Implementing a national digital ID program based on biometrics

Biometric face verification offers a reliable method of checking that citizens are who they claim to be. Are you ready to use it for your digital ID program?

IDENTITY

POSTED ON 05.23.22

Before the pandemic, there was a general initiative from governments around the globe to implement remote governmental services so that citizens could renew ID documents, fill in their tax returns and complete other basic tasks without in-person interaction with the administration. However, the Covid-19 pandemic has revealed that governments globally are far from their aim of **becoming fully digital**. It has also demonstrated that **preventing online identity fraud** will be one of their main challenges in the coming years.

Now let us consider the fact that we all have a secure way to prove our identity: our biometrics. Easy, accessible and secure, **biometric face verification offers a reliable and convenient method** of checking that citizens are who they claim to be. Before governments embark on this journey, we have identified three key success factors that must be considered. Are you ready to unlock the potential of your national digital ID program using face biometrics?

Remote governmental services a necessity for the functioning of states

The pandemic has shown that remote governmental services such as applying for and renewing ID documents, filling out tax returns, requesting repeat medical prescriptions, accessing online telemedicine appointments, voting, etc. are necessary for the functioning of society. It is vital that governments provide their citizens with eServices, and the only way to do it is through a **digital ID system that is secure and easy to use**. The pre-requisite for citizens to access eServices is to be able to easily and securely prove their identity, and this is **where biometrics step in**.

The aim is clear: offer remote services through a national digital ID scheme facilitated by secure face verification. But what are the key ingredients to make such a complex project a success? How can citizens be reassured that their data is safe? And how can citizens and the private sector be encouraged to embrace the project for its ultimate success—the widespread adoption and the true digitization of private and public sector services?

The growing adoption of biometric technologies

Today, face verification is commonly used across a wide range of technologies and services. People can securely unlock their smartphones, access their bank accounts and health records, check in for a flight—the list is endless.

According to several surveys, the use of biometric technologies is becoming more and more accepted by users. The 2021 Global Passenger Survey from the International Air Travel Association (IATA) revealed that **73% of passengers would be interested in using their biometrics** instead of boarding passes and passports for all airport processes. From the USA to Asia, many airports have already adopted face verification technology.

And the travel industry is not the only one trusting biometric technologies to offer faster and seamless services. Fingerprint and face verification are **also used to authorize payments**: Juniper Research[1] forecasted that biometrics would be used for more than 18 billion transactions by 2021, growing at a compound annual growth rate of 83.7% from 2016. BAXE, an Australian FinTech, launched the first decentralized blockchain ecosystem using a facial authentication solution for identity verification—enabling their users around the world to authenticate high-value transactions, reclaim lost passwords and regain access to locked accounts using face verification.

Three key success factors that governments must consider before they embark on a digital ID program

In the USA, four states – Oklahoma, Mississippi, Delaware and Arizona,—have already introduced Mobile ID to their residents. This digitized version of the physical driver's license can be accessed via a free app using the holder's fingerprints or face biometrics. This is only an example and the implementation model for **national digital ID systems might vary from one region of the world to the others** depending on the existing infrastructure. However, there are three main success factors that governments should consider whatever the model they choose for their digital ID program, and in particular for the use of biometric technologies in that context.

Success factor one: The securest authentication and the highest protection of citizen personal data

Multibiometrics to strengthen the digital ID system

The widespread adoption of any national digital ID scheme will only happen if all users involved trust that their **personal data is secure** and that the **authentication technology is accurate**. We have already clarified that biometric technologies offer an accurate and convenient method of authenticating the identity of a person. To ensure that an individual is who they claim to be, using one form of biometrics is a good idea, but combining two or more reinforces accuracy. Multibiometrics, for example, verifying a person's face along with their fingerprints, prove beyond a shadow of a doubt that they are who they claim to be.

Attack detection to prevent fraudulent access to governmental services

Fraud is a serious issue; therefore, biometric algorithms need to continually be strengthened and improved in order to **stay one step ahead of fraudsters** to thwart all attempts of ID fraud.

Attack detection techniques offer additional reassurance for all parties involved in a national digital ID system. Face verification technologies often include a passive and active approach to prevent spoofing attacks. The **passive approach** consists of taking a selfie to prove that they are actually presenting their face to the camera (and not a picture or a mask). The **active approach** relies on interaction between the user and the application, aka the 'challenge request'. Several methods are available on the market such as nodding, blinking and smiling. Both the active and passive approaches ensure that the person is alive and is not an impostor wearing a mask.

