone. The app gives full control to choose what information to share and with whom, ensuring privacy and autonomy over their data. Starting with driving and marine licences and a photo ID card, with additional industry credentials now being added. The solution is aligned with international ISO standards for mDL and digital credentials, enabling selective disclosure of attributes and future cross-border interoperability. (Thales Group)

This paper explains how Queensland is delivering mobile identity today, the lessons learned from earlier implementation challenges faced elsewhere in Australia, and what is needed for mobile credentials to become a trusted, reusable foundation for both in-person and online services.

1. Why mobile identity matters

Governments worldwide are under pressure to modernise identity systems. Citizens expect fast, fully digital services, while businesses face rising compliance costs and fraud risks. Traditional approaches to identity verification – repeatedly presenting physical documents and checking them against central databases – are costly, friction-heavy and increasingly vulnerable to data breaches and synthetic identity fraud.

Mobile identity offers a different model. Instead of asking people to share all the data on their physical credentials every time, a digital wallet on their phone can hold cryptographically protected credentials and share only the attributes required for a given transaction – for example "over 18" rather than full date of birth. This reduces data exposure, supports privacy, and allows credentials to be refreshed and revoked in near real time.

However, mobile identity only works if citizens trust the system and if businesses can rely on it. The Queensland experience shows what it takes to get both sides of that equation right.

2. Queensland's Digital Licence: programme at a glance

The Queensland Digital Licence app is an opt-in digital wallet developed for the Queensland Department of Transport and Main Roads (TMR). It stores digital versions of key government-issued credentials on a mobile device and allows citizens to share them securely when they need to prove who they are or what they are authorised to do. (qld.gov.au)

Supported credentials today

At the time of writing, the app supports a growing set of credentials, including:

- Driving licence
- Recreational marine licence
- Photo ID card for residents who do not hold a driving or marine licence
- Queensland Building and Construction Commission (QBCC) credentials, such as site supervisor, plumber and pool inspector licences

Additional licences and permits are being integrated as part of a "whole-of-government" digital wallet roadmap, allowing residents to access more of their government credentials in a single app. (Department of Transport and Main Roads)

Thales provides the core technology – the wallet, credential issuance and verifier components – operations and professional development, integration and security services. With local Queensland partners Code Heroes and Aliva contributing to app development and support.

3. A citizen-centric, standards-based design

A defining feature of the Queensland solution is its alignment with international standards for mobile driver's licences (ISO/IEC 18013-5) and the focus on decentralised, user-controlled credentials. The app:

- Stores credentials locally on the user's device, protected by strong authentication.
- Uses standardised, signed data structures so that verifiers can check authenticity without needing to query a central database in real time.
- Supports selective disclosure, so only the minimum required data is shared for a given use case

This approach addresses a key lesson from early digital identity initiatives: centralised databases that track every transaction are unpopular and raise concerns about surveillance and security. Queensland's more distributed model helps to mitigate these concerns and has been cited by analysts as a "blueprint" for other mDL deployments. (ABI Research)

4. Everyday use cases: from night-life to parcel pick-up

Although the Digital Licence is a relatively new service, it already supports a wide range of everyday, in-person use cases:

- Age and identity checks in restaurants and bars
- Identity verification when entering events and venues
- Hotel check-in and car rental
- Proof of identity for parcel pick-up at post offices

In these scenarios, the citizen presents their digital credential and the relying party scans or visually inspects it using either the verifier app or, in some cases, the wallet app itself.

From a user perspective, the experience is simple: they open the app, select the relevant credential and present a dynamic, signed representation (often via QR code) that can be checked for authenticity and freshness. Multi-factor authentication and integration with the Queensland Digital Identity (QDI) service provide an additional layer of assurance. (Thales Group)

5. Overcoming challenges with implementation

In Australia, each state is responsible for its driver's licence. As a result, each state developed its own. In the initial deployment of digital wallets, before the international standards were utilised, some implementations had vulnerabilities that allowed digital licences to be modified and used for fraudulent presentation, e.g. for age verification. This undermined the trust of the relying parties in the digital credentials and limited the acceptance to low value transactions. The general public also became cautious about the security and trustworthiness of the digital credentials and identities.

With the development of standards for digital credential and the implementation of standards-compliant mobile driver's licences, the vulnerabilities have been eliminated. However, the early challenges have left some businesses preferring physical IDs as the more familiar and trusted form of proof.

Thales always took a standards-based approach from the start, emphasizing cryptographic security, and subjected their solution to thorough security and privacy testing. This careful approach has helped build confidence among both Queensland citizens and businesses.

