iProov

Biometric Authentication

Government

What is Biometric Authentication?

Authentication is the process of establishing someone or something as genuine, true, or valid. The biometric element refers to using unique biological characteristics such as a person's face, irises, fingerprints, or voice to accurately identify the user. In the digital sphere, it means establishing and verifying the identity of a person when that person is in the act of claiming or asserting that identity. Biometric authentication can enable this to be done remotely with the highest levels of security.

During an online enrollment process, for example, a customer can be asked to scan a government-issued identity document such as a passport or driver's license to verify their identity. They then complete a selfie-style face scan to confirm that they are who they claim to be.
Once they have enrolled, ongoing biometric authentication can confirm the user's unique biometric characteristic against the template created during this initial verification process.

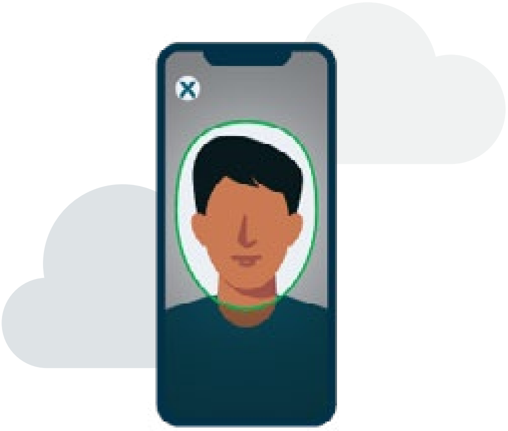
There are two key processes where biometric authentication can be implemented for access to government services:

1. Enrollment

Biometric face authentication can be used for an online enrollment process. A citizen can be asked to use a mobile device or computer to scan a trusted identity document such as a passport, or, in some countries, access a government held database to verify their identity. They would then complete a selfie-style face scan to confirm that they are who they claim to be.

2. Ongoing Authentication

Once the citizen has enrolled, they need an appropriate level of security for future authentications. Biometric authentication can be used for many different services such as completing a tax return, applying for benefits, or accessing health data.



The Advantages of Biometric Authentication for Government

Drives high digital adoption and completion rates

A McKenzie report shows that governments that do not provide adequate access and coverage of services struggle to achieve digital adoption at a wider scale. Estonia has 99% of public services available online and a high adoption rate by its citizens. Their Smart-ID service uses biometric authentication technology that allows citizens to authenticate their identity, provide digital signatures online, and renew a Smart-ID account without having to visit a branch.

The accessibility and usability of some biometric authentication solutions can reduce friction both in the enrollment stage and during ongoing authentication. The technology can streamline enrollment by simplifying the user experience, which leads to higher enrollment completion rates. Additionally, an effortless user experience can encourage citizen uptake of other digital services down the line.

Did you know?

Many citizens are willing to pay for online convenience.

86%

of Americans said they would consider paying to renew a driver's license or ID online.

Did you know?

Although

165

countries provide at least a partial digital ID system, 72% of those countries do not provide access to digital public services

(McKenzie)

Protects against cybercrime

Hackers and fraudsters are always on the lookout for gaps in security and ways to exploit organizations and their users. Traditional authentication processes such as passwords are easy targets for attackers. Passwords are frequently lost, forgotten, manipulated, or stolen meaning they are not accurate in confirming a user's authenticity as criminals can repurpose credentials. Without secure verification, a fraudster can use fake or stolen identities to access government benefits or services. Wider data breaches that expose usernames and passwords also weaken the integrity of the security process, exposing governments to risk and impacting their reputation with citizens.

As criminal methods become more advanced, governments must find new ways to defend against these attacks. Biometric authentication can robustly reinforce fraud prevention efforts and help ensure the right user is accessing their accounts. For example, when authentication is required to enable a citizen to enroll or access services, a selfie-style biometric face scan can be completed quickly and effortlessly on the user's personal device. This presented image is then matched to a verified document issued by the government and checked for liveness. This process protects against cybercrime during remote enrollment and authentication by accurately verifying that the remote individual is the right person and a real person. iProov Dynamic Liveness® also provides the critical additional check that the individual is interacting right now. This delivers thorough and sustainable security measures that defend against sophisticated attacks, working to provide considerable protection while also delivering an effortless user experience.

