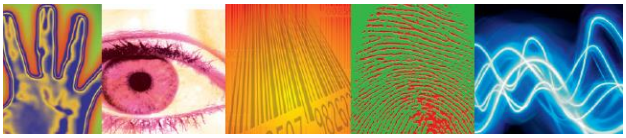


Digital Onboarding and Biometrics

Introduction

We are a society that increasingly demands instant gratification and minimum waiting time for many processes that are part of our everyday lives. Now with the need for remote interaction foisted on much of the global population by COVID-19, organisations are under increased pressure to facilitate secure digital onboarding of customers to services. Business functions which rely on in-person implementation have been impaired by the pandemic, while remote onboarding and service delivery have experienced dramatic growth in many areas.

This paper provides a high-level overview of how biometrics intersects with digital identity onboarding to guide decision-makers considering, or already implementing, the use of biometrics in online sign-ups. It is aimed at bodies considering the attachment of a digital identity to a human identity using biometric technology. For example:

- The use of biometric data held in a government-issued identity credential such as a passport or electronic identity (eID) card to facilitate a bank setting up a new account
- An agency enabling access to citizen services, as part of a digital identity creation process

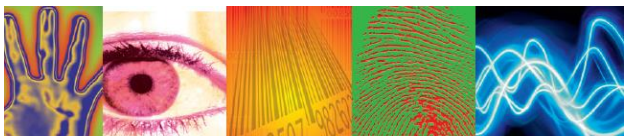
The paper covers:

- The re-use of an existing digital identity
- Considerations in the process of attaching a digital identity to a person
- De-duplication – the process of ensuring a unique representation of a person
- Guidance in formulating strategies
- Making ethical and responsible decisions in biometric applications, with reference to specific sections of the Biometrics Institute's *Good Practice Framework* [1]

Background

Online sign-up processes – or onboarding – have been part of the digital transformation landscape for some time. In low-security contexts, like social media, onboarding requires minimal identity proof from the new customer. In more sensitive contexts, like banking and government services, greater identity proof is required to link the digital service to a specific person. These contexts have until recently typically used in-person, rather than remote, sign-up processes.

Pressure to streamline onboarding experiences in these more sensitive contexts is building from different directions. Customers have raised expectations based on simple sign-up experiences elsewhere. And as COVID-19 has curtailed our ability for face-to-face engagement, a remote option has become imperative for many organisations. Such streamlining usually aims to move the onboarding process to being completely online in nature, except perhaps in some cases where in-person contact is still necessary.



A major challenge in online onboarding is proving the identity of the person signing up. Often the proof-of-identity process relies on the presentation of documents assumed to be under the control of the person being signed up, such as a driver's licence or passport. With the understanding that there are bad actors who may attempt to sign up imposters comes the responsibility of the organisation to make the misuse of identities as difficult as possible. Jane Smith has a right to expect that reasonable steps will be taken to prevent bad actor Sarah White from signing up using Ms Smith's credentials.

The challenge, therefore, is being able to confirm with more confidence that the person signing up is the one whose identity is being used.

Biometric technology can be used for such confirmation as the technology measures distinctive physical or behavioural characteristics of a person. Two example use cases of digital onboarding using biometric data are:

- Signing up to a new banking service online, using a biometric passport or driver's licence to both tie the service to that person, ensure all banking services for the person are linked and there is no duplication of people
- Signing up to a new telecommunications service online, using a person's driver's licence to link the provided service to that person to satisfy regulatory requirements

Scope

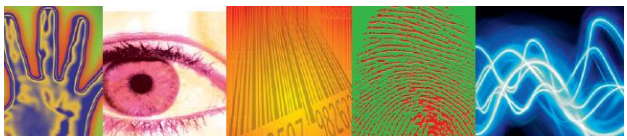
This paper sets out the Biometrics Institute's recommended good practices for digital onboarding in these remote, unsupervised scenarios. Other use cases are possible for biometrics both in onboarding and in digital identity more generally. These are not covered in this paper but may be the subject of future work by the institute. A partial exception is account recovery. Several issues that arise in design of account recovery processes are shared with onboarding, therefore, implementers of such processes may find aspects of this guidance useful.

