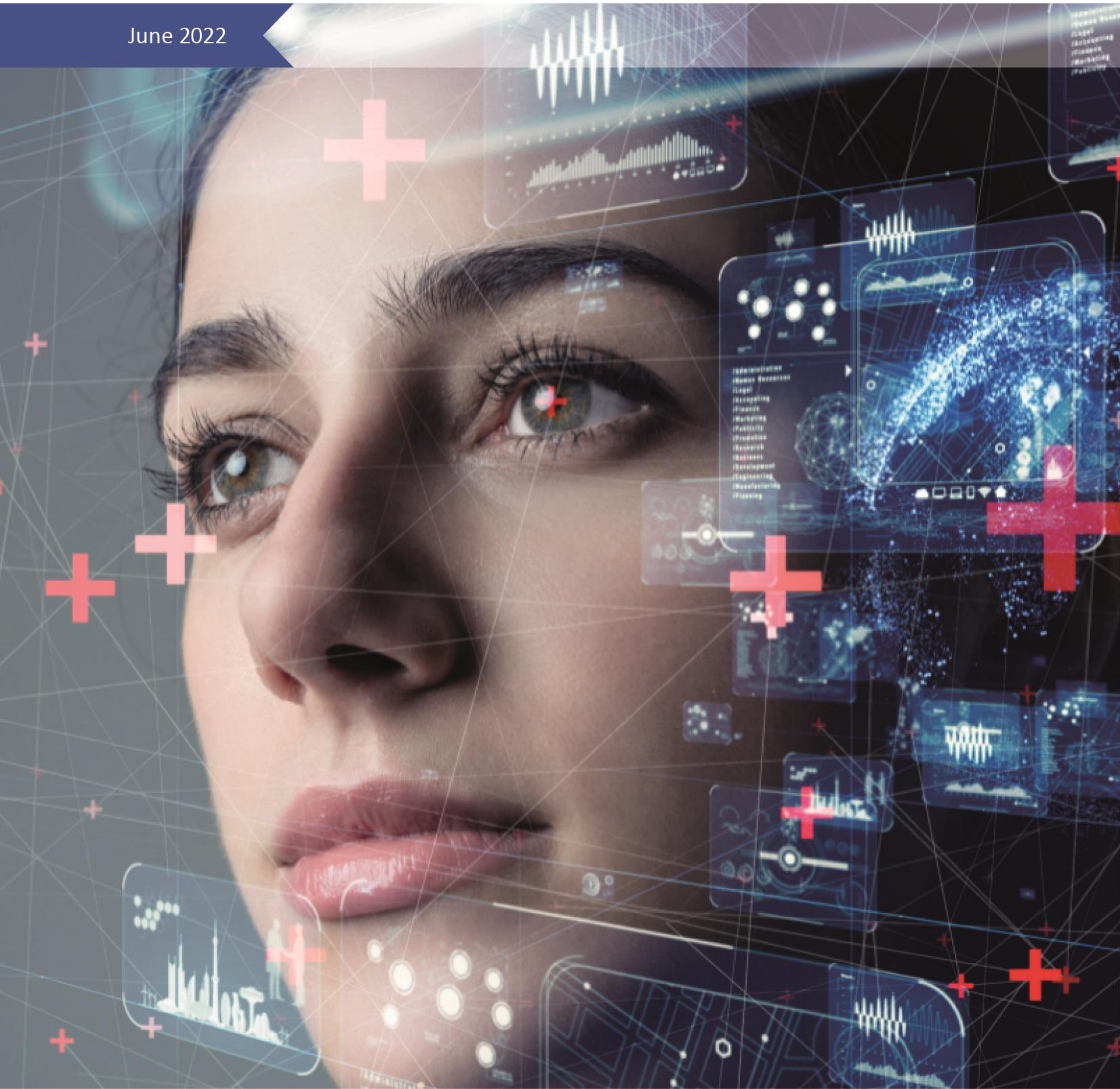
Biometrics Institute Concepts and Solutions Report

Biometrics and Digital Identity

June 2022



Contents

1. Introduction ... 3

2. Anonybit: Deploying biometrics with privacy, inclusion and scale in mind ... 4

3. Austrian Institute of Technology: Upcoming challenges concerning biometric capturing of fingerprints ... 6

4. Daltrey: Passwordless authentication – it starts with identity ... 8

5. FacePhi: Ethical biometrics: the challenges of video surveillance and fundamental rights ... 10

6. Giesecke+Devrient: The need for strong, seamless and phishing resistant Multi-Factor Authentication (MFA) ... 12

7. ID R&D: How ID document liveness detection helps prevent fraud in digital onboarding ... 14

8. InnoValor/ReadID: Balancing AI probability and crypto certainty in identity verification ... 16

9. Innovatrics: How to enhance passive liveness detection for greater accuracy and improved customer satisfaction ... 18

10. Onfido Ltd: The use of biometrics and other signals at onboarding for the prevention of fraud ... 21

11. Paravision: Future borders are digital: There are two sides to this coin ... 23

12. Reason360: Biometrics x Service ... 25

13. secunet Security Networks AG: Man or morph? ... 27

14. Secure Logistics B.V: A trusted digital identity combined with an on-card biometrics solution ... 29

15. SISSA Integral Monitoring: Personalized biometric solutions: the importance of technology integration ... 30

16. SITA: Digital identity and travel ... 32

17. Veridas & dasGate: How a facial biometric system provides access to a Spanish Football League ... 34

1. Introduction

In 2020 and 2021 we published two editions of this report which focused on a COVID-19 response.

1. COVID-19: Effective and responsible biometrics solutions and concepts in a time of pandemic – building a resilient response
2. COVID-19: Effective and responsible biometrics solutions and concepts – one year into the pandemic

Since then, they have had over **8,000 downloads.** Thank you to everyone who has participated in this and previous reports.

For this 2022 report, we asked our members to focus on effective and responsible biometric solutions and concepts for **biometrics and digital identity**. As new products are often of interest, we have also allowed our members to place an advert in the report.

This report is a compilation of submissions from some of our supplier members who wanted to share their thoughts and ideas. The submissions provide insights, lessons learnt and solutions available and tested that may provide answers to the use of biometrics and digital identity.

Proposed themes for the report were:

- Challenges the world is facing and potential solutions for digital identity
- Biometrics for digital identity authentication
- Preventing and recovering from account takeover: how biometrics can help
- Potential consequences of biometrics for digital identities e.g. digital surveillance risk
- Public perception of the use of biometrics for digital identity
- Re-use and interoperability – sharing of digital identities
- Use cases for digital identity: biometrics where and why?
- New technology solutions and what they offer
- Digital passports – what is available and what will come next?
- Questions about digital onboarding and liveness
- Governance and new legislation

Please note that the Institute does not endorse any of the submissions nor have we edited the documents. We are sharing them to help generate discussion as the world searches for solutions to new challenges.

If you have any questions about the content of the submitted papers, please contact the authors directly. For anything else relating to the work that the Biometrics Institute does, please contact me.

Many thanks

Isabelle Moeller
Chief Executive
Biometrics Institute
manager@biometricsinstitute.org

2. Anonybit: Deploying biometrics with privacy, inclusion and scale in mind

Introduction

The biometrics industry has grown and changed rapidly during the pandemic. Many companies and government agencies realized the power of biometrics and digital ID. Some of the programs that were deployed came under very strong criticism, creating a significant backlash for the industry, causing practitioners to consider how they can ensure privacy and inclusion at scale while implementing strong security. This piece analyzes many of the issues raised and offers a proposal for a reference architecture that adheres to industry best practices.

