Digital Identity in Drivers Licencing

Bringing convenience and security to drivers and their governments

Insights from Interac Corp.

> "A digital driver's licence housed on a mobile device would enable faster interactions with government and business, as well as remote registration for services and accounts."

Introduction

As in every developed country, cars and trucks are critical to the smooth and efficient operation of the economy — getting commuters to work, moving goods from city to city — and road-related testing, licencing, and enforcement make up an important part of the responsibilities of provincial, regional, and municipal governments. Due to the importance placed on its accuracy and authenticity, the driver's licence has become one of our society's core and most trusted pieces of identification, used for everything from operating a vehicle, to buying alcohol, to registering for a bank account.

Yet today's system has weak points: physical licence cards can be faked, paper permits can be lost, and much time and effort is spent on tracking and storing enforcement mechanisms like speeding tickets. A more effective and efficient system would benefit drivers and their governments, as well as those businesses that rely on authentic customer documentation to stay within the law. Digital identity promises to be a critical element in any new system.

Drivers and residents would be the first beneficiaries. Getting a licence would be faster and more convenient, and a digital driver's licence housed on a mobile device would enable faster interactions with government and business, as well as remote registration for services and accounts. What's more, user security would be significantly improved through the abstraction of personally-identifying information that need not be seen by other people in the course of enabling a simple transaction.

Governments would benefit too. The cost and effort of printing, mailing, collecting, sorting, and archiving paper forms and paper tickets would be markedly reduced. Cash flows should improve to the extent that immediate, digitally-enabled payments for penalties can be incentivized. More rapid completion of traffic stops and less paperwork would free both in-field and in-office resources for more productive tasks. Efficiencies would likely accrue to the wider economy, too: banks, for example, would be able to offer online account opening without having to verify customer documents in person, while still complying with "Know Your Customer" regulations.

