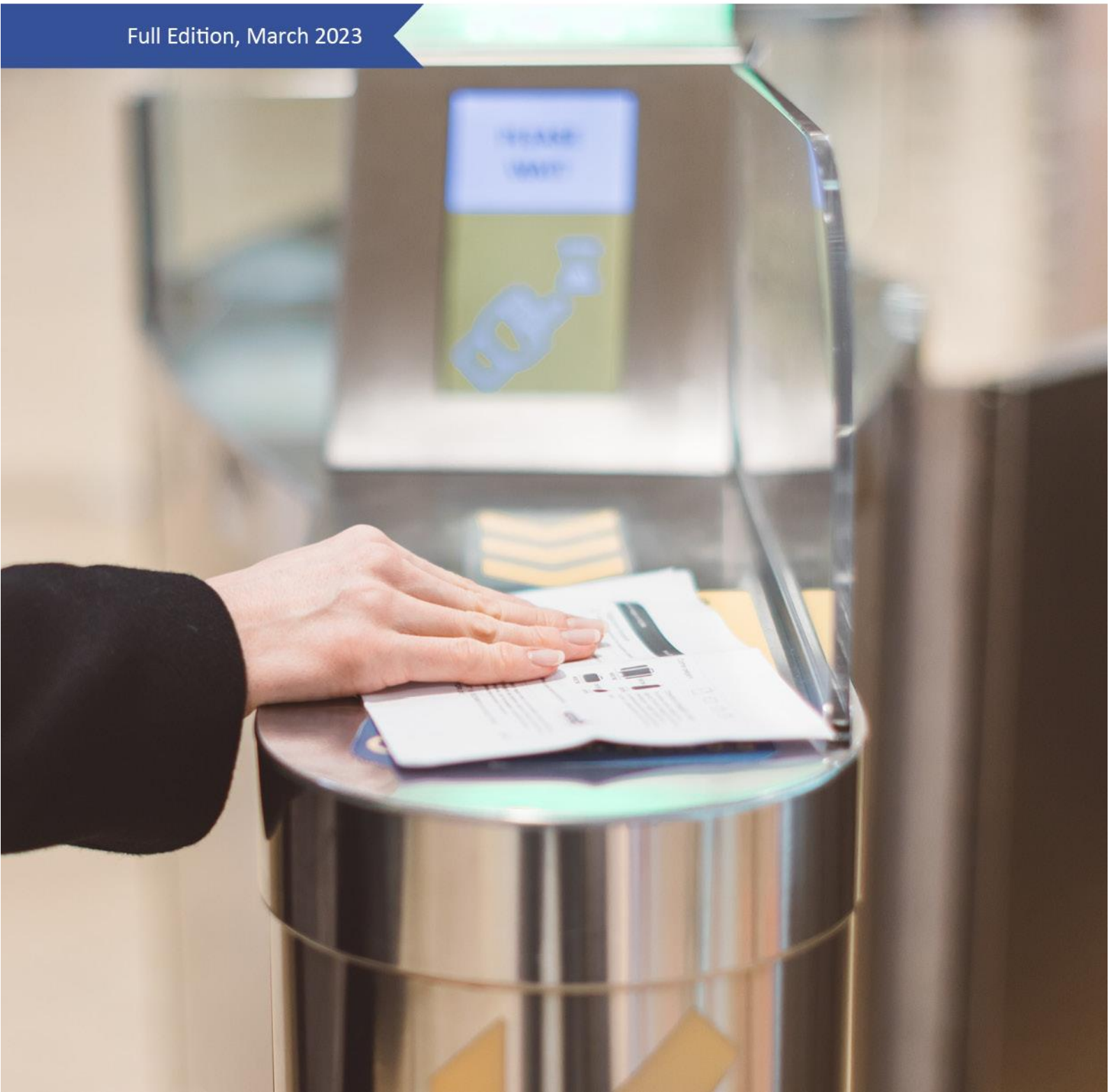
Digital Identity and Biometric Authentication

Making sure the right person
is using a digital identity

Full Edition, March 2023



Digital Identity and Biometric Authentication

Making sure the right person is using a digital identity

Whenever a digital identity is used to perform an action like requesting information or executing a transaction, it is invariably important to check that the correct person is using that identity. Many techniques are used to perform these checks including the use of biometric technology. This material provides guidance on recommended practices in the use of biometrics for this purpose.

The process of checking that the correct person is involved goes by different names in different fields but is often termed the 'authentication' or 'verification' of a digital identity. However, use of these terms is sadly complicated by their use to mean different things in other parts of the biometrics world. For consistency and clarity within this document, 'authentication' is used throughout.