Biometrics are not foolproof

Biometric accuracy rates are measured in two ways - false accept rate (FAR) and false reject rate (FRR). The point at which they meet on a graph is called the Equal Error Rate (EER). In some cases, it is better to optimize for one or the other, but when deploying across a very large population, both need to be taken into account because you cannot have too much friction for people that need to access their accounts, yet it is critical to keep the imposters out. On the false reject side, the concern is that too many people will need assistance to get into their accounts in what is supposed to be a seamless process.

On the false accept side, it is the opposite consideration - that imposters will be able to get through the system. Given the scarcity of real deployment data, it is hard to know what actual performance is in the field, but this much we do know: high level NIST performance testing shows 99.5% accuracy among the general population, and a recent DHS study shows that top performing algorithms will hold up against different skin tones.

Communication is key, but practically speaking, alternative processes are needed for mass market rollout of biometrics

A widely deployed system must take into account a number of considerations, biometric accuracy being only some of them. Exceptions will abound; some people may not feel comfortable interacting digitally or may not have access to internet services (elderly, disadvantaged, rural).

One thing that is well established is that when biometrics technology is deployed, and people are given the option to participate, acceptance rates will be tremendously high if there is perceived value. In fact, in a recently released report, the International Air Transport Association found that 73 percent of passengers are willing to share their biometric data in order to streamline travel processes.

Consumers expect their data to be protected by the entity they are sharing with

In 2018, it was disclosed that 87 million Facebook users had their personal data collected and used by a third party consulting firm called Cambridge Analytica for political advertising. The data was collected through a Facebook app that users willingly interacted with, but had no active consent or idea that their data would be used for this other purpose. Simply put, there was no expectation that their information should or would land with a third party that would then own their data for other purposes and we have seen similar concerns in more recent attempts to roll out large scale biometrics with third parties.

The concerns go beyond user privacy. As stated earlier, given that 40% of US businesses were the target of a hack last year (or 70% if focusing only on large businesses), and that most personal data is kept in central honeypots, there is a high likelihood of a data breach with long term ramifications. Most data protection regulations focus on consent, notice and penalties if there is a breach but are silent on best practices to avoid them.

Designing robust biometrics systems

Designing systems for the masses is not simple. There is a lot to be considered. By deploying a robust identity management architecture, governments and private enterprises can avoid many mistakes and responsibly deploy biometrics and ID systems into the future.

1. **Biometrics, not PINs, passwords or KBAs, should be used as the primary means of authentication**. The biometrics themselves should be protected, ideally in a decentralized manner to prevent any misuse or data breach. This can be done using a multi-party computing (MPC) system of nodes, where some nodes are responsible for storage and some are responsible for computation. A system like this affords zero-knowledge authentication, which allows the individual to prove their identity without the original biometric sample being shared.

2. **Enterprises should balance the need for accountability and control over the data they collect with data protection needs**. Blockchain applications create relying party dependencies which may be at odds with KYC and AML regulations that require enterprises to maintain and manage personal data on their customers. Leveraging an MPC framework noted above, enterprises will be able to still control and manage the data they collect in a decentralized manner without sending to a third party.

3. **A selfie collected at account opening can be enrolled into a decentralized biometrics framework for use in down the line authentication**. Multiple biometrics can be enrolled upfront to handle different applications (i.e., voice biometrics for call center uses). For maximum security, a deduplication can be done at each enrollment to ensure there is only one person under each identity in the system, even if they hold multiple accounts.

The benefits of this approach:

- **Significant cost-savings and better user experience**: Using biometrics for self-service account recovery can save a large enterprise up to $1 million per year
- **Data protection compliance and reduced risk of a breach**: With a decentralized approach, data is minimized and privacy by design ensured in compliance with data protection regulations
- **Greater security and less siloes**: Instead of relying on passwordless authentication solutions only to fall back on a password or KBA, this approach ensures that there are no holes in the IAM security posture.

Organisation: Anonybit
Name: Frances Zelazny
Telephone number: +1 917 862 1373
Email: frances@anonybit.io

3. Austrian Institute of Technology: Upcoming challenges concerning biometric capturing of fingerprints

The exchange of forensic data is a vital tool for investigations into transnational crimes as well as an important capability in the identification of terrorists and foreign terrorist fighters (FTFs), including returnees and relocators. In the context of border security and management (BS&M), biometrics supports the process of verifying the identity of those who seek to enter, transit or depart international borders. In this regard, a lack of biometric data being collected and shared internationally has the potential to create a critical security gap which may be exploited by returning and relocating FTFs. The collection, use, and sharing of biometric data to enhance BS&M has to be done in a responsible manner in line with States' obligations under both laws domestic and international. In particular obligations under international human rights law, refugee law and humanitarian law have to be considered. Respect for human rights and the rule of law is complementary with effective counter-terrorism measures and essential to successful counter-terrorism efforts.

The outbreak of the COVID-19 pandemic presents a number of serious challenges regarding the collection of biometric data to monitor the cross-border movement of individuals to counter terrorism. One of the first preventive measures adopted worldwide in response to the outbreak was the requirement for individuals to wear facemasks and gloves to limit the spread of the virus. This measure presents a risk of weakening the current screening procedures and risk assessment measures at borders by preventing the proper detection of individual's facial features and, consequently, the available technologies are significantly exposed to vulnerabilities and failures [NISTIR 8311]. Additionally, what previously had been a simple procedure for cleaning and maintenance of the touch-based fingerprint sensors at border control points, has rapidly become a complicated procedure due to new public health and safety standards.

In response to public health concerns resulting from the pandemic, the global biometrics industry has to develop new solutions which supports verification and identification measures to face off these new challenges. While many States may favour the use of existing (and already operational) biometrics applications, the private sector has begun to invest in solutions to integrate biometrics recognition to detect other data, such as temperature measurement while filtering out non-human heat sources. Furthermore, ***new contactless biometric sensor technologies*** have been developed based on new technical capabilities to address the new challenges. Touch-free access control and monitoring systems as well as ***contactless identity verification and identification systems*** are promising new solutions which not only address the health requirements in times of pandemic but also increase potentially the accuracy, quality and performance of biometric systems.

From the user-perspective viewpoint there are three main issues which have to be addressed and solutions or implementations should be accordingly communicated to the broad public: Convenience, hygienic concerns and data privacy concerns.

Convenience: In fact, it seems to be simple: press your fingers to a device and that's it. Unfortunately, diversity in human mankind prevents a smooth recording simply because there are finger-types which are dry or wet or simply worn with poor identification features. There are additional pitfalls in using fingerprints at borders because not everybody is a technical specialist and knows how to deal with devices which do not always have a friendly user interface. A placement picture and a green or red light are often the extent of user guidance. Capturing 4 fingers with high quality without attendance from trained personnel is not easy to achieve and even more complex in a completely unattended scenario. This situation, however, exists in in many airline operations.