Key benefits from digital identity

Improved user experience

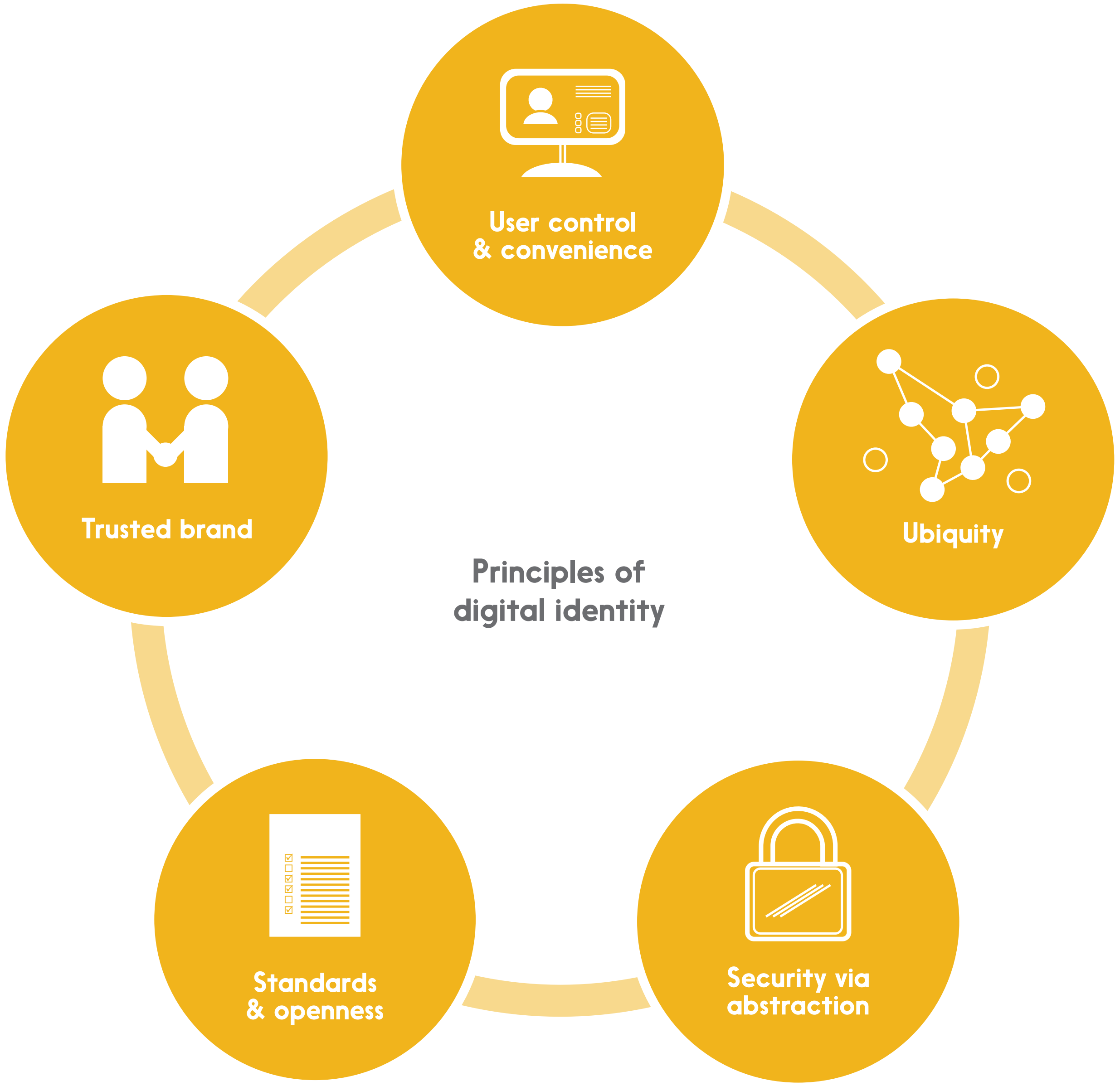
Efficiency

Security & fraud reduction

In the following sections we'll review the five guiding principles that we think should lie at the foundation of any broadly-adopted digital identity system, and we'll look at three examples of how its capabilities could help create a more convenient, more secure, and more efficient driver's licencing ecosystem — with benefits for all.

Our principles

Digital identity is easy to theorize about, but architecting and implementing a comprehensive, secure, and sustainable system is another matter entirely – and an important part of getting it right is having a clearly articulated set of principles to guide the effort. We believe that there are five:



User control & convenience

No one wants to entrust a system with their personal details if those details are going to be transferred to and stored by numerous parties – especially if this happens without the user's knowledge and express consent. While ensuring user control, an identity system must also be convenient and easy; if it isn't, it won't be adopted by users, many of whom are already used to intuitive apps on mobile devices.

Ubiquity

Security risks abound when people have to create different identities and passwords for each public and private service they access: they'll often default to a single, easy-to-remember (and easy to crack) password, for example. At the same time, a digital identity that only applies to a handful of services will probably not be well-adopted. A ubiquitous system is a more convenient and a more secure system.

Security via abstraction

Even with the best user controls, a certain amount of identity data must necessarily be part of transactions in any given ecosystem. A highly effective way of securing that data is to "abstract" it, by replacing a private identifier with a publicly-available one (like a person's email address) or by replacing it with a randomized number that serves as an authorized "token" for the purposes of the transaction – and is not useful for any other purpose.

Standards & openness

In any dynamic system, it's difficult to predict what the future will look like – so it's important to build today's solutions on universally-agreed standards. Not only does this reduce costs by eliminating the expense of building and then later having to adapt custom, one-off solutions, but it enables solutions built by others in the future to "plug into" the initial solution. Openness encourages adoption, innovation, and flexibility.

Trusted brand

No user is likely to adopt an identity solution built or maintained by an organization they don't trust; the question of identity is simply too important, and the impact of identity theft too great, to leave this to chance. Further, building a large-scale (and ubiquitous) solution will require the cooperation and coordination of many players, and these players need to trust each other and the organization leading the effort.