Supports digital transformation

In the past few years, enterprises in the private sector have reacted swiftly to become a part of the burgeoning digital economy. Seeking to meet the evolving needs of modern consumers, these businesses have enhanced their infrastructure and operations to provide digital solutions - but much of the public sector is still in the developmental phase of digital transformation.

While the impact of COVID-19 has accelerated the rollout of government digital programs, legacy manual processes have impacted many governments' ability to meet citizens' expectations of an effortless user experience. However, incorporating biometric authentication with digital access to core government services can enable secure and efficient access for citizens, increase operational efficiency, and reduce fraud. This technology can also future-proof infrastructure, enabling governments to safeguard their citizens in an ever-turbulent threat landscape while also providing convenience.

Inclusive and accessible

As the public sector explores how digital transformation can be used to enhance citizens' experience with government services, this brings up the question - how can you make these new digital services inclusive and accessible for the entire population?

For a digital solution to be widely adopted, it must be inclusive. Government services provided online must be simple to use, regardless of age and education, and offer convenience rather than obstacles for a citizen. For example, in some countries, citizens are required to submit their tax return paperwork at a physical location and verify their identity using an approved document or identification. Biometric authentication can provide a secure online option that ensures the right person is accessing this service, delivering inclusive access irrespective of literacy, cognitive ability or other constraints. Additionally, self-serve kiosks offer an alternative for citizens that don't have access to or possess their own devices, and for those that require additional assistance in person. For governments, a biometric authentication solution also delivers increased operational efficiency as human resources can be reallocated to areas where they are most needed, rather than on administrative tasks.

Did you know?

Over

70%

of individuals would prefer a single secure digital identity for accessing services online

(iProov survey)

Increased Efficiency

Manual verification and authentication processes can impact the quality of the service that governments deliver to their citizens. Biometric authentication can replace manual verification to both reduce overall costs and increase accuracy. The technology is quick, secure, scalable, and more reliable than humans when it comes to verifying identity.

For government services, online biometric authentication can provide secure and expedient access to citizens. However, for those that don't have access to or possess their own devices, alternatives are available that still deliver improved efficiency. In Singapore, thousands of citizens use face verification to access government services at self-serve kiosks. Additionally, citizens who visit the service centers to reset their Singpass passwords have also seen a reduction in waiting time of over 10 minutes.

Supports a citizen-centric approach

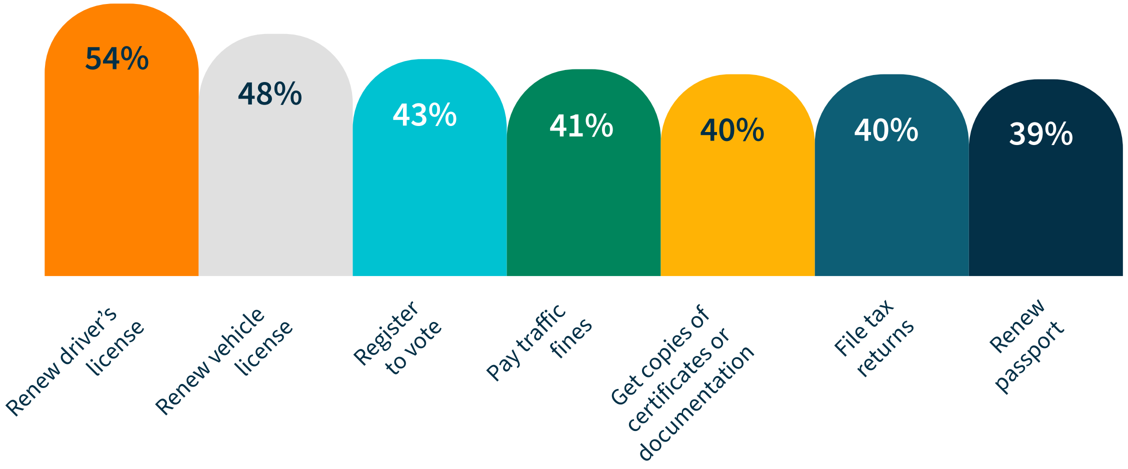
When it comes to digital services, users value convenience, efficiency, security, and privacy. Most people now expect to be able to complete even the most secure processes online. For a government to meet this expectation, they must ensure that the correct and necessary checks are completed with high degrees of accuracy as well as meeting the needs of the citizen.