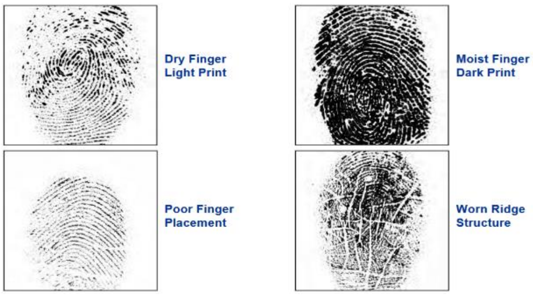
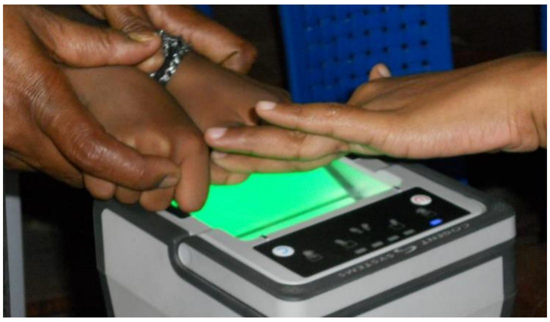


Figure 1: poor image quality: dry/wet finger, alignment and worn ridge structure (Source NIST)



It is essential to understand in this context the quality requirements for the different principle use cases: identification and verification. The first works only with the highest possible capture quality. Recognition rate drops significantly when using low quality fingerprints!

Figure 2: How to use a contact based fingerprint scanner

Hygienic concerns: Shared contact with potentially contaminated surfaces can spread diseases to others. Little is known about the effectiveness and amount of certain pathogens on biometrics touch surfaces. Obviously, the global pandemic demands new procedures and practices: Cleaning the surface of a scanner before/after each use and incorporate the person to identify with these new rules. Anyway, a faint – psychological based - uncertainty remains, also after surface cleaning.

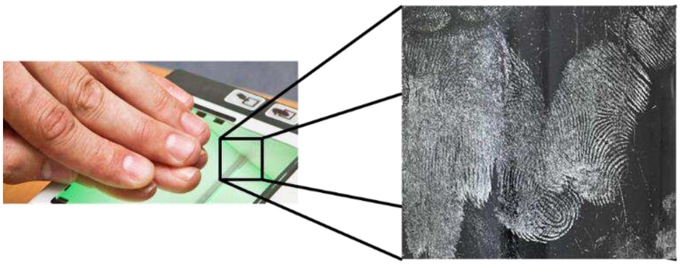


Figure 3: possible (COVID-19) pathogens and fingerprint traces on the sensors glass surface

Data security concerns: As an example, in Europe, the GDPR (General Data Protection Rules) are very strict, also the population is somewhat restless when it comes to the storage of biometric data. Once hacked or exploited, there is no way to take back the data or assign new data as is possible with passwords. There is an urgent need to think about better protection of those unique datasets. There are some first approaches like multiparty computation of homomorphic encryption where data is NOT decrypted at the server side and, therefore, a potential data breach has very low impact.

Summary:

- It will be of utmost importance in the future to increase convenience & speed, while decreasing hygienic concerns in the capturing process
- Increase trust by using modern privacy preserving technologies
- Enable and introduce worldwide standards to measure contactless fingerprint capture quality
- More practical demonstrations and pilots of contactless fingerprint access control solutions
- Development of standards (e.g. like NFIQ 2.1 Fingerprint Image Quality Measurements adopted to new contactless capture devices)
- Independent evaluations about matching quality (especially contactless to contactbased existing databases, similar to the NIST report [NISTIR 8307]
- More collaborative work between infrastructure operators, governmental applications providers, industry and independent research centers
- Research work and proof-of-concepts for privacy preserving biometric matching solutions, like homomorphic encryption or multi party computation and biometric matching in the encrypted domain.

[NISTIR 8307] NIST, National Institute of Standards and Technology, Interoperability Assessment 2019: Contactless-to-Contact Fingerprint Capture, https://doi.org/10.6028/NIST.IR.8307

[NISTIR 8311] NIST, National Institute of Standards and Technology, Ongoing Face Recognition Vendor Test (FRVT), Part 6A: Face recognition accuracy with masks using pre-COVID-19 algorithms, https://doi.org/10.6028/NIST.IR.8311

Organisation: AIT – Austrian Institute of Technology
Name: Bernhard Strobl
Telephone number: +43 664 815 78 42
Email: bernhard.strobl@ait.ac.at

4. Daltrey: Passwordless authentication – it starts with identity

The concept of a passwordless future is nothing new. It's nearly 20 years since Bill Gates predicted the end of the password at the 2004 RSA Security Conference. Numerous vendors now promote their own passwordless solutions promising 'seamless authentication' and 'absolute security'. And yet, much of the passwordless movement so far has failed to deliver on these promises.

Why? Because going passwordless isn't about passwords – it's about identity. And this is where much of the existing approach to passwordless authentication has fallen short. It may improve the authentication method, but still fails to confirm the identity of the person authenticating.

The problems with passwords are well established:

1) They're weak – easily shared and hacked through brute force attacks, and
2) They're frustrating to use – frequently forgotten and frequently needing to be reset.

The statistics are well documented. Depending on which report you read, between 60 and 80 per cent of breaches are perpetrated from compromised passwords and the average user now manages up to 100 different passwords, with an average cost of resetting a password at US$70 per reset. It's no wonder the development of passwordless authentication technology has gathered such momentum.

But to truly solve the problem with passwords, a passwordless authentication solution needs to adequately address both issues. It needs to remove the security vulnerability of a credential that can be easily shared and stolen, and it needs to be simple and convenient to use. Solutions like one-time codes, hardware tokens and even device biometrics have all failed this test because they don't fix the underlying issue – if you don't know who's authenticating, you can't adequately defend against the risks posed by the current cyber threat environment. Particularly in a distributed workforce with teams working remotely all over the world.

What's the point of replacing passwords with an alternative that doesn't provide the outcome of ensuring that the person authenticating is who they should be?

It starts with identity

In the same way an organisation can't control who is using a password, they can't control who's using credentials like one-time codes or device biometrics to access their assets. When biometrics are only bound to a device (and not a verified identity), multiple people can enrol their own biometrics on the same device, creating an additional attack vector. For truly secure passwordless authentication, you need to verify the person, not just the device or token.

Without verifying a user's identity and binding this identity to their biometric data, there's no way to control the process of confirming who a person really is, and who is using a credential to access an asset.

Redefining strong authentication

The only truly secure option for any protected environment is strong authentication, i.e. understanding who a person is when they use a credential.

Unlike single-factor and many traditional forms of multi-factor authentication (MFA), strong authentication must start with a reliable user onboarding process to create a biometric credential, which involves:

- Identity proofing to verify that the person is who they claim to be,
- Deduplication to ensure the user isn't already onboarded, and
- Binding the person's identity attributes (e.g. nationality, age, employment status, security clearance) to their biometric data.

Ensuring the passwordless authentication process binds the biometrics to the relevant identity attributes is what upgrades an MFA practice to strong authentication, providing the highest level of assurance that the person authenticating is who they say they are.

Ensuring the integrity of the authentication

The integrity of any biometric authentication depends on the advanced security techniques that need to be deployed to protect the authentication workflow. In other words, there's no benefit in a best-in-class biometric algorithm performance if the end-to-end security of the authentication workflow isn't addressing the holistic risks presented by the cyber threat environment.

It's the responsibility of both organisations and passwordless authentication vendors alike to ensure the integrity of the authentication by:

- Protecting biometric templates – encrypting biometric data end to end and decrypting it to the selected server
- Securing end points – ensuring the protection of end points through application and device-level security
- Adapting to new presentation attack methods – working collaboratively to share information about biometric attack methods and ensuring the models being used for PAD can be updated as needed to protect both organisations and users.

