Digital Identity Considerations for the NSW Office of the Registrar General.

Australia Post

Introduction

Australia Post plays a current role in the Property Transfer eco-system, utilising our vast retail network to provide Verification of Identity (VOI) services acting as an Identity Agent on behalf of Conveyancers, Lawyers and Mortgagees. The discussion paper references the note that "in future, eConveyancing in NSW may utilise digital identity systems" (4.3 Other Considerations). We would like to share with the NSW Office of the Registrar General some learnings we have identified with regards to Digital Identity.

In September 2018, the Digital Transformation Agency (DTA) published an initial release of the Trusted Digital Identity Framework (TDIF) which considers 'level 4' security which would be equivalent to the current VOI framework. Given the swift pace of change in this area, Australia Post is keen to share our latest experience, and provide information from our security and policy team, and information regarding the DTA standards.

Background

IT security is always changing, and in consideration of strong reusable digital identity means many organisations across Australia will need to look forward and prepare to adjust their security posture in advance of actual threats. Online digital identity is a powerful tool for enabling consumers and citizens, but once established, a reusable identity requires significant security protections around it.

In the context of high value transactions, such as eConveyancing, we believe there are a number of areas where the NSW Office of the Registrar General may want to begin planning to use the improved security services that are becoming available. Services such as the Document Verification Service (DVS) and the Facial Verification Service (FVS) are becoming available for commercial identity verification, and technology such as ePassport chip reading is becoming more practical with modern smartphones.

The NSW Office of the Registrar General could also consider how the use of strong digital identity at various stages of a customer interaction could change the nature of transactions. The reuse of digital identity is seen by the DTA and others as key not only to customer convenience, but also for improving security, lowering error rates and improving compliance. Additionally, as digital identity becomes more widely used, it is seen as opening up new technological opportunities such as the use of digital signatures in contracts.

Verified identities could be used multiple times by multiple parties during a property transaction; explicitly during VOI checks, and implicitly at other stages such as during the signing of documents and during financial transactions.

Strong, consistent electronic identity can streamline many of these processes, particularly when combined with the other documentation procedures involved in transactions –

e.g. forms can be pre-filled, lowering error rates, and more preliminary work may be done online.

Better and more consistent communication channels can also be established (as changes in contact details can be easily notified), and in future electronic signatures can be used to make contract signing more convenient and more secure.

Digital Identity - Emerging Risks

Identity Verification Risks

The identity checks currently completed for Property Transfer transactions are generally done to a high standard, however the DTA and Australia Post have identified a number of fraud vectors that are becoming more common with lower value transactions.

While Australia Post has not experienced any concerns in relation to its current VOI service, we are conscious of these threats and need for industry to get ahead of them. The DTA's new TDIF provides good guidance as to how to address these threats.

Specifically, the DTA has addressed a number of the concerns around relying on document based identity, either online or in-person, and in co-operation with the Department for Home Affairs (DHA) has developed checks that make it increasingly difficult for fraudsters to impersonate others, or create fake identities.

Some of the risks addressed are:

- **Identity Theft -** stealing personal data, document details or actual documents and using them to impersonate others is becoming more common in a variety of frauds.
- **Document Forgery -** very high quality forgeries are now available online, particularly on the dark web. These forgeries include hologram overlays and other security features, and can be difficult for even trained operators to detect.
- **Creation of Fraudulent Identities -** some individuals have been able to create entirely false identities by starting with low-security documents and using them to slowly obtain more and more credible documents.
- **Credential Theft -** people stealing credentials, or masquerading as others when 'recovering' credentials, has become a significant security problem.
- **Biometric Impersonation -** technology to allow people to masquerade as others using recordings, photographs, videos, masks etc. is becoming more common.
- **Operator Fraud -** the risk of dishonest or incompetent operators falsely verifying documents or photo ID.

In general, there are a number of controls to manage these risks. For example, the in-person checks that are currently mandated for Property Transfers (ARNECC) discourage many types of fraud already; document theft is less useful if an in-person photo ID check is required.

Nevertheless, fraud tends to move around; as one area of fraudulent activity is closed down, fraudsters move to the next; and as new technology becomes available, fraudsters will find new ways of defeating existing controls.

For this reason, the DTA has defined a new set of standards, and the Department of Home Affairs are making available new security tools, to help authorities such as the NSW Office of the Registrar General maintain high levels of security.

Issues with Online-Only Verification

There has been significant recent progress with online verification, and this is now commonly used for lower security identity checks, where it is often more convenient than in-person checks.

Unfortunately, the increased use of video and automated facial matching has led to an arms race between both verifiers and fraudsters.

While many of these attacks are still limited to academic research, this is now a contested space with rapid, and not always even, progress made between attackers and defenders.

On the defending side, new breakthroughs in using infra-red sensors and 3D mapping of faces are improving the accuracy of facial recognition. Unfortunately, these techniques often rely on the very latest smartphone technology, and only a minority of users have such cutting-edge phones.

Similarly, research is continuing on facial matching algorithms, with a wide range of approaches being trialed. Current research appears to be concentrating on deep neural networks, which, when correctly trained, can show very good results.

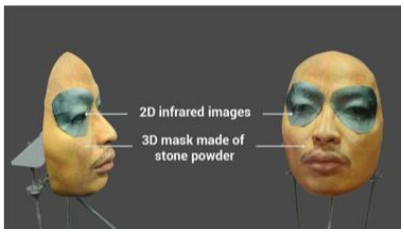
These neural networks are also now becoming available for smart phones (although wide spread deployment is probably some years off).