This paper also does not address digital onboarding processes outside of the areas that intersect with biometrics and therefore does not by itself describe an end-to-end digital onboarding process. Many non-biometric steps are expected to occur both before and following the involvement of biometric processes in the onboarding journey.

It is important to remember that biometrics are based explicitly and entirely on distinctive physical attributes of a particular human being. For this reason, technology using biometrics is well suited to identity-related processes that are aligned with individual humans.

Conversely, where identity processes are not clearly aligned with individuals, biometrics may be an inappropriate technology choice. For instance, where a digital identity consists only of information about an account held by a household, biometric information would be unsuitable for inclusion in an onboarding process.

The remainder of this paper therefore is applicable to cases where a level of certainty is required that a sign-up process is associated with a specific person. Identities for corporations, for anonymous groups of people, and for sign-up processes where verifying identity is not paramount are all excluded from consideration.



Key considerations

Re-use: adopting an existing digital identity

An existing digital identity may be used to support onboarding in a different context. In general, such re-use is encouraged, in that re-using a satisfactory existing identity removes the need for the relatively complex identity proof process at the time of sign-up. Two models for this are described below with recommendations where relevant.

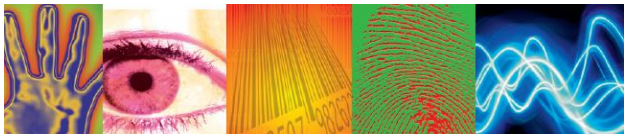
1. Model one: In some contexts a digital identity may be available from a trusted party which satisfies the requirements of the organisation, and integration of such identities may be possible from a legal, commercial and technical perspective. An example of this might be a digital identity managed by a central government, where the identities held satisfy the requirements of the organisation and are available for use. For some organisations, digital identities might be re-used from several other contexts, for example where several government jurisdictions are involved with disparate digital identity schemes.

2. Model two: Sometimes re-use of an existing identity is required. For instance where third parties may access customer data through a standardised mechanism designed to improve service portability or access to additional services. For example where a person called Jane Smith, who has a bank account with organisation BankCo, wishes to allow a third-party financial service organisation FinCo access to specific aspects of her account. Regulated access to customer information, in this example of an open banking system, allows organisations like FinCo to provide services to customers of organisations like BankCo. An example of this kind of use case is the mechanism designed into the banking Consumer Data Right in Australia [2], which enables fintech companies to offer additional services to customers of retail banks with a level of standardisation.

In either context the identity in question may be protected by a range of authentication mechanisms, including biometrics. Care should be taken to ensure that the security of the customer's sensitive data is not impaired through such re-use. This security risk could come from either the identity issuer, or from the third-party organisation. For example, imagine if BankCo allowed users to enrol in a well-implemented voice recognition system to protect their data, then the open banking mechanism mandates that all banks – including BankCo – have to allow fintech companies like FinCo access to BankCo's customer data. If the mechanism to access allows FinCo to just use a username and password – bypassing the biometric system our user enrolled into – the security of BankCo's customer data has been reduced.

Binding: attaching a digital identity to a person

The use of biometrics, implemented well, can provide relatively high-quality binding of digital to human identity. This process ensures that the person being onboarded owns the identity in question. The use of biometrics gives assurance that the person completing the digital onboarding process is the person they claim to be, by comparing biometric data from the person onboarding with biometric data from a trusted source. In one common use case, this means comparing a selfie – where the person signing up takes an image of themselves – with the image from a passport or driver's licence provided by the person onboarding as evidence of their identity.



The following issues should be considered when performing such a process.

1. **Use of biometrics to support onboarding should be administered to the same standard as any other biometric system.** This means addressing:
   - Governance
   - Privacy
   - Data security – both at rest and in transit
   - System access
   - Understanding and management of any algorithmic differentials or so-called bias
   - Ongoing performance management
   - Auditability
   - Testing of performance and efficacy

   The **Biometrics** Institute's *Good Practice Framework* is a guide to these issues and more to ensure all bases are covered in the planning, execution, and on-going operation of biometric systems.