Example 1

Onboarding & records

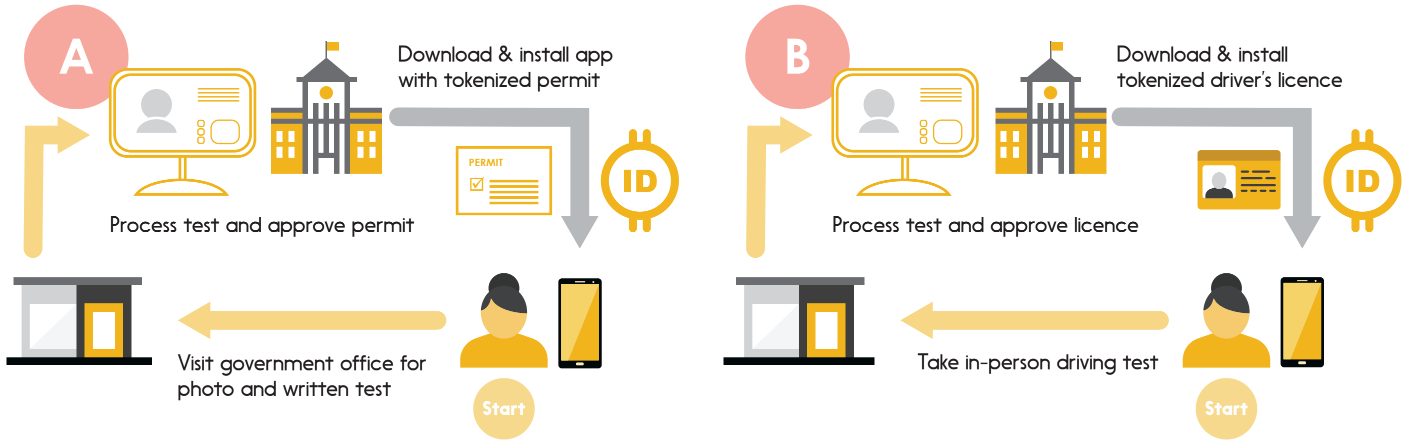
Digital identity promises new efficiencies and new capabilities for Canadian drivers and their governments. Consider the following scenario.

To obtain a licence for the first time, a new driver reports to her nearest government services bureau. She completes a vision test, has her picture taken, pays the service fee, and sits down to take her written test. While she writes the test on a mobile device provided by the bureau, her digital photo and other government-validated information are integrated into both a paper permit and a digital permit card. On passing the test, the driver receives a notification on her own mobile device saying that her digital permit is available. Following a link, she downloads a government app and uses it to install the permit on her device. The app then prompts her to take a selfie so it can verify her identity against the photo taken earlier, and once this is done, it activates the card in its digital wallet. Later, after passing her in-person final driving test, she goes through a similarly quick process to download her permanent driver's licence before leaving the service bureau.

Renewing her licence is equally easy. The government app on her mobile device prompts her well in advance of the renewal date, and she follows its instructions to take a selfie in front of a white wall (without smiling, of course). The system verifies her identity against the last two photos it has of her, allows her to update her address information if necessary, and then offers her some options for paying the fee digitally via her mobile device's digital wallet. That done, her digital licence is updated and renewed instantly, and its physical counterpart follows in the mail a few days later.

After a few years, she moves to another province for a better job, and upon arrival, accesses that province's online services. The government's system requests a new selfie and authorization to access the digital driver's licence on her device, and verifies that information with the province she came from. Within seconds, she receives a notification to download a provincial government app and her new digital driver's licence, and on doing so, her old one is automatically revoked.

Onboarding with digital identity


A
Download & install app with tokenized permit
PERMIT
ID
Process test and approve permit
Visit government office for photo and written test
Start
B
Download & install tokenized driver's licence
ID
Process test and approve licence
Take in-person driving test
Start

Example 2

Enforcement & payment

Traffic enforcement and payments could similarly be improved to the benefit of both drivers and municipalities.