Underpinning all of this is also the adherence to privacy and security standards. Fortunately, recent standards development around biometrics management (like ISO/IEC 24745:2022, for example) is contributing to increased security assurance for organisations and privacy protection for users. Compared to its 2011 iteration, ISO/IEC 24745:2022 provides more concrete requirements for enforcing privacy protection and introduces new options that take into consideration more recent privacy-enhancing technologies.

Because ultimately, the goal of strong authentication using biometrics is to make the passwordless authentication process safer for both organisations and users.

Organisation: Daltrey
Name: Edwina Lawry
Telephone number: +61 429 621 539
Email: michael.warnock@daltrey.com

5. FacePhi: Ethical biometrics: the challenges of video surveillance and fundamental rights

In a global and interconnected world where the way we relate to each other has become largely digital in the wake of the pandemic, biometric recognition and the field of video surveillance are advancing faster than the law. In this context, the processing of biometric data through facial recognition technologies affects the right of individuals to the protection of their personal data and their right to privacy.

It is important to distinguish in this area the processes related to the collection and use of biometric data of individuals for identity verification purposes in public spaces. This has been one of the most controversial issues in recent years. The European Parliament has requested EU member states to limit the use of facial recognition and has underlined, with regulatory reflection, that the use of this technology can only be deployed by the authorities for public interest purposes, strictly regulating those aims.

When legislating on the use of facial recognition systems in public spaces and, specifically, seeking to facilitate video surveillance techniques, some legislators expressed their desire to go a step further and ban the use of facial recognition technology and automated biometrics. On this issue, the General Data Protection Regulation comprehensively categorizes the conditions under which the processing of biometric data must be carried out.

As a consequence of this ethical debate, already in 2020, the White Book on Artificial Intelligence is drafted on the basis of a European approach oriented towards excellence and trust. A year later, in April 2021, the draft EU Regulation on Artificial Intelligence is drafted with the objectives of ensuring that AI systems are safe and in line with fundamental rights and values of the Union, ensuring legal certainty to facilitate investment and innovation in AI, improving governance in terms of rights and facilitating the development of a single market to make legal, safe and reliable use of this technology.

Despite these advances, specific data protection requirements are still taking shape and this is not an issue that should confuse or limit developers and operators from relying on and improving such technologies. For this reason, technology companies that develop this kind of cutting-edge solutions are the first interested in guaranteeing companies solutions for verifying the digital identity of their users developed on the basis of ethical principles, preserving and protecting the privacy of their biometric data when performing authentication processes, in addition to providing extra value to the end user.

Ethical biometrics, our hallmark

The ethical debate that accompanies technological advances is part of human history. The moral implications of the development of authentication technology have also been with us since the company's inception and have been a key part of its business growth.

In the development of any technology, we are firmly committed to ethical biometrics, as it always relies on the user's consent. It is essential not to carry out unauthorized authentication by end users; they are responsible for authorizing their recognition by accepting the use of this technology. In this way, the companies guarantee that the end user is fully aware of the process being carried out.

In addition, facial recognition technology allows access to online banking, cash withdrawal at ATMs, access to an airplane or allows retirees and pensioners to give proof of life to collect their monthly pay from their cell phone.

In this sense, biometrics must ensure compliance with the main standards that regulate the digital identity verification industry, so that all information obtained from the user's consent is used to protect what is most valuable: their digital identity.

Organisation: FacePhi
Name: Cristina Lidón
Telephone number: + 34 965 108 008
Email: clidon@facephi.com

FacePhi
Identity Platform

Portrait Assessments
Eyes open
Eye distance
Even lighting
Proper exposure
Correct focus
Normal eye color
Uniform background
Hot spots on skin
Incorrect ratio of head/image

6. Giesecke+Devrient: The need for strong, seamless and phishing resistant Multi-Factor Authentication (MFA)

Background

With the continuing acceleration of online services and remote working activities triggered by COVID-19, there is an increasing number of cyberattacks, identity thefts and account takeovers. The situation is further exacerbated by new or previously offline users who have been forced to transact online; they are the most vulnerable to cyber scams and fraud. Additionally, more sophisticated attacks are becoming harder to detect, even for digitally savvy and security conscious users.

In response to several high profile cyberattacks, the US government has mandated the use of multi-factor authentication (MFA) [(1)]. The Australian government is also strongly encouraging the adoption of MFA as part of its Essential 8[(2)] risk mitigation strategies against cyber attacks.

> *Multi-factor authentication (MFA) is one of the most effective ways to protect against unauthorised access to your valuable information and accounts.*
>
> *- Australian Cyber Security Centre[(3)]*

In recent months SIM swapping attacks have occurred, including in Australia. The Australian government is now mandating more stringent identity verification checks (such as MFA) for the porting of numbers to new SIMs.[(4)]

The factors in MFA refer to:

- what you know (knowledge based factors eg. password, PIN code, personal information such as date of birth, driver license number, etc),
- what you have (possession based factors eg. mobile phone, watch, card, hardware tokens with one-time passcode, etc) and
- what you are (inherent based factors or biometrics eg. fingerprint, facial, voice, iris, etc).

MFA refers to the use of two or more of these factors.

Dangers of reliance on knowledge based factors

Most of us grapple with the complexities of managing passwords and are aware of the potential vulnerabilities when they are compromised, exposed or forgotten. This is even more problematic with stolen personal identities. You can change your password but you can't really change your name, driver license number or your date of birth. When such information is exposed, shared or published on the dark web and organisations still rely on them to onboard and to recover accounts, this can become a never ending nightmare for victims.

The basic problem with 'knowledge based factors' is that they are based on 'shared secrets'. Both parties, the user and verifier, need to know or share the same 'secret'. The secret needs to be protected by both parties, including during the transmission of this information. A shared secret is susceptible to phishing or smishing - phishing via SMS(5), where the man or machine in the middle (MITM) can intercept and capture the secret from the user by impersonating the verifier. The problem lies in both the user and verifier needing to authenticate each other before the secret can be transmitted securely.

The need for stronger authentication factors

Although having a "possession based factor" as a second factor (such as a mobile phone) helps to increase security, it is still susceptible to phishing attacks. Legacy MFA applications such as SMS-OTP and push notifications via a mobile app do not prevent phishing, and are vulnerable to Man in the Middle (MITM) attacks.

A possession based factor combined with cryptography, in particular public key cryptography, can be used to fundamentally solve the problem of phishing and verifier impersonation by providing mutual authentication between the user and verifier. This is done by means of a key pair, where the public key is bound to the legitimate verifier, while the private key is under the possession of the user. Secure authentication can then be achieved.

In the physical world, possession based factors such as smart cards that utilise strong cryptography have received worldwide adoption and are used by governments, defence and enterprises for identity verification, authentication, secure payments and communications. The 'Smart Card' also serves as a hardware root of trust[6] for securing cryptographic keys and data. Additionally, secure provisioning and lifecycle management are employed to ensure unique and immutable identity.

In the online world, it is even more important to use non-knowledge based factors with strong cryptography that are phishing resistant. Many organisations have implemented MFA, but most are still relying on passwords as the first factor, coupled with a phishable factor such as SMS-OTP or push notification. An increasing number of organisations have progressively moved towards passwordless and non-phishable authentication. Microsoft has developed and is offering completely password free options for their enterprise customers[7] as well as for individuals using Microsoft accounts for online services such as email, OneDrive, etc.