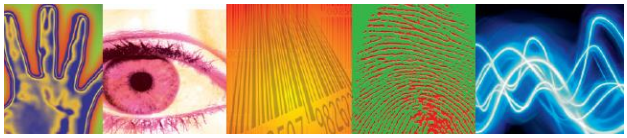
2. **Biometric usage should be based on known good quality, reliable data**. A particular issue in onboarding processes is ensuring that both the presented data from the person performing the signing up – for example a selfie of their face, and the data from the claimed identity – like a photo from a driver's licence, should not have been tampered with in any way. There are existing standards and industry testing bodies which address some aspects of these processes, but not all. A particular challenge is ensuring that the data from the claimed identity is of good quality and has not been manipulated. For example, passport images are often higher quality than driver's licence images, and relying on an image of a document supplied by the person signing up exposes the risk of document image manipulation through photoshopping or overlaying a new photo. Administrators managing data sources like the fingerprint or face image stores associated with passports or driver's licences have their part to play too in ensuring that data quality is satisfactory for biometric comparison.

Good Practice Framework grid reference: A.2.6, A.3.8, D.2.1, D.2.2, D.3.1, E.4.1

3. **The assurance level achievable through the use of biometrics varies**. Which biometric mode is chosen, the level of confidence in the data used and the technical measures implemented to protect against attacks on the system will all impact the outcome. For instance, a system capable of detecting the use of high-quality 3D masks may achieve a higher level of assurance than a system which performs a simple comparison between two images. Bodies like FIDO and NIST [3] publish acceptable performance levels in certain environments and jurisdictions. These should be used to determine acceptable concrete performance levels for the context you are working in. Performance to these levels should be independently tested for the system in-context to a recognised standard by an appropriately qualified body. Since biometric performance can vary widely across different contexts, error rates on pristine data sets are unlikely to be replicated in the real world.

Good Practice Framework grid reference: A.4, E.4.1, E.5.1, E.5.2

4. **Given the probabilistic nature of all biometric matching, errors must be considered and adequately planned for.** Errors to consider include both:
   - Mistaken matches (also known as false positives), where the machine mistakenly accepts an imposter, leading to polluted identity data



- Mistaken non-matches (also known as false negatives), where the machine mistakenly rejects someone who should have been accepted, leading to user experience issues, potential manual processing, and a reduction in successful onboarding events

User experience design around errors requires particular care given requirements for both procedural security and user convenience in the onboarding context.

Good Practice Framework grid reference: D.5.1

5. **Maximisation of user experience is related to biometric matching performance.** Poor matching performance will result in poor customer perceptions of usability. However, there are other non-performance-related dimensions to user experience and these too should be carefully considered. Users are more likely to successfully complete a biometric onboarding process if it is simple, clearly explained and reliable.

Good Practice Framework grid reference: E.2.2

Watchlists

Maintaining a biometric gallery of known fraudsters can be a useful mechanism for screening the opening of accounts, particularly where a fraudster could derive immediate financial benefit from fraudulently opening multiple accounts. For example, a fraudster could attempt to open multiple post-pay mobile phone accounts with the fraud only being discovered after they have taken possession of multiple handsets. The use of a biometric gallery or watchlist has the potential to limit the fraud to a single instance.

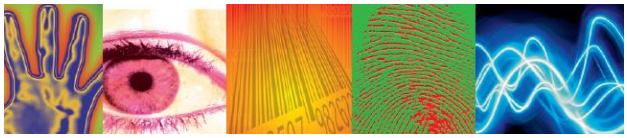
The gallery can be compiled from biometric data, such as face images, submitted during previous account opening processes that were at some point determined to be fraudulent. Checking presented biometric data against the gallery during the onboarding process can counter the way a skilled fraudster may learn, through successive attempts, how to break the account opening security mechanisms. As for other biometric uses during onboarding, care must be taken to ensure that biometric good practices are adhered to as outlined in the *Good Practice Framework*. Of particular note is determination of the closeness of matching required against the watchlist. If set too tight, many fraudsters will be missed. If set too loose, many legitimate onboarders will be mistaken for fraudsters.