On the other hand, fraudsters and academics have come up with a number of mechanisms for fooling facial verification systems, including[1]:

High quality synthetic videos of people (https://www.bbc.com/news/technology-47296481)

3D printed rubber face masks (https://motherboard.vice.com/en_us/article/qv3n77/iphone-x-face-id-mask-spoof%20)

Using pre-recorded video of the target (https://www.gizmodo.com.au/2015/03/man-its-still-so-easy-to-fool-facial-recognition-security/)



Misleading a deep neural net facial recognition system with spurious training data

https://www.theregister.co.uk/2017/12/20/fool_ai_facial_recognition_poison/)

Most of these attacks are currently (February 2019) impractical for the general public, requiring specialist knowledge and skills.

However, software moves quickly, and what was a difficult image manipulation task that cost millions of dollars yesterday becomes a toy for children today, with animal masks and 'face switching' apps now available for free download.

Given the back-and-forth nature of the struggle between online verification technology and imposter technology, and without a clear advantage being obvious for verification, the DTA has decided to maintain the requirement for in-person face

checking for “Level 4”, their highest level of security[2].

In-person verification checks address all of these attacks, as humans are remarkably good at recognising rubber masks, videos and printed photographs, and are not easily confused by extraneous details in the way that automated systems currently are.

There are of course many other ways that human operators can be fooled though. As a result the DTA directs that human operator checks be combined with automated checks.

This creates a very strong level of security, as the types of fraud which can fool computers are generally very different from those that fool humans; in particular facial recognition performed by both a human and a computer is generally very strong[3].

1 This is in contrast to the latest US standard, NIST SP.800-63-3, which allows video verification to be performed if the identity provider can satisfy themselves of the security of the complete end-to-end process.

However even under NIST, the requirements for online facial verification are very strict, requiring the consumer to be in a controlled environment; something that is likely to be impractical for the majority of verification use cases considered in eConveyancing.

2 https://www.nist.gov/news-events/news/2018/05/nist-study-shows-face-recognition-experts-perform-better-ai-partner

The DTA ‘Level 4’ Standard

OTA: 'Level 4' Verification

The DTA addresses the risks of identity verification through a series of 'Identity Proofing Levels' ranging from 1-4, where level 3 is suitable for general purpose, sensitive government transactions, and level 4 is suitable for high risk transactions, or transactions that have very significant monetary value.

The DTA requirements for Level 4 Verifications can be summarised as:

- A ‘Commencement’ document such as a birth certificate, checked to an online data source.
- A ‘Photo Bind’ using both a human operator and an algorithmic check to a reliable source.
- Checks that the applicant has been ‘operating in the community’ for at least five years.

There is a particular emphasis in the new standards on checking documents to a reliable source, including checking the facial data on documents (in particular passports and driver’s licenses).

The standard is flexible to an extent on what the source may be; e.g. it might be checked with the Department of Home Affairs 'Document Verification Service' (DVS), it might be checked directly with an issuing body, or it might be checked against a cryptographically secured chip (such as is embedded in modern passports).

The permanent record left by these digital checks can also reduce the need to store document details, which may reduce the administrative load for some of the current identity checking parties.

Recommendations to the Registrar General for High security ID reuse

The key challenge with security in ID reuse is ensuring the end-to-end security of an online identity verification check. To be completely trusted, the applicant must perform the check in a secure and controlled environment, using a secure device, over a secure channel to a secure identity service provider. Unfortunately, this ‘chain of security’ from the applicant to the identity provider is largely out of the control of the provider.

Due to the lack of direct control, the provider must rely on indirect methods such as liveness detection and device scanning to try to ensure security - mechanisms which, while currently reasonably secure, are under threat by technological developments elsewhere. Our judgement is that in future this may not be able to be done completely securely, particularly as technology moves on and video impersonation software continues to improve. Accordingly, while the DTA and ourselves still consider digital authentication and re-use to be appropriate, even at the highest level of security, we suggest supporting in-person identity checks to establish a digital identity, while allowing identity reuse with appropriate security, such as outlined by the DTA standard.

We suggest that the NSW Office of the Registrar General could:

- Align verification checks with the TDIF standard for a common trusted

standard for identity verifications across the property ecosystem

- Either Accredit, or use Accredited, Providers – the DTA has outlined detailed requirements for Identity Providers, including Privacy requirements such as formal PIAs, Security requirements such as ISM compliance accessed via the IRAP program, and a variety of operational, risk and UX requirements.
- Consider Digital Contracts – Digitally signing documents with strong digital identities is convenient for all parties, and removes the temptation to cut corners that has been found to occur in other sectors of the financial industry.
- Allow Digital Identity Reuse (with appropriate security). This would allow parties to conveniently transact across multiple stages of related property transaction activity with both greater convenience and improved security. We believe this will also lay the foundations for systemic efficiency improvements throughout the conveyancing process, with advantages for legal practitioners, financial agents and conveyancers. Independently of identity security, it will allow for more accurate data entry, better analytics, improved access security, and lower risks such as vendor impersonation.

Conclusion

We recommend the Office of the Registrar General consider some of the themes and learnings in this paper before adopting a digital identity solution as part of their eConveyancing requirements.

While automated face matching continues to improve, a human verification against a photo ID combined with back to source document checks, is a strong control against impersonation by reducing the risk of advances in imposter technology and high quality forgeries that are becoming more available.

Any Questions:

Peter Unkles
Industry Pursuits Lead
Level 1, 111 Bourke Street Melbourne VIC 3000

T 03 9107 1054

M 0458 340 020

E peter.unkles@auspost.com.au