Microsoft's passwordless strategy is based on the open authentication standards such as FIDO (Fast IDentity Online) and the FIDO2 standard which incorporates the web authentication (WebAuthn) standard, allowing FIDO compliant devices to work with all the major browsers and operating system platforms on Android, iOS, Windows and Mac.

Combining possession with inherent factors like biometrics enhances usability

Strong authentication needs to be coupled with seamless usability, as it is an essential element in gaining wide consumer acceptance. From a usability perspective, biometrics is an inherent factor that has gained popular acceptance by consumers due to availability on mobile phones. Consumers are now accustomed to using biometrics to unlock their phones and to access their banking apps, as well as to authorise transactions.

FIDO uses the convenience of biometrics to protect private keys for simpler and stronger authentication. FIDO's certification programs help to ensure interoperability, scalability and adaptability. The FIDO authentication protocols have been designed via industry collaboration with a strong focus on usability, security and privacy, while addressing a full range of use cases and offering consumers a growing number of authentication choices[8].

The FIDO standard can also be leveraged by technology providers to further enhance their product offerings. One example of possession based strong customer authentication is Convego® Tap[9] where consumers can use their existing banking card for secure online banking. Another example is the StarSign® Key Fob[10], a biometric device that combines FIDO with other use cases such as physical access and payments.

Conclusion

With the growing threat of cyber attacks, relying on 'knowledge based' factors for online or call centre verification is no longer sufficient. The government and enterprise sectors need to actively plan to provide options for strong authentication methods based on 'possession based' and 'inherent based' factors that are phishing resistant, such as FIDO.

References:
(1) https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
(2) https://www.cyber.gov.au/acsc/view-all-content/essential-eight
(3) https://www.cyber.gov.au/mfa
(4) https://minister.infrastructure.gov.au/fletcher/media-release/new-rules-protect-consumers-against-sim-swap-fraud
(5) https://www.cnet.com/tech/services-and-software/check-your-messages-scam-texts-on-the-rise
(6) https://www.microsoft.com/en-us/research/wp-content/uploads/2017/03/SevenPropertiesofHighlySecureDevices.pdf
(7) https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/passwordless-strategy
(8) https://media.fidoalliance.org/wp-content/uploads/2022/03/How-FIDO-Addresses-a-Full-Range-of-Use-Cases.pdf
(9) https://www.gi-de.com/en/payment/digital/authentication/convego-tap
(10) https://www.gi-de.com/en/identities/enterprise-security/hardware-based-authentication/starsign-key-fob

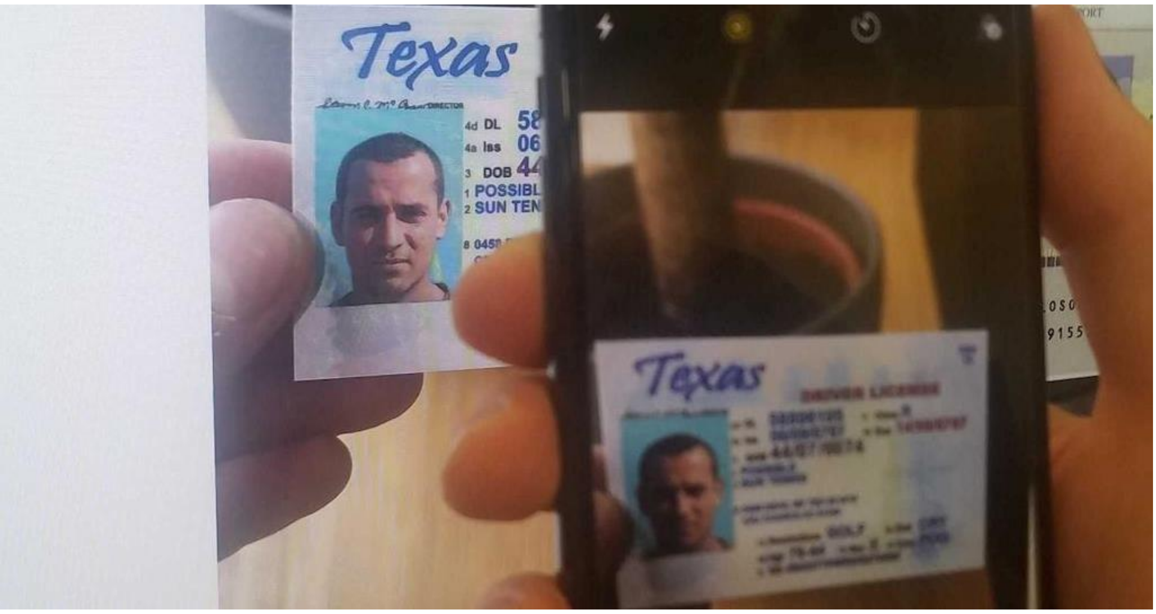
Organisation: Giesecke+Devrient
Name: David Tharm
Telephone number: +0401 988 133
Email: david.tharm@gi-de.com

7. ID R&D: How ID document liveness detection helps prevent fraud in digital onboarding

Without effective countermeasures, bad actors can present an ID document displayed on a screen instead of one that is "live" and in their physical possession.

The powerful sensors and processors common in today's mobile devices can be leveraged to conduct onboarding in a way that is cost-effective for organizations and convenient for users. The technologies let us verify identity without in-person supervision, but the process must include countermeasures for each vector of attack that a bad actor could attempt to intentionally misrepresent their identity.

The "presentation attack" is one such attack, where fraudsters falsely *present* biometric and other identity data that is not "live" and physically present during an onboarding process. For example, without facial liveness detection countermeasures a fraudster can use a digitally displayed image of someone else's face in place of their own selfie. In this way, a fraudster could open multiple fraudulent accounts and avoid accountability.



ID document-based presentation attacks

There is an analogous mode of presentation attack that prompts the need to perform ID document liveness detection. ID document liveness detection helps ensure that images of documents are not a "replay" displayed on a screen or printed on paper. There is an extensive identity proofing process behind the issuance of trusted government-issued ID documents, and so they can play an extremely useful role in verifying identity during digital onboarding, assuming the validity of the documents and their presentation can be validated.

While document security features help prevent the use of a "fake ID", preventing document-based spoof attacks ensures that the ID presented is *live*; that it is *physically present* and *in the possession* of the presenter. Otherwise, bad actors could source large volumes of digital images of ID documents–such as from the dark web–modify them, and then use them to apply for fraudulent accounts at scale.

"Portrait substitution" is yet another related threat. A fraudster might present the ID document with an image of a different face placed over the original portrait. Without countermeasures, a fraudster could use an ID with a substituted portrait for account applications, perhaps while also spoofing the live selfie. By combining multiple presentation attacks, bad actors can be even more effective at fraud.

ID document liveness detection is an important enhancement to digital onboarding processes

While ID document liveness detection is effective as countermeasure on its own accord, there are benefits from a comprehensive approach to liveness. By ensuring that the face and the ID document are live, and the face on the ID document is genuine, there is greater trust in the identity data provided and the conclusions of the identity proofing.

With greater trust in the security of the onboarding process, the user can be permitted to make higher-value transactions, be granted higher credit limits, or be granted access to more data.