Implementing such a watchlist must be done in compliance with local privacy laws and policy.

De-duplication: one digital identity per person

Where association of a digital identity with a person is desirable, circumstances arise where it is also desirable to ensure that each person is associated with one digital identity at most. The process to ensure unique representation of a person – and removing duplicates – is often called de-duplication.

Such uniqueness is not always necessary. It may be entirely reasonable for a person to hold multiple accounts with an organisation. Therefore, an initial decision must be made about the context in which the digital identity is to be used. For example a person may have multiple accounts for different telecommunication services with the same company. However, in a banking context it might be legislated



that all accounts held by a particular person are linked together under one umbrella. These questions then need to be considered:

- Does the use case preclude multiple digital identities?
- Is a single natural person entitled to hold more than one account or point of access?
- Even if the accounts are separate, is there a systemic need to know that they are used by the same natural person, even if the exposed identity is hidden or different?

If the answer is yes, consideration must be given to how to detect attempts, whether deliberate or accidental, to associate a person with multiple digital identities. Simple attempts, such as using the same government-issued identity document to enrol two digital identities may be easily detected through examination of underlying document data such as serial numbers and extracted data fields.

Biometrics may have a role in detecting more sophisticated duplication attempts, like those involving legal name changes. In such cases, biometrics should be considered as part of a system to perform such de-duplication, and not as a complete system in itself. In a one-to-many matching context, each onboarded person needs to be compared with many other digital identities to determine whether they are already present in the data. Because of the sheer volume of these comparisons, the statistical nature of biometric technology means that the outputs of such a system will almost certainly need to be combined with other factors to form a practical de-duplication mechanism. These other factors may range from checking biographic data, to advanced proprietary fraud detection technology. Systems designed to carry out de-duplication are only practical where a mechanism for cross-comparisons of enrolled biometric data is possible. Even if this is practical, it may be cost-prohibitive when compared against investment in other techniques for de-duplicating records.

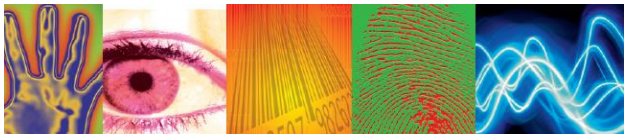
Where re-using an existing digital identity scheme – as encouraged earlier in this document – consideration should be given to whether the de-duplication efforts of the administrator of those identities is satisfactory for the organisation's intended purpose. Where a range of potential existing digital identity providers may supply an identity to the organisation, de-duplication across those providers may become a material issue if uniqueness is needed. For example if Jane Smith signs up for an account using a government-issued digital identity and another account using a private sector digital identity, the organisation needs a method for ascertaining whether the two accounts relate to one Jane Smith or two different Jane Smiths.

Good Practice Framework grid reference: A.3.4, D.4.3

Further use: authentication after onboarding

Also of note, but not covered in detail in this paper, is that biometrics can intersect with onboarding processes in the sense of capturing enrolment data to support future biometric authentication. Later authentication processes should be designed and implemented to ensure that the benefits of using biometrics in onboarding are not lost. For instance by only achieving a low standard of assurance for key transactions because of allowing simple password-only access to information.

As examples, biometrics can support authentication of the human against their digital identity during account logon and account recovery – the latter being a key avenue for account takeover fraud. The use of biometrics, if well implemented, can support higher levels of assurance for these processes than authentication relying on simple password controls alone [4].