Introduction

Governments and others have been developing plans for digital identity, digital trust frameworks and digital wallets [1, 4, 10] for several years as a way to regularise the access to, and delivery of, citizen services by digital means with many potential uses across both commercial and public sectors. There are also many examples of commercially developed digital access mechanisms in frequent consumer use that require confirmation that the right person is being granted access, for example, financial services. Several external factors have accelerated these plans and consumer uptake of digital identities, and the need to authenticate holders of those identities has accelerated too.

In many use cases, biometric technology can be used to ascertain that an interaction is with the right person. It should be considered in the context of the classic three pillars of identity verification: 'something you have', 'something you know', and 'something you are'.

> EXAMPLE: Australian Government Digital Identity
>
> When a *myGovID* is used to access higher risk or higher value services – such as obtaining a Tax File Number or receiving a government benefit from Centrelink – biometrics can be used to increase the confidence that the person using the digital identity is the legitimate holder.

This paper sets out the Biometrics Institute's recommended good practices for the use of biometrics in authenticating existing digital identities. As such, it aims to provide useful insight to readers considering either the creation of a new authentication process – or the reuse of an existing authentication process – to digitally confirm that a user is the right person as they go through a transaction or service usage process. The contents cover:

- Using biometrics to authenticate a user after they have signed up to an online service
- Reuse of an existing digital identity and impacts on biometric authentication
- Continuity of identity and the involvement of biometrics in maintaining this
- Guidance in identity recovery strategies where an error or breach has occurred or is suspected
- Making ethical and responsible decisions in biometric authentication applications, with reference to specific sections of the Biometrics Institute's *Good Practice Framework* [3].

Many of these issues are important to everyone considering the use of biometrics to authenticate digital identities, including those thinking about:

- On-device biometrics to verify high-frequency transactions, for example, payments
- Centralised biometric systems to verify secure transactions such as government services
- Designing their own authentication processes for use by customers
- Reuse of digital identities provided for or by another party (e.g., when designing for, or relying upon, an identity provider or digital trust framework, whether in a centralised, federated or distributed model)
- On-device biometrics to support confidence in self-sovereignty of identity and/or usage of a digital wallet.

Out of scope

This paper only addresses authentication processes related to areas that intersect with biometrics, and therefore does not by itself describe end-to-end digital authentication processes. Many non-biometric steps are expected to occur both before and following the involvement of biometric processes in the authentication journey.

For people seeking guidance on:

- Onboarding or creating new digital identities, see the Institute's *Digital Onboarding and Biometrics* [2], which provides similar good practice material to this paper for the onboarding process and using biometric technology when attaching a digital identity to a human identity.
- Reuse and interoperability between digital identities, consider the material both in this and the onboarding paper.Other use cases are possible for biometrics in digital identity more generally, including watchlists and continuous authentication. These are not covered in this paper but may be the subject of future work by the Institute, which welcomes feedback on demand for such guidance.

Where authentication fits

There are many points within the life of a digital identity where biometrics may be relevant. A summary of these points and the risks involved follows, to set the context for the guidance material herein:

- *Identity theft* occurs when someone attempts to create a new digital identity using someone else's real-world identity and is countered by using strong digital onboarding identity processes as covered in the Institute's *Digital Onboarding and Biometrics* [2].
- *Account takeover* involves a bad actor taking control of an existing digital identity, usually through being authenticated to perform a high-value transaction such as a change of physical address. This is countered using strong authentication processes that protect an already established account, especially for high-value transactions.
- *Account recovery* allows a defrauded person to retake control of their account, where an account takeover has occurred, despite the countermeasures in place. The same process may also be used if a trusted device (such as a mobile phone) is lost by the account holder. Because the account recovery process cannot rely upon the authentication mechanisms usually used, it presents significant security and user experience challenges. In some cases, the recovery mechanism may in effect be a re-onboarding – in which case the Institute's onboarding guidance [2] may be helpful.
- *Unauthorised usage* can occur in some digital identity contexts, usually through a bad actor performing some action or function that impersonates the holder of the digital identity but does not result in the bad actor taking complete control of the identity. This is usually countered using better authentication processes for high-frequency transactions, such as the use of biometrics for day-to-day payments.

Individuals: Biometrics and people

It is important to remember that biometrics are based explicitly and entirely on distinctive physical and/or behavioural 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, or may require further considerations for good outcomes. For instance, where a digital identity consists only of information about an account held by a household, biometric information may be unsuitable for inclusion in an authentication process. However, were information about the members of that household to be available, biometrics could be of value.