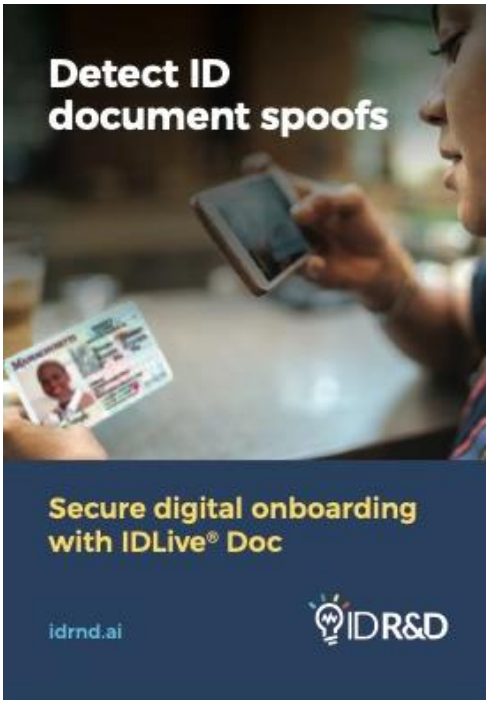
Liveness techniques and technology – security without negative UX impact is key
The impact of attack countermeasures should be as transparent and as effortless as possible for honest customers in terms of user experience. A process that takes too much time or causes false-reject errors will drive customers away from digital onboarding or to a competitive service. Solutions that require user interaction, video capture, lots of waiting time, or large app downloads can all degrade the user experience.

Technologies applied to achieve frictionless spoof detection vary, but there are analogies between face and ID document liveness detection, and several techniques proven most effective for facial liveness detection can also be applied to ID document liveness. For example, an algorithm that effectively detects a digital screen regardless of the subject of the image can be effective for both faces and for documents.

Presentation attacks	Face	ID Document
Printed spoof	Selfie taken of facial image printed on paper	Image taken of ID document printed on paper
Digital spoof	Selfie taken of facial image displayed on a digital screen	Image taken of ID document displayed on a digital screen
Mask; portrait substitution	Selfie taken of a face while wearing a 2D or 3D mask; paper, plastic, composite, etc.	Image taken of ID document with paper image of face overlain upon the genuine portrait on the document

ID document liveness detection is essential for secure digital onboarding
As adoption of digital onboarding grows, fraudsters will continue to try to attempt to exploit perceived security gaps. ID documents play such an essential role in identity proofing, and so spoofing of ID documents presents a serious threat to digital onboarding integrity where reliable countermeasures are not in place. But data shows that machines are now better than humans at recognizing faces and at detecting facial spoof attempts. ID document liveness techniques leverage many of the same approaches and can be applied as an important and complementary fraud countermeasure without adding user friction, enabling higher-value transactions and other benefits for customers.

Organisation: ID R&D
Name: David Benini
Telephone number: +1 617 306 5086
Email: david.benini@idrnd.net


Detect ID document spoofs
Secure digital onboarding with IDLive® Doc
idrnd.ai
ID R&D

8. InnoValor/ReadID: Balancing AI probability and crypto certainty in identity verification

The dilemma of artificial intelligence

Biometrics is under scrutiny, especially with respect to face recognition and liveness detection. On the one hand it has made tremendous progress using improved artificial intelligence (AI) and machine learning (ML) technology, making it fit for use in many situations. On the other hand, intrinsically linked to AI and ML, it is unclear how accurate it is and whether or not the results are biased with respect to ethnicity, demographics or gender. Also, deep fakes and morphing have entered the stage. In a different way this also holds for optical identity document verification based on AI and ML: it is still unclear how reliable its verification performance is and how well the algorithms are trained. With no certification in place, statements on its reliability are hard to validate. Experiments show that often optical verification technologies can be spoofed easily.

Summarising, AI in IDV faces a number of challenges:

- No certification for optical document verification;
- Limited availability of training data, needed for face verification and document verification;
- AI and ML are intrinsically not transparent in their results;
- Training in the wrong way creates bias – as long as you are a white male person of about thirty years old, you're fine.

Document verification and face verification are two cornerstones of remote identity verification: the logical approach to identity verification is to prove that a genuine person is holding his or her genuine identity document. But if both steps are based on AI and ML techniques that are not certified nor benchmarked, to what extent can we trust the outcomes? Does this make the scrutiny towards biometric identity verification justified?

We think it does. But that does not mean automated identity verification cannot be done reliably.

Improving certainty with cryptography

No identity verification step can be done with 100% certainty. But important components in the process can, improving the overall reliability tremendously: chipped identity documents can be proven valid. This chip is standardised as part of Doc 9303, Machine Readable Travel Documents, by ICAO (part of the United Nations). The information on the chip is digitally signed by the issuing country and has protection against cloning. Complex cryptography is needed to verify the authenticity of and information on the chip. It provides a smart and simple way to verify the authenticity of the identity document (passive and active authentication). It can also detect if a chip was copied. In this way we can guarantee that a document has not been tampered with, is not copied, and was issued by a specific country. This does not require additional hardware; any modern smartphone will do.

The data inside the chip includes the full name, date of birth, nationality and gender. In addition, it contains the original high-resolution face image of the holder. And this is great, as it is a second means to improve the reliability of identity verification. Compare the two face images in figure 1. The image to the left is read directly from the chip. It is in full colour without watermarks. The picture on the right is obtained using a high quality camera from a smartphone. The quality difference is obvious, and will even be bigger when the camera quality is less, non-ideal lighting conditions or glare on the document. Cropping a good-quality face image for a small identity card or driving license is an even more daunting task.

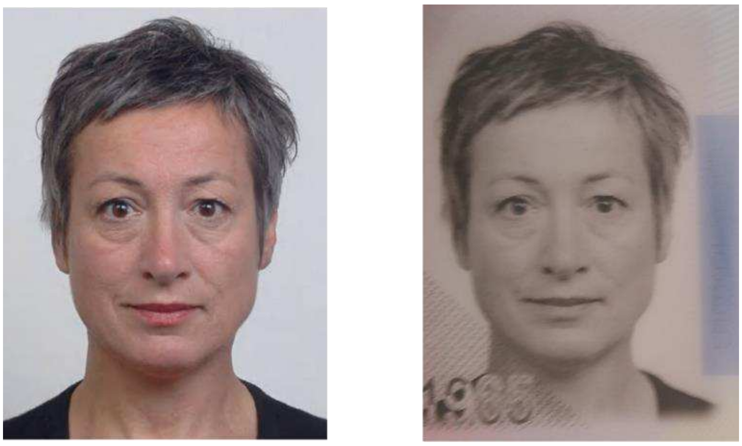


Figure 4. Face image read from the chip (left) and captured from the data page (right).

The face image extracted from the chip (which cannot be manipulated as it is cryptographically signed by the issuing country) provides an optimal starting point for face verification. From our partners we know that they can raise the threshold substantially (i.e., over 20 times better performance) when using the chip image over the cropped image taken from the picture, without reducing conversion! Increased quality does not come at a price. Nobody can guarantee correctness, but we can strongly improve the identity verification reliability.

The way forward for identity verification

Despite the current controversies concerning bias and quality of biometrics, there is no need to take a step back in time to video verification or the like. These techniques are costly, intrusive, do not scale, and, in the end, are really unreliable. Taking the cryptographic certainty of chipped identity documents as a starting point and using the face image from the chip for face verification on top of that reduces the uncertainty enormously. You are certain the document is not fraudulent, has not been tampered with and you are much more certain the holder is present in the verification. Often, improved security comes at the price of lower usability or reduced conversion. This is not the case. Our customers have shown that conversion of over 95% can be obtained following this approach.

