Citizen Identity: The Key to Unlock a 24/7 Online Government Service Model

THE AUTHENTICATION COMPANY

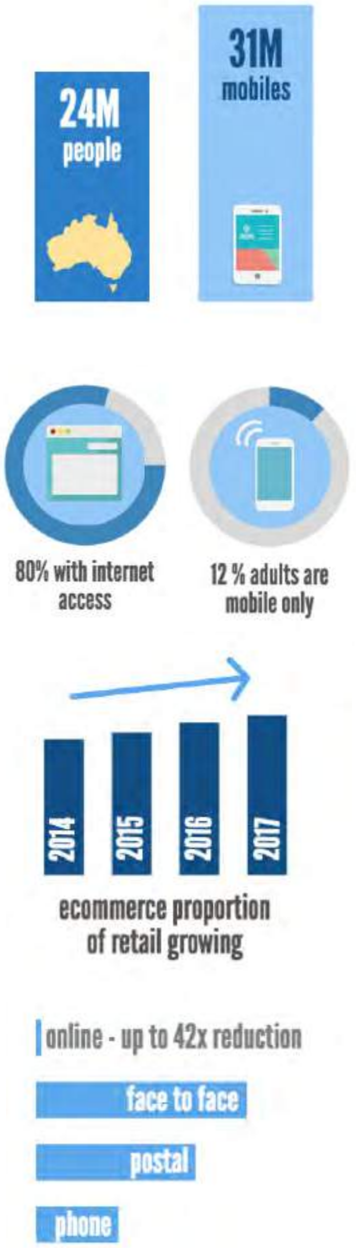
Introduction

The numbers say it all.

- There are over 31 million mobile phones[1] in Australia, that's more than one for every man, woman and child in Australia[2].
- Over 80 percent of households[3] have access to the internet in Australia and 12 per cent of adult Australians[4] use mobile devices for voice, messaging and internet access.
- eCommerce accounts for more than A$11 billion[5] every year and is growing as a proportion of total retail sales.
- Digital and online channels deliver up to a 42x reduction[6] in customer servicing costs.

Australians of all ages have already embraced the digital world for work, school, communication, entertainment and shopping. With such broad digital acceptance, it's logical that government services can harness this acceptance to simultaneously deliver services faster to citizens, and save taxpayer dollars.

But in designing services for the digital world, the expectations of citizens for fast, simple and easy access and the security, transparency and privacy responsibilities of government can seem to contradict. And it is these contradictions that need careful consideration in the planning, framework development, operation and oversight stages of any identity verification and authorisation initiative.


24M
people
31M
mobiles
80% with internet access
12 % adults are mobile only
2014
2015
2016
2017
ecommerce proportion of retail growing
online - up to 42x reduction
face to face
postal
phone

[1] ACMA, December 2014, Communications Report 2013–14
[2] According to Australian Bureau of Statistics, Australia's population was 23.8 million at the end of the September quarter 2015 (Australian Demographic Statistics, Sep 2015)
[3] ACMA, December 2014, Communications Report 2013–14
[4] As reported by ACMA in its 'Australians get mobile' Research Snapshot, 9 June 2015, based on data from Roy Morgan Research's Single Source Jan 14 to Dec 14
[5] eMarketer, Forecast of the global retail market and retail ecommerce sales worldwide, December 2014
[6] Deloitte Access Economics 2015 'Digital transformation of government' report commissioned by Adobe

Contradictions abound

It’s a conundrum faced by many governments across the globe and distils into five main factors:

1. Transparency
2. Customer-experience (or Citizen-experience)
3. Trust, privacy and security
4. Cost
5. Future-ready technology