The remainder of this paper therefore is applicable to cases where a level of certainty is required that a digital identity is associated with a specific person. Identities for corporations, for anonymous groups of people, and for digital identities (and uses thereof) where verifying identity is not critical are all excluded from consideration.

Considerations when introducing biometrics

Biometrics is inevitably linked with other authentication mechanisms – whether pre-existing, or as part of a new service design; and some of these linkages are outlined in detail in later sections. The following key points should be kept in mind when considering introduction of a new biometric mechanism:

- Focus on business benefits
  The trade-off between the cost to implement biometric authentication and the risks mitigated for users by using biometrics when authenticating to a service needs thought, noting that the costs include the implementation of technology, registration of users, and lifecycle management – as well as other, non-technical elements; and the risks mitigated may well be extensive, especially for high-value transactions.
  In essence, this boils down to whether the costs to the organisation justify the benefits. [*Good Practice Framework* reference: A.1.1, D.1.2]
- Impact of biometrics on other mechanisms
  Careful attention to the impacts on other authentication mechanisms and their usage is therefore warranted, including whether these are still relevant if biometrics are available. [*Good Practice Framework* reference A.1.1, A.2.6]
- Differentiation between biometric and non-biometric mechanisms
  The trade-off between the security and convenience of biometrics versus that of other potential mechanisms (including for instance secret passwords and one-time codes) should be considered. Of note is that these benefits may vary across different groups of users. For instance, those with accessibility issues may, with good biometric design, find it easier to access certain services; and for those experiencing domestic conflict, partners are likely to know knowledge-based (i.e. non-biometric) authentication data information making control of their identity difficult for the fleeing party. In essence, this point boils down to whether the benefits to consumers are clear. [*Good Practice Framework* reference A.1.1, A.4.1, A.4.3]
- Use of biometrics to minimise uncommon negative events
  A desire to better handle events such as attempted account takeover and/or recovery influences both the selection of biometrics and places for their use. This may include:
    - Use of biometrics at intervals to strengthen confidence in identity continuity (i.e., the same person is in control of the digital identity, and when there is strong evidence of non-continuity, consider repeating the onboarding process (see also “continuous authentication” below);

- Use of biometrics upon the occurrence of specific events such as when an individual's identity has been the subject of a cyber security or fraud incident, when the user changes contact information, or when unusual activity is detected
- Use of (especially centrally held) biometrics to support moving the services associated with identity-breaking events from in-branch to remote delivery. [*Good Practice Framework* reference A.1.1, A.1.5]

Reuse of authentication

Where possible, reusing existing authentication mechanisms should be seriously considered. Such reuse comes from two broad types of use case:

- Reusing a digital identity provided by another party
  This might come from an interoperability or reuse agreement with another party (such as one government agreeing to trust the digital identities supplied by another); or from a mechanism such as a digital trust framework. As outlined in the Institute's guidance in *Digital Onboarding and Biometrics* [2], reusing an existing digital identity is often the easiest path to onboarding: many of the challenges may have already been solved by another party. Where this is possible, reuse of any associated authentication mechanisms may, too, represent an opportunity to reduce rework.
- Reusing existing authentication within an organisation
  This most commonly arises when one part of an organisation is authenticating customers, and another part needs a mechanism for authentication (such as when designing service delivery across different delivery channels like over-the-phone and in-app experiences).

Reuse of either type can deliver significant benefits. The need to authenticate can occur in several different contexts, service delivery channels, and transaction types – with multiple digital services, encompassing websites, apps, devices and so on. The ability to apply the same authentication processes can allow individuals to use a single means of authenticating themselves despite this complexity.

Especially when using biometrics within authentication processes, reuse can provide a range of benefits:

- Consistency of experience to customers, meaning on average faster experiences and greater user confidence where authentication is required
- Reduced cost due to not repeating work to design and build authentication processes
- Reduced user confusion, especially compared with pathological cases such as different parts of the same organisation having two different sets of biometric data of the same type held separately (for instance, two face recognition systems working from different data)
- Ability to better tune performance characteristics due to larger volumes. Combined with the point above – ultimately reusability drives economies of scale
- Moving beyond insecure passwords, shared secrets, Knowledge-Based Authentication (KBA) and One-Time PINs becomes easier and thus more consistently implemented across an organisation
- Removal of replication of customer data (especially biometric templates) across an organisation
- Where biometrics enables service types in digital channels that might otherwise be limited to face-to-face channels, consistency of biometric authentication across channels can also assist with transitioning customers from a face-to-face traditional identity to a digital identity.