Even more so, in many use cases you can stick to the document verification only. Take mobile app activation for internet banking. The KYC process was already done when opening the bank account, but the bank needs to ascertain the (new) phone is linked to the bank account holder. This can be done automatically using a chipped identity document with 100% certainty. Similarly, when resetting a second factor for authentication of an employee can be done reliably.

The fact that this is the way forward is confirmed by many regulatory bodies that are either promoting this approach (HM Land Registry and Good Practice Guide 45 in the UK, FINMA in Switzerland), imposing it (Austrian FMA) or embracing it (UK Home Office, Bank, Qualified Digital Signature Issuers). If parts of the identity proofing can be done in a 100% correct manner, without compromising performance, why settle for less? The combination of smart face verification with NFC-based biometric passport has proven to create trusted identity verification.

Organisation: InnoValor/ReadID
Name: Wil Janssen / Maarten Wegdam
Telephone number: +3 162 240 3433
Email: wil.janssen@innovalor.nl

9. Innovatrics: How to enhance passive liveness detection for greater accuracy and improved customer satisfaction

Until now, most algorithms have applied active liveness detection (ALD) to ensure that fraudsters can't gain access to banking and other accounts via printed or digital images. Activity detectors follow eye movements, but they also make the login process somewhat cumbersome, obstructed by different variables such as eyeglasses, poor camera quality, or other technical errors. As with any service technology, the use of facial recognition for onboarding and digital account enrollment stands or falls on customer experience. With ALD, the dropoff of potential customers can be anywhere between 20 to over 70 percent, depending on the method used. The largest drop-offs are seen with interactive checks such as video calls. This means a loss of a significant part of potential customers in enterprise settings.

The solution the industry offers to make operations smoother, faster, and more accurate is passive liveness detection (PLD). Passive liveness detection doesn't require user interaction and provides a better customer experience. Let's dig a little deeper into how this technology works, and what benefit it has for the end-user.

Current liveness detection models in place

Face verification determines that the person in front of the camera corresponds to another face that may already be registered. Since no physical contact is required, this ensures the smooth operation of facilities with access controls during closing hours or at night. Businesses implementing digital user ID can avoid bottlenecks at entrances as access to the premises is seamless and doesn't require staff to be present. For example, for gyms, it is possible to provide secure access to members even outside of day hours. This gives customers the freedom to work out whenever they want—something that can easily be replicated in other industries.

Liveness detection can determine whether the face is real or an object, such as a photograph, a 3D mask, or a cut-out mask. The currently applied software solutions work with two types of activity detection: active or passive.

How passive liveness detection yields better results

Passive liveness detection works with a single snapshot of a person taken on a digital device and does not require any user interaction. With most systems, a user receives a registration link allowing complete remote onboarding. The biometric template is generated and stored in the database throughout this process. An algorithm then identifies faces via a video stream and matches them against the recorded data. This allows a more streamlined and effortless experience for the end-user. Any company using digital onboarding, such as car driver registration, e-Visa issuance, employee registration, or client account onboarding, aiming to improve their customer experience can benefit from exchanging their current liveness detection with passive liveness detection (PLD).

A PLD-optimized algorithm uses image recognition and deep learning techniques to understand even the tiniest differences between a real face and an image, hence, a fake. The algorithms' training set contains multiple different spoof techniques like printed photographs, printed masks, 3D masks, and screenshots taken on a mobile selfie camera or PC webcam.

Nonetheless, passive liveness detection is only accurate, reliable, and valuable when executed on high-quality images. When algorithms receive low-quality images, they are prone to two types of errors. In one case, the neural networks find it's probably not a spoof and give access to an unauthorized person. In the other case, the image is genuine, but the system deems it fake and denies entry. The vast majority of images where the system has problems detecting the forgeries are of poor quality, e.g., poor resolution or lighting. Therefore, only an algorithm trained to recognize the quality of facial images, weed out low-quality photos, and identify typical fakes can provide consistent and reliable results.

A multimodal approach to defying spoofs

The main passive liveness algorithm is augmented by several approaches that increase the accuracy of passive liveness while keeping the user experience unchanged.
Images displayed on a screen exhibit the "moiré effect"—those blurry lines you often see when you take a picture of your screen with your smartphone. Once the algorithm starts to discern the moiré patterns in the image, it detects

that images above a certain sharpness threshold are all fake, which is a reliable way to detect fraud with digital images.

There is another dimension that the passive liveness algorithm must detect: the “frame effect”. Fraudsters could use an enlarged face frame with lower resolution and attack via printed images or a phone display, so the algorithm would not detect the moiré effect. However, using an “in-scene face analysis” in this case, the system can see the background and check whether the person fits into the scene or is simply added to it, as would be the case with a photo or display image.

How we improved the accuracy of PLD

If we allow poor-quality images into the database, the neural network has trouble distinguishing faces. These are borderline cases, but we need to understand them to minimize the chances of failure to make biometric technology secure.

Therefore, an algorithm first cuts out a certain percentage of the images with poor quality. They will quickly see that the system’s accuracy increases immensely when detecting liveness. Therefore by weeding out the poor-quality images, the accuracy increases without sacrificing any aspect of the customer experience.

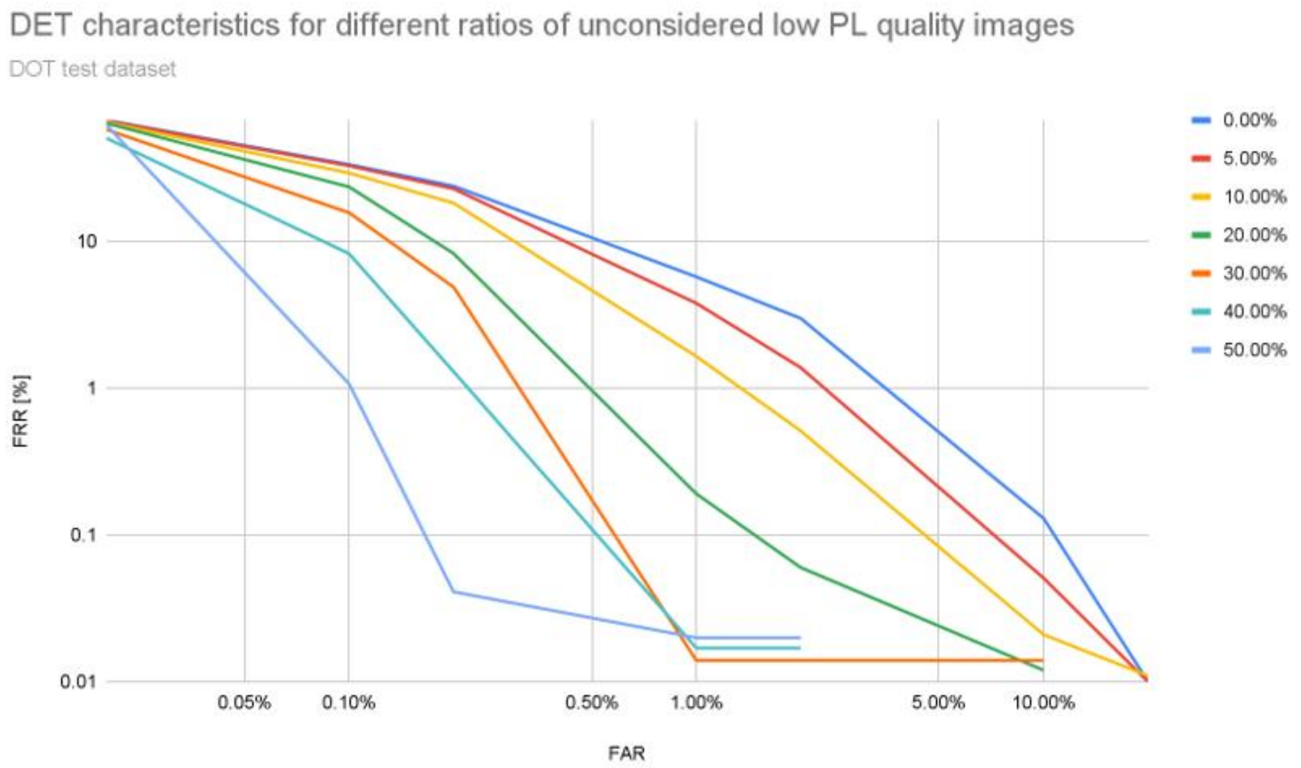
The algorithm needs to immediately inform the presenting person that their image is low quality by giving feedback such as “image too dark, or image not centered”. This way, the customer can try again and not be surprised afterward by having to repeat the entire process. Most significantly, this type of real-time feedback combined with auto-capture of a high-quality selfie increases both user satisfaction and quality of the liveness detection.