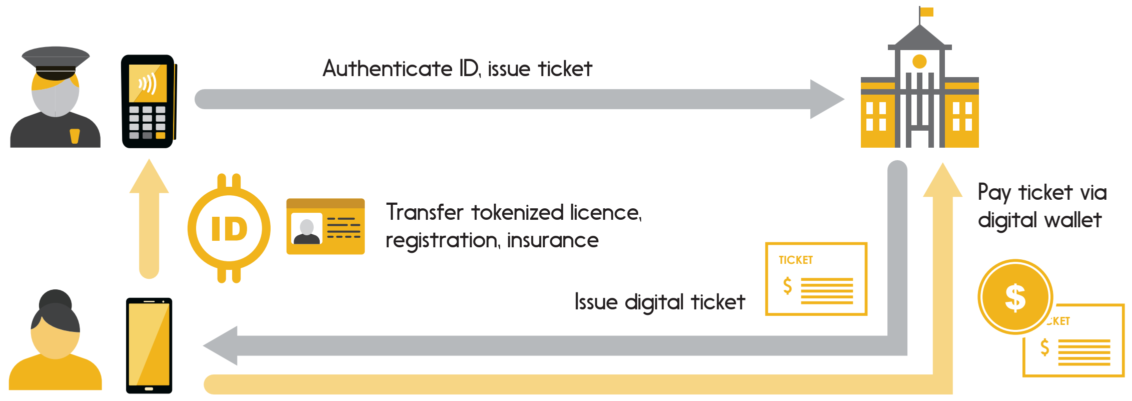
A police officer stops our driver for speeding. The driver holds up her phone, which contains digital versions of her vehicle registration, her insurance, and her driver's licence; the police officer taps it with an NFC-enable device, authenticating the driver's identity and licence status immediately. This approach reduces identity fraud through encryption and other digital security measures meant to prevent tampering or replication of the licence. It also reduces the risk of identity *theft* by minimizing the personally-identifying data that the officer can see and abstracting the rest into a digital "token" that would be inspected and authenticated remotely (and instantly) by a trusted third party. (This feature would be even more useful in the many places where driver's licences are demanded as proof of age — like night clubs.)

This means that if a driver's licence were to be suspended for any reason, the suspension would be logged by the third party and the driver immediately informed via a notification — serving as an effective and timely spur to action. It would also be flagged when the licence token is submitted for authentication by a police officer, allowing them to take appropriate action without uncertainty or further delay.

Luckily our driver has a licence in good standing and only has to pay a fine for speeding. This too can be done digitally: the officer creates a ticket on his device, attaches the driver's tokenized licence to it, and submits it to the municipality's traffic enforcement system. The ticket then appears on the driver's phone, with a small discount highlighted if the ticket is paid that day (since encouraging prompt payment helps the municipality's cash flow), and the app provides its usual options for paying the ticket immediately using the device's digital wallet. The driver pays, and is on her way again — having spent only a minute or two interacting with the police officer and the app.

Even more importantly, the police officer has now been freed for other duties — or further stops — and the burden of handling paper tickets has been removed from the department's shoulders.

Enforcement with digital identity


Authenticate ID, issue ticket
ID
Transfer tokenized licence, registration, insurance
Issue digital ticket
TICKET
$
Pay ticket via digital wallet
$

> As proof of her identity, she authorizes the app to transfer the "tokenized" information from her digital driver's licence

Example 3

Registering for services

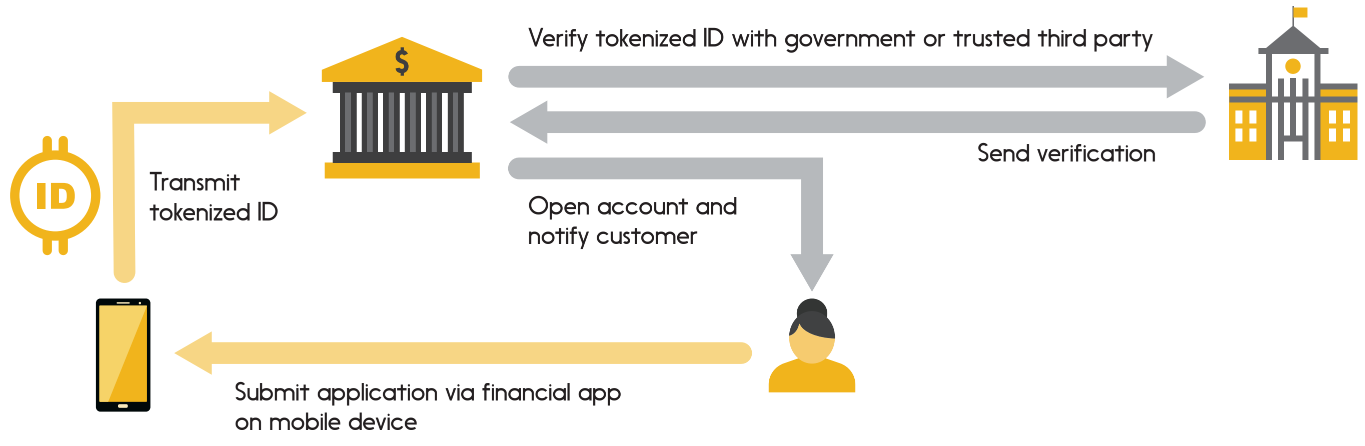
Digital identity in licencing would be useful not only for driving situations and related procedures, but also for any situation in which a driver's licence has traditionally been required to prove identity.