Biometric authentication can reinforce security infrastructure, helping governments to avoid the loss of public trust that comes with fraud and data leaks. When governments provide secure services based on the needs of the citizens they can increase public satisfaction. For example, iProov Dynamic Liveness® can help governments to protect against fraud and cybercrime while also facilitating a simplified user experience that enhances citizens' trust and satisfaction.

In an iProov survey, American citizens were asked about their willingness to use digital government services. The three top choices for which services should be available online were all sensitive processes requiring secure identity verification: driver's license renewal, renewing a vehicle license, and registering to vote.

Biometric authentication can provide secure verification for many online government services and satiate the increasing demand for convenience from citizens.

Which government related services would you like to use online rather than in-person or over the phone?



Everyone's already using it!

Did you know that over 75% of U.S. consumers have used some sort of biometric technology? In a 2019 study regarding online payments, participants highlighted the main benefits of biometric technology were that it was quicker and more convenient than traditional verification methods such as passwords, with 44% of respondents noting each of these benefits. Another 37% also said it was more secure than other verification methods.

Over the past decade, biometric technology has become a staple of everyday life. Ranging from facial verification to fingerprint scanning, the public has become increasingly competent, comfortable, and experienced in the use of biometric technology. Face authentication, in particular, has a major advantage over other biometric options as it does not require specialist hardware; most devices have a front-facing camera, making facial authentication available to a large portion of the population.

Why do Governments Need Biometric Authentication?

Protection Against Cyberattacks

Biometrics provide defense against account takeover and identity attacks, helping to safeguard citizen digital identity, as well as the reputation of government organizations offering the digital service.

Boosting Government Reputation with Citizens

Replacing legacy processes with biometric systems can help to increase operational efficiency and reduce fraud. Ultimately, this will boost citizen satisfaction and enhance the reputation of the government.

Inclusivity

Digital solutions must be simple for all to use. Employing effective biometric technology means any citizen, regardless of device, platform, or access to a smartphone, can have secure usage of government services.

Improving Citizen Trust

There is increasing concern about data privacy and identity theft in the public sphere. Governments need to maintain citizen trust with secure authentication.

Citizen Convenience

The public expects government services to match the usability of the services they receive from the private sector. Biometric verification can be used as part of a multi-factor authentication strategy, providing the extra security factor while simplifying the citizen user journey.

Win at Digital Transformation

Whether it's attracting new digitally native citizens, saving money or streamlining processes, digital transformation goals can be achieved with biometrics.

Accessibility

Biometric authentication can improve usability and provide citizens access to government services irrespective of age, language, disability, or education level.

Growing the Digital Economy

A McKinsey report shows that pre-pandemic the potential economic gain by 2030 for countries implementing a digital ID was between 3-13% of GDP - since COVID-19 this estimate has increased by 20%.

Interested in learning more about how biometric authentication can support your digital transformation? Visit iProov.com.

iProov is the world leader in providing facial biometric authentication technology to financial institutions, governments and other enterprises that need to securely verify customer identity online. Used for onboarding and authentication, iProov customers include the Australian Taxation Office, GovTech Singapore, ING, Rabobank, UBS, U.K. Home Office, UK National Health Service (NHS), and the U.S. Department of Homeland Security. In December 2023, iProov was included in the Gartner Innovation Insight Report for Biometric Authentication. Accuity Market Intelligence listed it as a Luminary in the 2023 Biometric Digital Identity Prism. The company was also recognized as an Innovation Leader by KuppingerCole, in the Leadership Compass, Providers of Verified Identity 2022 report.

Follow us on LinkedIn and Twitter for the latest news and industry updates.

iProov

For more information on how to assure the genuine presence of the **right** person, **real** person, authenticating **right now** contact us at:

contact@iproov.com

iproov.com