Record-keeping: capturing the process used

Whatever model is used to onboard the new customer – whether re-using an existing identity from another provider, using biometrics to achieve a satisfactory proof of identity or some other mechanism – adequate records should be kept of the processes used and any key data pertinent to the operation. For example, records of the scoring data output by a biometric system for that onboarding event, the versions of the technology used – in the event that an upgrade generates an issue, or versions of the user experience – to track the impact of any changes. And were a future data breach or attack vector to become apparent in any of the mechanisms used to establish identity, it will be much easier to mitigate if the processes connected to the affected records are identifiable.

Conclusion

Biometrics can support digital onboarding processes by helping to verify that the right person is doing the onboarding. Using biometrics in this way should be undertaken with the same care and diligence that applies to any biometric system. Specific issues for digital onboarding include:

- Determining that the person whose biometric information is shown to the onboarding system is actually present at the time of onboarding
- Determining that the data against which the onboarding person is compared is itself trustworthy
- Ensuring user experience design of the overall onboarding system is clear to maximise the quality of data used, and to improve uptake
- Being mindful of the statistical nature of biometric technology in system design as a whole

Adhering to the recommended good practices in this document should improve performance of biometric digital onboarding services, and increase confidence in the identity of the people being onboarded. Failure to adhere to these practices is likely to impair overall system performance and user experience, and may result in a false sense of security through the use of biometrics in inappropriate ways.

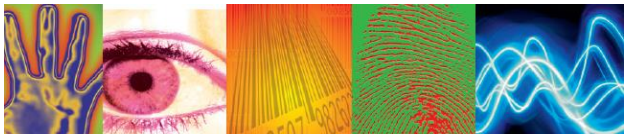
About the Biometrics Institute

The Biometrics Institute is the independent and impartial international membership organisation for biometric users and other interested parties. It was established in 2001 to promote the responsible use of biometrics and has offices in London and Sydney.

With more than a thousand members from 240 membership organisations spread across 30 countries, it represents a global and diverse multi-stakeholder community. This includes banks, airlines, government agencies, biometric experts, privacy experts, suppliers and academics.

The Biometrics Institute connects the global biometrics community. It shares knowledge with its members and key stakeholders and most importantly, develops good-practices and thought leadership for the responsible and ethical use of biometrics.

For more information, visit www.biometricsinstitute.org



References

[1] Biometrics Institute *Good Practice Framework*

The institute's framework for biometric systems encompassing all aspects of biometric system lifecycles

[2] Australian Consumer Data Right

[3] FIDO Alliance and National Institute of Standards and Testing (NIST)

[4] The NIST *Digital Identity Guidelines* 800-63, esp. 800-63A and 800-63B

Wide-ranging recommendations on digital identity including lifecycle model, guidance on authentication and identity assurance levels, and the role of biometrics

Further reading

Biometrics Institute spotlight on vulnerability including, Top 10 Vulnerability Questions, Biometrics Vulnerability Checklist and Presentation Attack and Liveness (members only)

Trusted Digital Identity Framework 13 policies including *Biometric Binding Requirements and Guidance*, Digital Transformation Agency, Australia

Recommendations regarding biometrics for identity proofing in the Australian context

How to prove and verify someone's identity Good Practice Guide 45, Cabinet Office and Government Digital Service, UK
Recommendations regarding identity proofing in the UK context

ISO/IEC 30107-3:2017 Biometric presentation attack detection, International Standards Organisation
International standard regarding the detection of presentation attacks against biometric systems

ISO/IEC 19795-1:2006: Information technology — Biometric performance testing and reporting — Part 1: Principles and framework, International Standards Organisation

Contact

Isabelle Moeller

Chief Executive, Biometrics Institute

isabelle@biometricsinstitute.org | +44 7887 414 887

Disclaimer

The Biometrics Institute provides guiding material as a tool to help its members conduct due diligence. While the institute has used reasonable care to ensure the accuracy of the material, due to the content and variable inputs during and after the process of implementing biometrics, the institute cannot be held accountable for outcomes or compliance. The material has been prepared for informational purposes only and is not intended to provide legal or compliance advice. Organisations should consult industry experts should they require advice on the technical, legal or compliance aspects of the material.

First released: March 2021