1

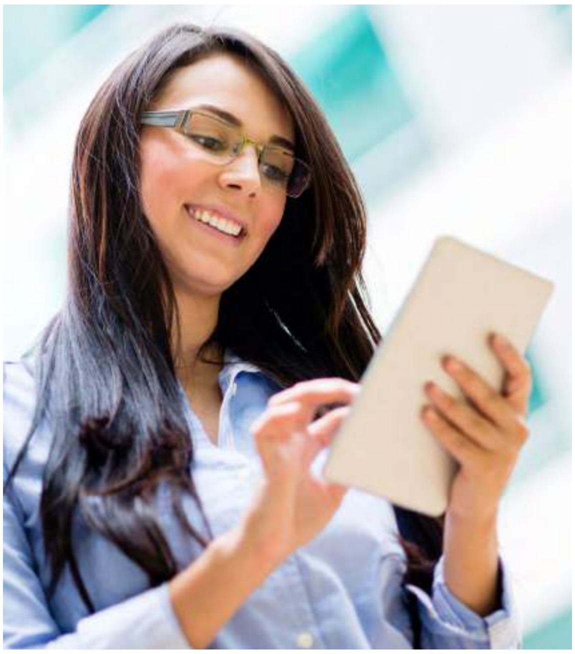
Transparency

Customers have the right to understand the personal data any organisation in Australia holds on them. Organisations can also gain huge benefits by linking relevant personal data across related businesses. However, current regulations limit the ability of organisations to share data unless explicitly authorised by the customer. While government can be a special case, many customers or citizens expect a similar level of transparency from government departments as the transparency they encounter in the business world.

However, without a single identity credential accepted and able to be verified by each government department, the process to enable transparency is clunky, slow, prone to human error and wholly unsatisfying for the citizen. Additionally, as each new agency or department is joined together for a more holistic view of a citizen, the value of that single source of identity data becomes increasingly attractive to hackers and identity thieves. The highest levels of secure access and identity management is mandatory but typically results in an ‘ugly’ experience for the citizen to perform normal government interactions.

A federated identity model provides a popular solution to this problem. A federated model reduces complexity and simplifies access to multiple government online properties within the same federated infrastructure. As validated credentials can be reused, once a user's identity is confirmed, access to authorised services and applications is granted. Users can securely switch between the different applications and collaborate with colleagues, business partners, suppliers, customers and partners using one single identity. Obviously, security at the point of initial access to a federated model takes on even more importance. Using two-factor, or strong, authentication is an efficient way to solve this security challenge.

This framework also benefits other levels of government. Local governments can leverage the identity infrastructure and strong user authentication to offer more services online such as rates, registrations and lodgements. This high level of trusted identity extends to mobile apps so citizens using local government services have a convenient, secure and easy to use channel for local issue interactions.



2

Customer-experience (or citizen-experience)

In embracing a customer-centric approach to improve the customer experience, the public sector can learn a lot from the private sector. Reorientating an organisation to think and act from the customers or citizens viewpoint is difficult and requires vision, dedication and planning. But with over 50 percent of the current government transactions having a problem, overcoming these difficulties can deliver huge benefits.

Already the Singapore government has sought to overcome these difficulties via a single, highly secure and massively convenient credential.

Launched in March 2003, Singapore Personal Access (or SingPass) is a gateway to hundreds of e-services provided by more than 60 government agencies. Users only have to remember one password when connecting and transacting with the Government.

Enhancements were made in mid 2015 to better meet users' needs, and included an improved user interface, mobile-friendly features and stronger security capabilities, such as 2-Step Verification (also known as 2FA), for sensitive government e-transactions. With 2FA, users are required to enter a One-Time Password (OTP). This is in addition to their SingPass username and password, thus better protecting their personal information. The same system offers three different two-factor authentication functions; one-time password (OTP), challenge response and transaction signing. These security functions add a proven extra layer of protection against hackers and from mid 2016 onwards, all government e-services involving sensitive data will require SingPass 2FA to perform sensitive e-transactions.

The highly secure credential ensures a simpler, faster and more convenient experience for the citizen and is equally usable for a mobile-only millennial, iPad-on-the-run mum or a desktop-based retiree.

3

Trust, privacy and security

A key element in the customer-experience equation is trust. Regardless of how convenient the credential might be, citizens will resist use if they feel it isn't keeping their sensitive personal data secure. That security is mandatory no matter where citizens are in Australia or even when travelling overseas. In fact, one viewpoint is that security should be even more stringent when the services are being accessed from outside of Australia - but still enable Australian citizen to easily complete their transaction.