> This example serves as a reminder that the success of mobile identity solutions depends greatly on effective implementation. Challenges are inevitable with an undertaking such as this, but it is important that we learn from these challenges and understand that any security flaws can have a long-lasting impact on confidence and adoption of a solution.

6. Adoption and perception: success with room to grow

Since the statewide launch in November 2023, adoption of the Queensland Digital Licence has grown steadily. TMR reports that over one million Queenslanders now use the app – around a quarter of the state's population – and analyst research suggests this represents one of the highest mDL penetration rates worldwide to date. (Department of Transport and Main Roads)

To increase citizen adoption of the licence app still further, policymakers are exploring ways to make the digital wallet more useful by aggregating more government licences and permits into a single place. (ABC)

This cautious yet positive adoption stands in contrast to more centralised identity schemes, which have encountered some resistance due to public perception of the government actively tracking the activities of citizens and data security concerns around having one large central pool of data. In contrast, the approach taken by Australian states by implementing wallet-based systems—a decentralized, user-centric model has fostered greater trust as it enhances privacy and gives individuals more control over how their information is shared.

Although the Australian Digital ID scheme does not explicitly support verifiable credentials such as the Queensland mobile driving licence, it establishes a legal framework for digital identities. States can utilize the Australian Government Digital Identity System (AGDIS) for identity verification and other use cases. The key challenge is to integrate decentralized credentials alongside AGDIS, progressively embedding them in legislation to provide citizens with privacy-focused alternatives.

The lesson for other jurisdictions is twofold:

- **Get the fundamentals right –** security, privacy, usability and standards alignment must be in place from day one.
- **Plan for ecosystem growth –** adding more credentials and use cases over time is critical to sustaining adoption.

Queensland's roadmap, which is evolving the Digital Licence into a broader whole-of-government digital wallet integrated with the Queensland Digital Identity, is a direct response to this dynamic. (Department of Transport and Main Roads)

7. Beyond the wallet: readers, revocation and legislation

For mobile identity to become a trusted alternative to physical documents, it is not enough to issue secure credentials to citizens. The surrounding ecosystem – readers, verifiers, legal frameworks and lifecycle management – must also be designed correctly.

Trusted readers and reader authentication

As digital credentials move from purely in-person checks to high-value or remote use cases, it becomes essential to authenticate the reader as well as the wallet. Queensland's experience highlights several requirements:

- Transactions should be cryptographically signed by both wallet and reader, proving that the credential was presented to a trusted verifier at a specific point in time.
- Readers themselves need their own digital identities and certificates, issued and managed by an appropriate authority, so that relying parties can trust the verification environment.

Without this mutual authentication, remote verification – for example, using a mobile credential to open an online bank account – is difficult to do in a way that meets regulatory expectations, and may also be vulnerable to fraud since the readers themselves could be exploited as a point of attack.

Revocation and "status lists"

A further challenge is ensuring that verifiers can be confident the credential is still valid, especially when checking driving entitlements or work permits. Today, Queensland and many other jurisdictions handle this by giving signed credential data a relatively short validity period – for example, one month – after which the wallet must refresh the data.

To enable more privacy-preserving, real-time status checking, emerging ISO mechanisms introduce the concept of an mDL revocation list or "status list". Rather than querying an individual's identity directly, the verifier requests

a block of sequential entries containing the relevant data. Upon receipt, the verifier checks the specific entry to ensure that the corresponding credential has not been revoked by checking its revocation status.

This approach reduces the risk of tracking citizens across multiple transactions while still giving relying parties the up-to-date assurance they need.

The role of legislation

Finally, legal frameworks must keep pace with technology. In Australia, for example, the deployment of online verification solutions compliant with ISO/IEC 18013-7 is awaiting the necessary underpinning legislation.

In Queensland, legislation already recognises the Digital Licence as legally equivalent to the physical licence for many purposes, but further clarity around how digital credentials can be used in sectors such as banking, employment and anti-money laundering will be crucial to unlocking their full potential. (qld.gov.au)

8. Opportunity to replace

One of the most powerful arguments for digital credentials is their potential to replace legacy document-based verification systems, such as Australia's Document Verification Service (DVS).

Today, many organisations rely on DVS to check physical documents. The relying party submits identity data from existing documents and receives a match/no-match response. This approach has several drawbacks:

- The same identity data is repeatedly shared and stored, increasing the impact of data breaches.
- Identity theft remains relatively easy if attackers obtain leaked document details.
- Each verification is a one-off, chargeable transaction, costing Australian businesses billions of dollars annually.