Personal data security for the user

Nearly all users will access remote governmental services using their smart device (smartphones and tablets). However, there are certain questions being raised regarding the security of accessing government portals and **sharing sensitive data using a personal smart device**. From a citizen's point of view, their smartphone has many benefits; it is convenient, always accessible and **personal data stored on their smartphone remains under their control**. Despite this, there is

some criticism to the reliability and security of a smartphone. For example, it is common for users to download third-party apps that are not always thoroughly vetted and may render information on a smartphone vulnerable. However, secure **data sharing and processing techniques** make it possible to offset these disadvantages.

Depending on the approach chosen for the national digital ID scheme, the user's personal and biometric data can remain on their smartphone, which is where the verification techniques are carried. The smartphone completes a verifiable calculation that it shares with the organization that requested it without ever divulging any of the user's personal data. This technology, called **verifiable computing**, means that one central entity can outsource the computing of data to another potentially unknown, not previously verified entity, while maintaining verifiable results. This means that citizens can do the matching of their own data to **verify their identity on their smartphone** (i.e., the unknown, not verified entity), **without anyone doubting the validity** of the computing done. Citizens control their biometric data at all times, and it never leaves their device.

Multi-party computation provides another layer of security. Whether the verification is built into the app or is centralized in the cloud, with multi-party computation, the processing of the data is shared by different parties. All the open, vulnerable data is not processed by one central player but several contributors. Only by breaching the data processed by each player would the data make sense to a malicious perpetrator. The right technology provider will offer both technologies for the national digital ID scheme.

Success factor two: The right technology provider

Finding a reliable technology provider to protect governmental services with biometric technologies can be a daunting task. Checking that the selected provider has worked with governments and private sector service providers worldwide and has a proven track record is comparatively easy. However, how do you know **which provider can be trusted with citizens' personal data?** Furthermore, algorithms can be tricky to understand. How do you know if the algorithms are working as they should, and if they are doing exactly what the technology provider states?

The simple answer is to always select a provider whose algorithms have been **certified by independent third-party testers**. To test the performance of algorithms, there are many independent bodies, such as the National Institute of Standards and Technology (NIST), that provide neutral evaluations that are available to the public. It is very important to check how biometric technologies from different companies measure up against each other based on large data volumes.

In order to have the best algorithms on the market it is important for technology providers to continuously invest in improving them. One of the most important aspects of AI-based automated face verification is to teach algorithms to be **accurate**, but also to be **fast** and **optimized for fairness**.

Accurate, fair and unbiased algorithms

Citizens of a population differ in age, gender, ethnicities and facial features (beards, glasses, and even makeup). These differences produce a variation in algorithm performance, which means the more diverse the data used to train it, the better the algorithm will perform.

Biases primarily come from training databases, which is why technology providers need make sure that their databases contain a variety of images of the same element in various acquisition conditions while **respecting local and international privacy regulations**—for instance, European providers are subject to strict regulations when using citizen personal data.

Ensuring face verification algorithms are fair and unbiased toward everyone is not an easy process, but the most advanced **deep learning solutions** are now up to the task.

Success factor three: The best user experience

Another key success factor to encourage the widespread adoption of the national digital ID scheme by all parties, and

thereby guaranteeing its success, is the **ease of use of the technology** involved. To ensure a digital ID is user-friendly, the face-capture environment has to be taken into account.

Face verification as a means of biometric identification to unlock phones, for example, has been in existence for many years, and therefore users are more comfortable with its usage. Yet, factors such as the lighting, time of day and even angle of capture cannot be predicted, which is why all remote governmental services need to include **software that guides the user** and provides easy-to-understand instructions.

Key takeaways for a robust digital ID system

We have identified three key success factors for a national digital ID scheme based on biometrics:

1. **Biometric verification and protection of citizen data** is the basis of a secure digital ID scheme.
2. Secure face verification can only be achieved by a **renowned technology** provider with an established international footprint and **vetted by an independent third party**. A provider that has long-standing relationships with governments around the globe proves that there is a good rapport of trust and confidence.

Security and convenience, i.e., the user-experience, go hand in hand for a successful digital ID program.

---

[1] https://usa.visa.com/visa-everywhere/security/new-report-on-biometric-authentication.html

---