ILLUSTRATIVE EXAMPLE: Telecommunications

For a typical telecommunications provider there are several different channels in which a customer might need to authenticate: retail (in-store), online, webchat, customer support and others. Being able to reuse authentication processes across these contexts – whether internal or from a partner –enables consistency of experience and standardisation of the approach to authentication.

For these reasons, authentication design should:

- Consider whether reuse of existing authentication can achieve the desired objectives; and
- Where this is not possible, new authentication design should consider future reuse.

For these considerations, both the scope of the digital identity under consideration, and current or potential future uses (for example, sharing an authentication process with a partner or aligned organisation), should be contemplated. [*Good Practice Framework* reference A.1.6, A.3.8]

The standard of the authentication mechanism being reused is of course crucial; and the remaining considerations herein should be applied in considering suitability for reuse.

Relationship with other authentication mechanisms

Often several different mechanisms are available to authenticate a digital identity. This can be due to:

- Characteristics of the specific service delivery mechanism
  (e.g., an app experience may require a PIN and optionally offer on-device biometrics)
- Differences between service delivery mechanisms
  (e.g., face recognition might be offered in-app but not over the phone)
- Differences in the involvement of supporting personnel
  (e.g., some processes may be supervised by staff but others might be unattended)
- Differences between the level of authentication required for particular types of service
  (e.g., low / medium / high security) See also 'Authenticator Assurance Level'

ILLUSTRATIVE EXAMPLE: Variability of authentication levels in banking, government

In a consumer banking relationship, access to account balances and payments up to a nominated value might be provided to a low security level by on-device biometrics (like Apple's *FaceID*), but access to critical services such as alteration of key account data or high-value transactions might require high security authentication using bank-controlled biometric information. Similarly, in a government relationship, access to personally identifiable information might necessitate usage of additional biometric security.

As illustrated in the example, the available authentication mechanisms may use different biometrics.

In addition to this, for any given mechanism, biometrics may be used in conjunction with other 'factors' to improve outcomes for individual authentications; and the need for such combinations should be carefully thought through. Examples of such combinations with other factors include:

- Overt biometric modes
  (for instance, using both on-device face recognition as well as centralised voice biometrics to verify an app-initiated high-value banking transaction)

- Covert biometric modes
  (for instance, using keyboard behavioural biometrics in conjunction with centralised voice biometrics to verify a computer-initiated high-value banking transaction)
- Behavioural biometrics to inform risk decisions
  (for instance, using user input behaviour as an indicator of whether additional security should be applied to this interaction or transaction)
- Non-biometric factors
  (for instance, possession of a particular token or device in conjunction with centralised face biometrics to verify a mobile-initiated high-value banking transaction)

[*Good Practice Framework* reference A.1.4, A.4.3, D.1.3, D.4.3]

Given that multiple means of authentication may use biometrics, and different biometrics may be used in different ways within them, there may be several places in which the biometric guidance in this document should be applied when designing authentication.

Potential for biometrics to be impaired by other authentication methods

Where choice is offered to those authenticating, care should be taken to assess the relative security of the alternatives to biometric authentication. There is little point designing a highly secure biometric authentication mechanism that can be ignored by the user (especially a nefarious one) in favour of an insecure 'known biographic data' authentication mechanism. [*Good Practice Framework* reference D.2.2]

Potential for biometrics to impair other authentication methods

Where consumers can choose how to authenticate, the convenience of biometrics as a mechanism often leads people towards extensive usage – sometimes, to the exclusion of the other available mechanisms. This can mean that people forget their other authentication information (such as passwords), and when trying to use service channels that do not support biometrics, they are unable to authenticate. Often this leads to complex escalation being required for service types that are not possible in the channels that do support biometrics.

> ILLUSTRATIVE EXAMPLE: Telecommunications company SIM swap
>
> Customers of a telecommunications company (telco) become accustomed to getting service through a new app using on-device biometrics to authenticate. Some then forget the password they created to login by phone. But if they need to replace their SIM – a high-risk transaction – the telco requires this to be requested over the phone and does not permit on-device biometric authentication. With no password, their authentication experience is likely to be complex and inconsistent with the simplicity of the biometric experience they use.

Selecting biometrics

A range of factors influence choice of biometrics to use in digital identity authentication, and this selection is entwined with the places in which authentication should be used. In other words, the question of 'where' influences 'what type', and vice versa.

The Biometrics Institute provides a range of general guidance information that may assist including the overview of *Types of Biometrics* on its website [5]. The sections below cover specific guidance for selection for authenticating digital identities.