Already individual Australian Government agencies are using sophisticated bank-grade credential and authentication systems from VASCO to enable staff and citizens to easily access government data without any reduction in the security of the data or the government systems. They join the governments in Singapore and Belgium as leaders in the quest for a frictionless citizen experience and a highly secure infrastructure.

4

Cost

Implementing a secure trusted identity solution involves costs - but on the flip side, the failure to deliver public services also involves costs. Government departments already bear the burden of correcting online transaction errors, manually processing what should have been a simple and quick digital transaction.

In Belgium, the agency responsible for defining and implementing the federal e-government strategy, Fedict, has found a way to drastically reduce the cost of a nationwide trusted identity system.

According to Walter Van Assche, general director at Fedict, “the criteria said the authentications made for government applications are made for free, so this is a real win for the government since we did not have to invest. It is also a win for VASCO, since building a system for ten million Belgian people gives them a good reputation. This is a real win-win situation.”

Implementation was easy as well. The only thing Fedict had to do was to adapt their log-in pages to add the option “log-in with partner authentication”, according to Van Assche. If the citizen chooses that option, they go directly to VASCO’s Trusted Digital Identity service MYDIGIPASS. “Then they are sent back to us. Before using it the first time they have to activate a MYDIGIPASS account with a connected device.”

5

Future-ready technology

At the core of any public sector data security initiative is the tug-of-war between the efficiencies and benefits of online access and the hacker / breach threat.

While it is impossible to future -proof the chosen technology base and framework, it is possible to develop an architecture that incorporates future-readiness. Future-ready approaches are built on open standards, high levels of interoperability and an expectation of innovations to come. The future-proof framework can operate effectively now but has the flexibility to morph into the verification and authentication backbone required to serve the citizens and departments of the future.

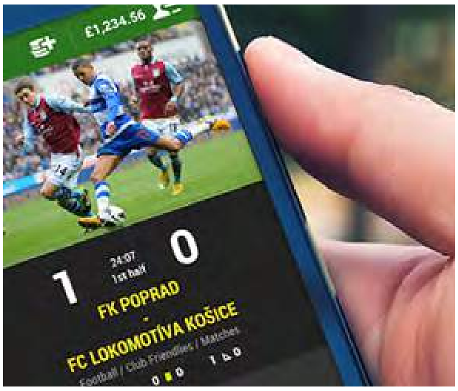
Already in Belgium, the eID digital identity of a citizen can be linked to the VASCO trusted digital identity service to provide digital ID proofing, electronic signing and super-convenient mobile access for citizens. Mobile access to certain government applications, such as tax declarations, policy reports or student registration, can now be granted with an eID-card in unconnected mode, while previously only USB-connected eID mode was accepted by the government. This greatly facilitates the use of eID in mobile environments.

“Our main goal is to give every Belgian citizen faster and easier, but above all, secure access to online government services,” stated Walter Van Assche, General Director at Fedict. “By offering citizens a solution to log in with the eID ... from any mobile device, we have taken a huge step forward in our mission to provide additional digital services to Belgian citizens.”

This frictionless access channel creates the opportunity for more government services to be available online 24x7 and strategically adopts the technology of choice (mobile) of the next generation of citizens.

Belgium businesses have even started to leverage the government investment in eID to improve their business processes and regulatory compliance. Unibet, one of the largest online gambling operators in Europe, will start using the VASCO solution to verify the registration of its users and optimise the registration process based on eID data. The strategy underlines Unibet’s ongoing commitment to provide a positive gaming experience within a secure digital gaming environment and to promote responsible gaming as part of a sustainable ‘value-adding’ relationship with its customers.

According to Ewout Keuleers, Head of Legal at Unibet, using VASCO means “the technical capabilities and tools (are) available in-house to meet the demand of the Gaming Commission and actually to surpass its requirements. We are also able to better protect people with a gambling problem against themselves. After all, we believe in quality players and will provide more transparency to improve the image of our industry.”