The driver from our previous examples can use her digital licence to easily access a range of services.

To open a new bank account, she first downloads the financial institution's app to her mobile device. As proof of her identity, she authorizes the app to transfer the "tokenized" information from her digital driver's licence held within the government app — as mentioned earlier, tokenization replaces private data in the licence with randomized data used only to authenticate that one transaction. The app auto-fills a handful of fields in her account application from data in her licence, and she completes the rest. The bank receives the application, and its systems use the tokenized card to authenticate her identity against a secure database maintained by the government or a trusted third party. It then opens an account for her within seconds of her submitting the application forms. She never has to visit the bank in person.

Similarly, she'll one day be able to register for additional government services just as easily as for financial services. Instead of having to visit a government office in person to present her identification documents (birth certificate, driver's licence, etc.), she'll simply pull up the government services website and use her digital driver's licence to prove her identity and to securely sign her completed registration. Since she'll be digitally authenticating herself, the system may well be able to source her address and other necessary details, with her express consent, from other government agencies, eliminating the need for her to fill in many of the fields in the registration, and as mentioned, removing the need for her to stand in line at a government office. Should she ever decide to change provinces, she would be able to access local provincial services in her new home in an equally simple fashion.

Services registration with digital identity


ID
Transmit tokenized ID
$
Verify tokenized ID with government or trusted third party
Send verification
Open account and notify customer
Submit application via financial app on mobile device

Conclusion

Driver's licencing is a critical government responsibility and a basic economic requirement, and digital identity is a powerful way to transform both its operation and its outcomes:

Improving client experiences, by speeding processes, eliminating wait times, and enabling remote registration for services.

Driving efficiencies for both governments and private-sector institutions by eliminating paperwork and freeing resources for additional assignments.

Strengthening security and reducing fraud, by using instant digital "yes or no" validation of a licence by a trusted third-party to eliminate the need for special training of in-field personnel (and for subjective human judgment), erasing a point of vulnerability to forgery and other identity-based crimes.

As we've noted in previous papers, digital identity systems can – and should – be rolled out incrementally, building on the capacities and the trust embedded in existing systems and processes. Yet while following a step-by-step plan, governments should develop a holistic strategy, keeping their eye on an ultimate vision that encompasses as many services as possible, establishing a rigorous structure of user control and consent, and using open standards to ensure that other levels of government – federal, provincial, municipal – can connect easily into the emerging framework when they're ready to do so.

> "Digital identity systems can – and should – be rolled out incrementally, building on the capacities and the trust embedded in existing systems and processes."

For more information on this topic, visit innovation.interac.ca

Published February 2019

Except as permitted by law, this document shall not wholly or in part, in any form or by any means, electronic, mechanical, including photocopying, be reproduced or transmitted without the authorized consent of Interac Corp. This document is for informational purposes only and Interac Corp., by publishing this document, does not guarantee that any information contained herein is and will remain accurate. Interac Corp., including its agents, officers, shareholders and employees shall not be held liable to any party or parties for any loss or damage whatsoever resulting from reliance on the information contained in this document.