Requirements to consider

- Ways in which the digital identity will be used and authenticated
  Multiple service channels are common in digital identity (for example, website; mobile app; phone); and the selection and effective use of biometrics depends on which service channels are relevant, both currently and in the reasonably foreseeable future.
  For some channels there are biometrics that are easier to use than others – voice for over-the-phone service; on-device for app experiences – and for others, out-of-channel authentication using biometrics may also be possible. [*Good Practice Framework* reference A.1.4, A.2.1, A.2.6]
- Technical capabilities available to customers
  The suitability of specific biometrics is closely aligned with user needs and capabilities to interact with the intended mechanism. It may be financially infeasible, for example, for an organisation to implement a face biometric system that uses visual cues to the user if a large proportion of their users are visually impaired. [*Good Practice Framework* reference B.1.4]
- Necessity for remote capture
  The availability of remote readers for the biometric mode in question is a key factor: for digital identity authentication, most use cases are remote and rely on user-provided equipment.
  If relying on camera hardware (for example, in mobile phones), are there any devices with cameras of insufficient quality or trustworthiness in capture to exclude them from use? If so, do these represent an acceptably small portion of the intended users? [*Good Practice Framework* reference A.2.1, A.2.6, D.2.1]
- Continuous authentication throughout engagement
  For some use cases, it can be beneficial to get information on whether it's the same person continuing to engage as a transaction is performed.
  If this is desirable, some modes are better suited than others (for example, voice information is provided throughout interactions over the phone; continuous video is needed during a transaction for face). [*Good Practice Framework* reference A.1.3, A.2.6, B.4.4]
  The Institute may consider producing material on best practices for continuous authentication using biometrics in future.
- Levels of convenience and security required
  Biometrics provide the potential for stronger and more convenient authentication. Where security requirements are not paramount, biometrics might be implemented by adding a native on-device biometric such as *FaceID* on an Apple device, in place of a PIN. This is often used where an increase in convenience is the primary objective – such as in day-to-day payments in retail banking.
  Stronger authentication is usually achieved using biometrics that are in some way controlled by the organisation holding the digital identity, whether centrally held or in an agreed federation model. This is partly due to the challenges of using on-device biometrics outlined in later sections, and partly due to challenges in ensuring the right level of identity assurance for the biometric enrolment process. Organisationally managed biometrics can be used for authenticating during an account recovery process, and because they can survive the loss of other credentials, they can also aid in the event of loss of a mobile phone and its built-in biometric credentials.
- Suitability for mid-engagement step-up
  Sometimes customers attempt a low security transaction then, later in the same interaction, perform a higher security transaction. This may mean that an increase in authentication confidence is required at the point the higher security transaction is requested.
  Some types of biometrics may be more suited than others for such a mid-engagement step-up of security levels. For example, in an over the phone transaction some biometric modes may be easiest to use if performed before any conversation occurs between customer and representative. The impacts of any mode choices taken on user interface and experience design should be considered.

Key controls and issues

The use of biometrics for authentication should be planned and implemented with the same care as for any other biometric system: there is a wide range of guidance from the Institute and other sources on this subject. The selection of key controls presented below reflects issues that often arise in this specific usage of biometrics.

It should be kept in mind that when reusing biometric authentication – whether from:

- Another department
- The digital identity system of a trusted partner
- Manufacturers of electronic devices such as smartphones, or
- A mechanism such as a Digital Trust Framework or FIDO

that operators should be aware of the risks associated with such reuse from another party especially in these areas, and to appropriately control for them. In this reuse scenario, these issues can be particularly thorny.

The following considerations are split into three sections for readability: those relating to functionality, performance and control.

Functionality considerations

- Mitigations for known vulnerabilities
  Most biometrics have existing, known vulnerabilities to attack; and mitigations of various kinds for these vulnerabilities are available (such as 'liveness' detection of varying types). The vulnerabilities protected against, how this protection is implemented, and the impacts on the user's experience resulting from the mitigation, especially in high-frequency contexts, should be understood. [*Good Practice Framework* reference D.2.1]
- Protection of biometric data
  The larger the pool of biometric data stored in one place, the more appealing it becomes as an attack target for bad actors. Therefore, consideration should be given to whether a centralised, federated, or user-held model is best for storage of this data – noting the intersection with other challenges such as recovery if users lose their devices.
  Good practice is that personally identifiable attributes – including biometrics – should be protected by appropriate privacy mechanisms. In centralised or federated models, an example of such a mechanism is the notion of 'zero-knowledge proofs'.
  Some frameworks such as FIDO [4] attempt to minimise the centralised risk by making user-held identity widely usable while also retaining biometric data on user devices.
  Whatever the mechanism, controls over data security should be carefully considered if others hold the data – as is the case when reusing biometric authentication.
- Maintenance of up-to-date biometric data
  Some biometric data changes over time in humans – for example, the face ages; the voice deepens at certain points – and so many biometric systems perform better when biometric templates are updated as these aging processes occur. Ensuring that any such updates are applied to the correct template is key, implying too that trust is needed in processes for this when provided by others. Where authentication is reused, an opportunity exists to keep templates more up to date than they would otherwise be, through the greater usage each template receives.

