UBISECURE®

Connecting Identity.
Transforming Digital Business.

Best Practices to Secure your Application with Biometric Authentication

Ramp up customer experience and security with identification of users' unique physical features

What are biometrics?

Biometrics have had a huge impact on digital identity. Whilst identity had traditionally been verified by 'something you know' (such as a password) and increasingly 'something you have' (for example, a FIDO authenticator), biometrics enable security with 'something you are' (like fingerprint or facial recognition).

Biometric authentication automatically matches unique physical features to verify that a user is authorised to access a service. Note that this differs from biometric surveillance which matches unique physical features to identify individuals in a database, such as public space facial recognition for policing.

Let's look at why biometrics are so popular, important considerations when planning to offer biometric authentication to users, and best practices for how to integrate biometrics to your application.

Why biometrics?

Why do service providers decide to offer biometrics as an authentication method, and why do their users respond so positively?

SECURITY

Biometrics are difficult to forge. Whilst passwords can be guessed or stolen (**80%** of data breaches are caused by stolen, weak or default passwords), biometrics stay with the user so it's much more difficult for hackers to gain access on this basis.

Biometrics can either replace passwords or add an additional authentication factor on top of passwords (multifactor authentication – 'MFA'), which is even more secure as hackers would have to replicate two sets of credentials to gain unauthorised access. Biometrics can also be used together with another factor (not a password) for MFA, such as users logging in to your service with their bank ID (concept known as Bring Your Own Identity – BYOI) plus fingerprint recognition.

To summarise:

Biometric authentication	Secure, better than easily compromised password authentication
Password + biometric authentication (MFA)	More secure due to benefits of MFA
Biometric authentication + another form factor (such as bank ID) (MFA)	Even more secure, due to eliminating issues with passwords and benefiting from MFA

CUSTOMER EXPERIENCE

Whenever you're talking about digital security it's important to also talk about customer experience, as the key to your app's success is finding the correct balance between the two. Users want an easy journey through your service, but they also want to know that you're keeping their data safe.

> Users want an easy journey through your service, but they also want to know that you're keeping their data safe.

While biometrics can enable robust security, a clear benefit of biometric authentication is also the incredibly fast and convenient user experience. Considering how many login credentials users are expected to remember for various services these days, replacing that necessity with a quick scan of a physical feature is much more attractive and means users are more likely to sign into your service on a regular basis. This represents a significant competitive advantage, as when faced with obstacles to app access many users will simply give up or turn to competitors.

Some biometrics can also provide contactless authentication, enabling reduced contact with shared surfaces, which is now a widely recognised hygiene benefit given the COVID19 pandemic.

They can also be an accessible identity solution, such as for people with disabilities (replacing the need for keyboard-based credential input) or children (who may struggle to understand the concept of other authentication factors). See more on ensuring accessibility later on – 'Authentication options'.

OPERATIONAL EFFICIENCY

Resetting forgotten passwords is a duty heavy operation for customer service or IT departments, depending on where the responsibility falls. According to Forrester, large organisations spend up to **$1 million** each year in staffing and infrastructure expenses to handle password resets.

However, users won't forget or lose their own biometrics. Therefore, biometric authentication helps to cut down on this resource-consuming operational task, enabling significant cost savings.

Getting biometrics right

We've seen why biometrics are so popular among service providers and their users, but it's also very important to get biometrics right. Getting biometrics wrong could lead to sensitive information being leaked or access to your service being hindered; getting biometrics right means trust in, and loyalty to, your brand.

> Getting biometrics right means trust in, and loyalty to, your brand.

WHEN CHOOSING YOUR PROVIDER, ASK ABOUT:

— ANTI-SPOOFING (LIVENESS DETECTION)

A common question around biometric authentication is whether it would work by holding up a photo of the user to fraudulently represent their physical attributes.

Ensure that your chosen biometrics provider has mitigated against this potential issue and built in anti-spoofing technology (aka 'liveness detection') to their solution. This ensures that the user is in fact a real human, with various movement and light reflection principles, and is used by most modern biometrics providers.

— ACCURACY

Check what the success rate of their biometric technology's algorithm is, as different biometric technologies have different success rates in matching users to their biometric attributes correctly.

The biometrics technology providers that you'll want to work with will be aware of potential issues with, for example, bias in their algorithms (such as recognition success rate being skewed towards a certain race or gender) and be working continuously to reduce that risk.

— DATA STORAGE

Another common question around biometrics is the potential for theft of biometric data – wouldn't it be awful if your fingerprint was stolen? Fortunately, most biometric solutions never touch actual biometric data; instead they rely on a combination of local (device) processing and hashing to authenticate the user without needing to store or transmit sensitive data.

> Biometrics rely on a combination of local (device) processing and hashing to authenticate the user without needing to store or transmit sensitive data.

WHAT YOU NEED TO ENSURE

— AUTHENTICATION OPTIONS

It's important to offer users options for authentication, and not just enforce one biometric (or other) method. Consider your entire user base, particularly if you have a wide audience (such as a government service) to ensure it is accessible for all users. As mentioned earlier, biometrics will help some users with disabilities, but no one form will be universally appropriate.

You will also need to have secure backup options for biometric authentication in case the situation makes it impossible to conduct. For example, facial recognition may work well in most settings but if the user is wearing a face mask then they may need another way to authenticate without removing it (although facial recognition is now evolving to recognise people with masks).