The combination of eID and VASCO Trusted Digital Identity service, via website or the mobile app, enables each citizen to easily authenticate and access applications beyond those traditionally provided by government. For example, organisations and businesses can now onboard customers faster online while still meeting regulatory requirements for customer identification.

Eliminating the contradictions with VASCO

VASCO is a recognised leader in trust security through two-factor authentication, electronic signature, mobile application security and risk management solutions to businesses and government agencies in over 100 countries worldwide.

Governments from across the globe have tapped into VASCO's market leading heritage and decades of data security experience and innovation to help meet the contradictions of government. In each case the resulting architecture and practical solution was bespoke but all leveraged VASCO's proven technologies, solutions and approaches.

The five government contradictions can be addressed in a robust and agile framework using VASCO's strengths in identity management, two-factor authentication and electronic signatures.

Addressing the contradictions

1. Secure transparency
With an identity proofing and management system to control access to government data, more data can be shared securely with each citizen enhancing the level of public sector transparency. The Belgium eID example shows how a digital identity system can enable greater sharing of government data and secured transactions with multiple government departments from a single credential.

2. An optimal customer experience
Regardless of the citizen population breakdown, VASCO's broad offering enables each organisation or agency to build an identity framework to suit citizen ease-of-use and government authentication and identity needs. Options include authentication via biometrics, mobile, software or hardware on any combination of desktop, tablet and mobile platforms. Additionally, risk-based authentication solutions provide broad and integrated authentication options that will "step up" to require additional user authentication as needed, based on activity score and level of risk.

3. Banking-grade security
Leading banks across the world entrust secure customer access to advanced VASCO solutions. These solutions that were developed to meet stringent regulatory banking environments deliver the same high levels of security for

government. Banks such as Commonwealth Bank, HSBC, Citibank and Standard Bank have proven the VASCO solutions to be highly secure while streamlining customer access to banking details.

4. Low total cost of ownership

VASCO's flexibility extends to ensuring your identity and authentication needs are met in the most cost-effective way. The Belgium Fedict eID example shows the innovative approaches VASCO has taken to achieve government objectives. Flexibility in pricing and deployments and the ability to leverage existing technologies help to deliver sophisticated identity and authentication capabilities for a low total cost of ownership.

5. Be future-ready now

An approach centred on a single credential relies on interoperability and open standards - essential elements for future-ready frameworks. As a member of the Fast IDentity Online (FIDO) Alliance with FIDO-certified offerings and the range of highly-interoperable solutions, VASCO is committed to innovation that can be easily assimilated into existing solutions and frameworks. Similarly, VASCO innovations are developed with the objective to balance ease-of-use and highly secure solutions. For example, VASCO's API-based authentication platform, as anon-premise or cloud-based service, enables world leading authentication and identity proofing to be embedded into government applications.

A digitally savvy Government

Every country is different.

However the need to overcome the challenges of transparency, customer experience, trust and security, cost and future-ready technology is universal.

While Australian Government departments have individually invested in securing data, access and identity; a broader government architecture approach can take lessons from overseas governments like Singapore and Belgium to find a faster path to a digitally savvy government of the future and a framework that works.

Find out more

Contact VASCO to:

- find out more about the Belgium and Singapore government approaches to identity frameworks;
- learn from VASCO's experience with identity initiatives across the globe; and
- discover the benefits a wide range of innovative trust security solutions can deliver for the public sector.

+61 2 8061 3700
info-australia@vasco.com.au

About VASCO

VASCO is the world leader in providing two-factor authentication and digital signature solutions to financial institutions. More than half of the Top 100 global banks rely on VASCO solutions to enhance security, protect mobile applications and meet regulatory requirements. VASCO also secures access to data and applications in the cloud, and provides tools for application developers to easily integrate security functions into their web-based and mobile applications. VASCO enables more than 10,000 customers in 100 countries to secure access, manage identities, verify transactions, and protect assets across financial, enterprise, E-commerce, government and healthcare markets.

Learn more about VASCO at www.vasco.com or visit blog.vasco.com

VASCO®

THE AUTHENTICATION COMPANY