Performance considerations

- Published sensor and system performance
  Does the providing party publish expected performance figures or how their sensors or systems are

resistant to biometric attacks? If not, there is an unknown level of risk associated with accepting these capabilities.

- Variation of performance across devices
  Do all variants of sensor type provide identical performance? For example, there are notable differences in the sensor hardware between flagship phones and midrange phones, leading to differing levels of trust. This forces the builder of the digital identity application to view the overall risk as being determined by the lowest performance devices allowed to participate in the ecosystem.
- Independent validation of performance
  Independently validation of claimed performance characteristics to ensure that the achieved performance and functionality of biometric comparisons and vulnerability mitigation methods in context matches what is specified. In the case of on-device biometrics, there is often little (or no) third-party validation of native capabilities by biometrics testing labs. [*Good Practice Framework* reference E.2.1, E.4.1, E.5.2]
- Achievable performance envelope
  Obviously technical performance of a particular biometric is important: it determines the confidence that can be derived from the outcomes and, to some extent, the consistency and perceived quality of the user's experience. Performance data used to determine the trade-offs between performance, convenience and spoofing possibilities should ideally come from use cases as close in parameters to the contemplated use as possible. [*Good Practice Framework* reference A.4.1, A.4.3, B.4.1, E.1.1]
- Changes in performance over time
  Two conflicting performance effects can occur in biometrics for authentication, related to the scale of many authentication use cases and the frequency with which individual people authenticate. When reusing biometric authentication from other parties, the extent to which these two effects occur is likely to be impacted by other usage of the same authentication mechanism.
    - Users can become more accustomed to using the biometric system over time, driving up performance. Where this effect dominates, initial performance may underestimate long-term business benefit.
    - Users can vary their presentation of (especially behavioural) biometrics over time, driving down performance. This is most commonly observed where initial baseline 'enrolment' data is gathered in an environment dissimilar to the eventual use when authenticating (for instance, if users are presented comprehensive instructions at enrolment, but are left to their own devices at the time of authentication). Where this effect dominates, initial performance may overestimate long-term business benefit.

Control considerations

- General biometric 'good practice'
  There are a range of well-known good practices for biometrics systems that are as applicable to authentication for digital identities as they are to other biometric uses. While the Institute's *Good Practice Framework* [3] should be consulted for broader guidance, some key points to consider are:
    - Appropriate consideration of privacy impacts including performing a Privacy Impact Assessment [*Good Practice Framework reference* C.1.4 and the Institute's *Privacy Guidelines* [8] and *Privacy Awareness Checklist* [9]
    - The method used to take the user's live biometric sample for the biometric claim [*Good Practice Framework* referenceA.2.1]
    - The mechanism used to compare the biometric claim sample against the biometric reference [*Good Practice Framework* reference A.3]
    - How the relying party gets access to the comparison result [*Good Practice Framework* reference A.3.8, C.3.3]
    - The mechanism in place to ensure the relying party can trust the source of data for both the biometric claim sample and the biometric reference, and by extension the authentication result [*Good Practice Framework* reference D.1.1]

    - The mechanism in place to ensure the relying party can trust the carriage of data for both the biometric claim sample and the biometric reference (normally done by cryptographic methods). [*Good Practice Framework* reference D.3.1]
- Correcting issues such as future vulnerabilities
  When vulnerabilities in biometric systems are uncovered – as they likely will, over the lifetime of the system – having resources, mechanisms, and responses in place to allow timely corrective action are important. If reusing, does the providing party offer guarantees about corrective actions if vulnerabilities are reported? If not, a relying digital identity operator may have little opportunity to take correcting action. Where correcting action is possible, it may involve removal of access for all parties using that authentication type (and, in turn, this may affect many more users than those affected by the original vulnerability).
- Control over matching parameters
  This is usually relatively uncomplicated when operating the biometric matching processes internally. But when reusing matching from elsewhere, does the providing party control all aspects of biometric matching that affect performance, to the exclusion of user controls? Some device manufacturers allow end users to adjust settings to make biometric authentication more user friendly (and thus less secure), creating unknown risk regarding reliance on them.
- Selection of security/convenience trade-off point
  Again this is relatively uncomplicated when operating internally (notwithstanding that the relevant performance testing must be performed to determine what trade-off points are possible). When reusing matching from elsewhere, can you adjust this trade-off? If not, does the providing party's target trade-off between user experience and security match your organisation's objectives? Device manufacturers often prioritise user experience over security, which may not be consistent with the desired authentic cation outcomes.
- Iterative nature of digital processes
  The iterative nature of improvement cycles for all digital processes means that the potential for future enhancement and refinement should be kept in mind. It is unusual that first attempts at design and implementation of biometric enrolment and verification processes for authentication are unable to be improved upon; therefore, future amendment should be considered.
- Record-keeping: capturing the process used
  Wherever biometrics is used as part of the authentication process – including at enrolment – 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 authentication 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 authenticate identities, it will be much easier to mitigate and recover if the processes connected to the affected transactions are identifiable. [*Good Practice Framework* reference C.1.6, C.1.7, C.4.1]