— REGULATORY COMPLIANCE

Compliance to data and Know Your Customer (KYC) regulations will depend on your location(s) and industry, but a lot of these requirements also represent best practice anyway when it comes to digital identity. For example, it's important to clearly provide users with details about why, how and where your company is collecting and storing biometric (and other) data, building trust and assuring people that their data is being processed securely.

ENSURING SECURITY AND USABILITY BEYOND BIOMETRICS

While biometrics may be a key step on your plan for complete app security and customer experience, also take into consideration other security and usability-enhancing identity capabilities, such as:

- single sign-on (SSO) – removes the need for multiple login credentials for multiple services (explainer video **here**)
- Delegated Authority – enabling users to delegate the right to use digital services on their behalf (explainer video **here**)

These capabilities, including biometric authentication, are easily implemented with a customer identity and access management (**CIAM**) solution.

Biometric authentication options

There are many options for biometric authentication and your choice of provider(s) will depend on the kind of service you provide and your expected user demographics.

One consideration may be with or without specialised hardware (like a fingerprint reader). Whilst most apps are trending towards options that do not require specialised hardware and instead make use of built-in smartphone cameras or readers, certain in-office/branch service providers may prefer to rely on internally-maintained hardware.

Another consideration may be physiological (recognition of physical trait) or behavioural (e.g. mouse movement pattern) biometrics. Physiological biometrics may provide more accurate results, but behavioural biometrics may be harder to reproduce fraudulently as systems get to know a user more in depth over time. Therefore, physiological biometrics may be better suited to an occasionally used app, whereas a frequently used app may make better use of behavioural biometrics.

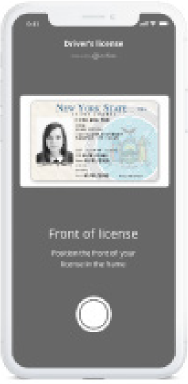
EXAMPLES

Spotlight on two of Ubisecure's biometric technology partners.

— ONFIDO IDENTITY VERIFICATION

Onfido technology assesses whether a user's government-issued ID is genuine or fraudulent, and then compares it against their facial biometrics. The simple process reduces the friction associated with identity verification processes during registration or KYC processes, and can make biometric based login fast, easy and secure.

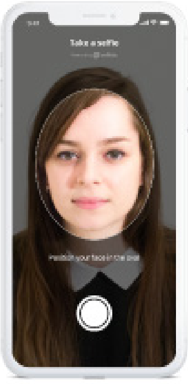
Document Verification



Front of license

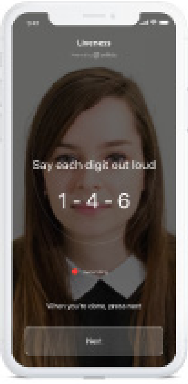
Position the front of your license in the frame

Facial Verification



Position your face in the oval

Liveness Verification



Say each digit out loud

1 - 4 - 6

When you're done, press next

— HITACHI FINGER VEIN RECOGNITION

Based on the patterns of veins in one's finger or hand, vascular pattern recognition (VPR) provides the ease of use of hand geometry with much improved accuracy, smaller readers and contactless use. Hitachi's finger vein system, VeinID Five, scans the veins in one's fingers and then matches the vein patterns of their respective pre-established templates.

Integrating biometrics

We've seen in this guide that, when implemented correctly for your individual service, biometric authentication can enable secure, customer-friendly and efficient digital identity experiences.

So how do you integrate biometrics into your application? If you know what you want, you can go directly to biometric solution providers who will likely use customer identity and access management (CIAM) partners, like Ubisecure, to deploy the necessary functionality around authentication and ongoing management of identities. You can also go to a CIAM provider who can give you advice about which biometric technologies would suit your digital service best and can deploy a full identity solution, incorporating your biometric needs.

> A CIAM provider can give you advice about which biometric technologies would suit your digital service best and can deploy a full identity solution, incorporating your biometric needs.

Identity-as-a-Service (IDaaS/SaaS-delivered IAM) is a very fast and easy way of embedding biometrics and other identity capabilities (like SSO and MFA) into your application.

Ubisecure's Identity Platform, which can be deployed as IDaaS, private cloud or on-premises, connects to various biometric authentication methods for different use cases and with easy integrations, bridging the gap between biometrics providers and your company.

Get in touch for bespoke advice based on our many years of experience providing proven identity solutions, or **start a free trial of IDaaS**.

About Ubisecure

Ubisecure provides feature-rich customer identity management software and services to help companies reduce identity data breach risk, improve operational efficiencies, and improve user experience.

The company provides a powerful Identity Platform, deployed as IDaaS, Cloud, or on-premises software. The platform consists of productised Customer Identity & Access Management (CIAM) middleware and API tooling to enable single digital identity benefits across multiple applications. Capabilities include enabling complex authorisation and delegation workflows, single sign-on (SSO), frictionless multi-factor authentication (MFA), user identity management, and pre-established connections to dozens of third-party identity providers (social, mobile, and verified).

Ubisecure's Right to Represent is a representation governance solution offering a fast and easy way to assert and verify an individual's mandated rights to electronically represent their company, including financial, signatory, or other authority. Ubisecure's widely used Delegated Authority solution allows individuals and organisations to manage which users and organisations can act on their behalf to dramatically reduce costly, time consuming and delay-prone manual workflows.

Ubisecure is accredited by the GLEIF to issue Legal Entity Identifiers (LEI) under its RapidLEI brand. RapidLEI is a cloud-based service that automates the issuance and registration of these highly assured organisation identifiers.

UBISECURE®

www.ubisecure.com
sales@ubisecure.com