By contrast, digital credentials in a secure wallet:

- Are far harder to steal or replicate than static document numbers.
- Can be revoked or updated dynamically, allowing "derived" digital credentials to be withdrawn without re-issuing documents.
- Enable reusable trust: once a person has a strongly verified digital credential, it can be reused across multiple services without repeating the full proofing process each time.

Because each sharing transaction is signed at the moment it occurs, attackers cannot simply replay leaked identity data or use AI-generated fakes of physical documents to impersonate someone else.

Examples of emerging online use cases include:

- Privacy-preserving age verification for alcohol purchase, access to age-restricted online services or entitlement to benefits
- Attribute sharing to prove specific rights or qualifications (e.g. trade licences, work permits) without disclosing full identity

9. Building a successful digital credential ecosystem

Queensland's experience points to a set of success factors that are relevant to any jurisdiction considering mobile identity:

1. Clarity of role within the national digital identity framework

Digital credentials must have a defined position alongside other identity providers and authentication methods. Citizens and service providers need to understand when to use the Digital Licence versus other digital identity options.

2. Integration with core digital identity providers

Linking the Digital Licence to the Queensland Digital Identity for onboarding and authentication ensures consistent proofing across channels and avoids parallel, inconsistent identity silos. (Department of Transport and Main Roads)

3. Mandates and policy alignment

Where appropriate, policies and sector-specific regulations should explicitly recognise digital credentials as valid for key processes – for example, right-to-work checks, banking KYC, or AML compliance – to drive adoption.

4. Harmonised proofing and authentication rules

Aligning digital identity proofing and authentication requirements across sectors (banking, employment, government services) reduces complexity for businesses and encourages reuse of a single high-assurance credential. It also ensures a consistent, systematic approach, recognising that a system's overall security is limited by its weakest link—by ensuring alignment, it helps prevent vulnerabilities arising.

5. Standards-based, re-usable design

Following international standards for mobile credentials, wallet interfaces and verification protocols is essential for interoperability, vendor choice and long-term sustainability.

6. Citizen control and privacy by design

Keeping credentials under citizen control, minimising data sharing and using privacy-enhancing status lists all help to build and maintain public trust.

10. Lessons for other markets: an example right-to-work scenario

The same technical building blocks used in Queensland can support a wide range of other credential types. One example is a digital right-to-work credential based on ISO/IEC 23220 "mDoc" specifications.

In this model:

- A government or authorised body performs strong identity proofing (in person or online) and issues a right-to-work credential to the citizen's wallet.
- The credential contains attributes such as name, date of birth, work permit ID and permitted work categories.
- Employers perform checks either online (before an interview) or offline (at the workplace) by verifying the credential's validity and status.
- No full copy of the identity document needs to be stored by the employer; only a record of the verification transaction is retained to meet regulatory requirements.

This illustrates how a well-designed mobile identity ecosystem, such as Queensland's, can be extended to solve adjacent problems beyond driving licences – reducing fraud, simplifying compliance and improving user experience.

Conclusion: Queensland as a blueprint – and a work in progress

Queensland's Digital Licence programme shows that secure, citizen-centric mobile identity is achievable at scale. The app has moved from pilot to mainstream use, supported by strong standards alignment, a decentralised design and a growing ecosystem of credentials and use cases. (Department of Transport and Main Roads)

At the same time, the journey is not complete. Uptake, while high by international mDL standards, still leaves significant room for growth; legal frameworks and sector-specific policies continue to evolve; and technical work on reader authentication, revocation and interoperability remains ongoing. (ABC)

For governments and regulators considering similar programmes, the key takeaway is that mobile identity is not just an app launch – it is the creation of a long-lived trust infrastructure. Queensland's experience demonstrates that when mobile credentials are implemented "right" – with no compromise on security or privacy – they can become a powerful enabler of safer, more efficient and more user-friendly digital services.

Central to this success is the development of a distributed system that does not rely on a centralised database approach for transactions, thereby reducing single points of failure and enhancing resilience. Crucially, such an approach puts citizens in control of their data, empowering them to selectively share information as needed while maintaining their privacy and ownership, which is fundamental to building trust and encouraging adoption.

THALES

Building a future we can all trust

350 Longwater Ave
Green Park
Reading
United Kingdom
RG2 6GF

+44 (0) 118 943 4500

thalesgroup.com