In summary – appropriate governance and agreements about functionality, performance, controls and service levels are important compensating factors if the underlying biometric technology is not under the application developer's control. Conversely, appropriate resources are required to adequately operate biometric systems if they are under the developer's control. [*Good Practice Framework* reference A.1.5, A.3.1, A.3.8, A.4.3, B.4.1, C.1.7, D.4.1 along with the Institute's *Biometrics Vulnerability Checklist* [6] and *Top 10 Vulnerability Questions* [7]]

Enrolment: obtaining baseline data on biometric features

Use of biometrics in authentication depends upon having trusted baseline biometric data about the individual to be authenticated – what is termed the 'biometric reference' by ISO, and which forms the foundation for what is often called a biometric 'template'. Obtaining such data is therefore a key factor for the success of biometric authentication; and therefore maximising user experience to maximise enrolment

rates is often a key determiner of overall success of the implementation of biometrics for authentication. [*Good Practice Framework* reference A.2.6]

Continuity of person

It is important to ensure that the trusted baseline data is indeed from the correct person. [*Good Practice Framework* reference D.2.2, D.3.1] This data may be obtained in different ways and times, which result in different issues to address:

- During an onboarding process
  In this case, a key issue is designing the onboarding process to ensure that the trusted baseline data is taken from the same person that was bound to the digital identity. This might include sequencing relevant parts of the onboarding process to minimise the possibility of another person's biometrics being enrolled; or use of data from trusted documents from the onboarding process (for example, using the image from a passport as the face for future comparison). See the Institute's guidance on digital onboarding for more details. [2]
- At a later point, after initial creation/onboarding
  (For instance, where a set of existing users has the option of biometric authentication added)
  In such cases ensuring that the correct person is the one being enrolled is often more complex than when performed during onboarding. Design of the process needs extra care to verify the identity of the person enrolling – some organisations effectively redo the identity proofing performed at onboarding (for example, rechecking faces); some require a very high standard of (usually non-biometric) authentication within the enrolment process; and some resort to external service channels to increase confidence (for example, sending a physical letter containing a one-time code to a known address).
- From another party or department, as part of identity or authentication reuse
  In this case, the level of confidence in that party's processes is of course paramount. Two notable such cases are:
    - The use of on-device biometrics for authentication: in this circumstance, the confidence which can be taken from the on-device biometric enrolment and consequences if it is not correct should be carefully thought through.
    - The use of a framework such as FIDO [4] for authentication, in which case trust in the framework and ability to link to the digital identities controlled is key.

Transition of populations and remaining non-enrolled users

A service provider does not need their entire population to transit to the use of biometrics in one go, and this is of special significance when enrolment occurs after onboarding. Service providers typically offer biometric authentication as an option, using marketing to target digital adopters and then other cohorts with a goal of transitioning the customer base towards the new mechanism. Despite this marketing, some people may never be enrolled. (For instance, they may decline to enrol; or enrolment may only be offered in a service channel they rarely use).

Wherever such a gradual transition occurs, the set of non-enrolled users will decline as the enrolled user base expands. These non-enrolled users, and the authentication processes available to and required of them, should not be forgotten. As the use of biometrics expands in a user base, this may lead to the presented volume of fraud being concentrated on the non-enrolled users. Once this set of users becomes small enough, previously satisfactory protections against fraudulent authentication may become inappropriate in the face of the volume of attempts per user. For this reason, security mechanisms for authentication may need to be boosted for this remaining cohort of non-enrolees. [*Good Practice Framework* reference A.1.1, A.2.2, A.3.1]

Identity assurance levels

Whether biometrics are relevant usually depends on confidence in the underlying digital identity: high security verification in later authentication processes may be irrelevant if the original creation of the digital identity wasn't very secure. (This confidence in the creation process is sometimes described more formally as an 'Identity Assurance Level' (IAL) as outlined in Notes on terminology below; an identity with a low IAL might not be appropriate for biometric enrolment.) [*Good Practice Framework* reference A.2.5, D.3.1]

In other words, there may well be little point being supremely confident about authenticating an essentially unknown person. However, there are some use cases where this may be valuable – perhaps where repeat users of a service must be authenticated yet anonymous.

Sometimes a person will seek to enrol biometric data for a low-confidence digital identity – perhaps because they are aware that a wider range of services can be delivered to them if they enrol. This is usually handled by increasing the confidence in the previously established digital identity – i.e., its identity assurance level. A consequence of this is that enrolment processes should be designed in such a way that these uplifts in identity confidence can occur if needed.

Deduplication

Some users of biometric authentication seek to use centrally held enrolment data to deduplicate enrolled users. Detailed remarks on mechanisms of this nature are outside the scope of this document, except to note the overlap with deduplication of digital identities themselves which is briefly covered in *Digital Onboarding and Biometrics* [2]. The overlap, and any consequence and benefits resulting from it, should be considered as part of any enrolment de-duplication. [*Good Practice Framework* reference A.1.5, A.3.4]

Conclusion

Biometric technology has a great array of uses in authentication of digital identities. Chief issues to consider include:

- The use of biometrics is not a 'bolt-on' to authentication. Rather, it is entwined with authentication processes over the life of a digital identity.
- Reuse of authentication is often easier than building your own, especially in the long term.
- However, users of authentication provided by other parties should be aware of the risks and reliance they will have to manage.
- Relying on on-device biometrics has additional challenges, especially for highly secure usage across broad populations.
- As the use of biometrics expands across a set of users, the remaining non-biometric users sometimes experience increased fraud.
- Like all uses of biometrics, good practices are important, such as: clarity and transparency of purpose and scope; privacy considerations; user experience; and the maintenance of quality outcomes over time.

Notes on terminology

Authentication versus verification

This paper discusses processes that use biometrics to confirm that the correct person is granted access to a service using a digital mechanism (for example, online portal, digital wallet). The terms 'authentication' and 'verification' are sometimes used interchangeably as names for this process, but as noted in the opening section, this paper will adopt common commercial usage of 'authentication'.

Identity Assurance Level

Often abbreviated to 'IAL', this refers to the level of assurance achieved when a digital identity is created or onboarded. Roughly speaking, 'how confident we are that the digital identity we are creating is associated with the correct person?' A precise definition is available from NIST [10].

Authenticator Assurance Level

Often abbreviated to 'AAL', this refers to the level of assurance achieved when confirming that a digital identity is being used by the correct person – i.e., the one who created the digital identity. Roughly speaking, 'how confident are we that the person presenting a digital identity is the same person who created it?' A precise definition is available from NIST [10].

References

[1] Global Government Forum *Principles for the Future of Digital ID* (article)
Article outlining a group of eight countries defining principles for digital identity.

[2] Biometrics Institute *Digital Onboarding and Biometrics* (members only)
The companion paper to this document, outlining recommended practices for the use of biometrics in onboarding processes for digital identities

[3] Biometrics Institute *Good Practice Framework* (members only)
The institute's framework for biometric systems encompassing all aspects of biometric system lifecycles

[4] FIDO Alliance
Provides specifications for a specific, fairly widely used, on-device digital authentication protocol

[5] Biometrics Institute *Types of Biometrics*
Provides a high-level overview of the various different biometric modes

[6] Biometrics Institute *Biometrics Vulnerability Checklist* (members only)
Provides a simple list of important aspects to consider regarding biometric vulnerabilities

[7] Biometrics Institute *Top 10 Vulnerability Questions* (members only)
Outlines key questions and issues relating to vulnerabilities in biometrics

[8] Biometrics Institute *Privacy Guidelines* (members only)
Outlines key principles and issues relating to biometrics and privacy

[9] Biometrics Institute *Privacy Awareness Checklist* (members only)
Provides a summary checklist to help understand the extent to which privacy has been considered

[10] 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 (members only)

OIX *Guide to Trust Frameworks*
Guidance describing key elements of trusted digital identity frameworks

Trusted Digital Identity Framework including *Role Requirements*, Digital Transformation Agency, Australia
13 policies including recommendations regarding biometrics for authentication in the Australian context

Requirements for secure delivery of online public services GPG 43; *Using authenticators to protect an online service* GPG 44, Cabinet Office and Government Digital Service, UK
Recommendations regarding securing digital services and selection of authenticators 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 2023