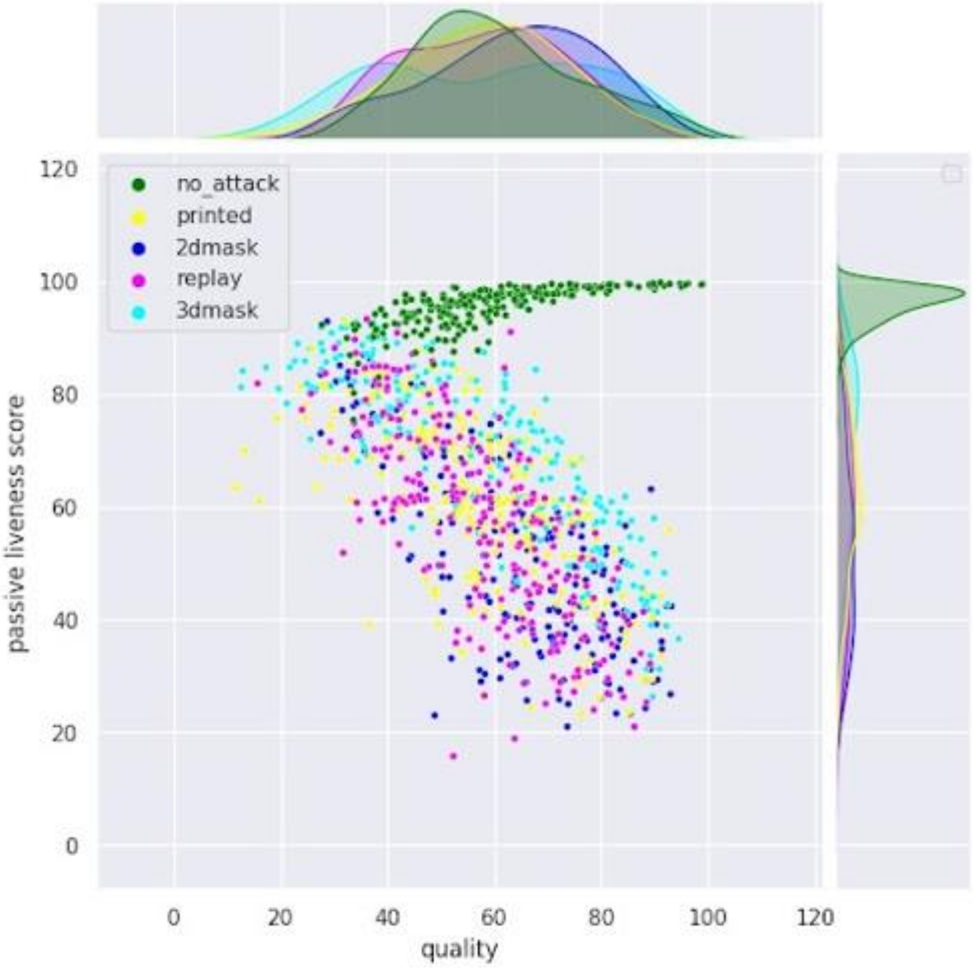
Benefits for the end-user

With the help of PLD, the customer receives feedback on where the problem lies and what they need to improve. Because the end users get clear feedback on what they should do to improve the quality of the images, the likelihood of a failed onboarding process and longer onboarding times due to errors decreases. Our studies have shown that PLD can decrease the liveness detection to one second, while current active liveness detection requires 6 seconds or more.

However, onboarding teams can additionally do a manual review of images in a small area as needed if the algorithm is not sure if the image is alive or not.

Companies using Face ID do not need to change processes or buy new software to combat fraud—they only need additional filtering with PLD. The passive liveness test required for banking, finance, and telecommunications can thus easily and cost-effectively become more reliable and accurate, ultimately leading to a significantly lower number of counterfeits. From airports to coworking spaces, passive liveness can help resolve some of the notorious issues that were only aggravated by the pandemic. A remarkable customer experience has become critical to the sustained growth of any business in any industry. In a world where customers have the power, not the sellers, the need for new technologies, and constant improvement, is immense.





Organisation: Innovatrics
Name: Marian Beszedes
Telephone number: +421 2 2071 4056
Email: roman.sevec@innovatrics.com

10. Onfido Ltd: The use of biometrics and other signals at onboarding for the prevention of fraud

It would come at no surprise for anyone reading this report that more and more businesses are relying on the progress of biometric technology to conduct their high-risk interactions online (e.g. account creation, account recovery). While it has never been easier to open a bank account online, the democratization of *deep fakes* and other image manipulation software has also rendered fraud pervasive. In fact, recent research found that the rate of sophisticated identity fraud increased 57% in 2021 when compared to the previous year. Failing to defend against these attacks can have significant consequences, leading to mass revenue losses and damage to a company's brand reputation.

Years of biometrics fraud expertise lead us to believe that most of the fraud attempted at account-creation time could be broadly put into two categories; we called them "large-scale attacks" and "targeted attacks".

The first category, large-scale attacks, typically occur when there is a direct benefit of opening as many accounts as possible. A prime example we have encountered is when businesses offer a sign-up bonus for any new incoming customer. The bonus itself can take many forms but, mostly it will equate to some sort of monetary reward.

In order to exploit the sign-up bonus and maximize their gains, fraudsters are incentivized to create as many accounts as possible, as fast as possible. Unsurprisingly then, they will resort to using automated scripts to perform the various fraud tasks (e.g. face swapping). This typically results in fraud attempts that are generally of low quality, but coming in at colossal rates. In fact, we have seen fraud rates as high as 75% during a recent sign-up bonus campaign of one of our customers. That is, 3 in 4 account creation attempts were fraudulent!

Large-scale attacks can typically be detected with a collection of preventive methods. The most common is the use of 1-n face matching. That is, for any new potential account creation, we look in the database if this very individual has not already opened an account before. Similar image similarity techniques can be conducted on the image of the identity document to check if the same image of a document has been used and re-used. These methods are effective at catching the low-effort, large-scale frauds.

The other type of attack, that we call "targeted" is on the complete other side of the spectrum: they tend to be lower in volume, but higher in quality. Money laundering is a typical use-case of a targeted attack, where it is in the interest of the fraudster to pay a little extra time crafting a convincing fraud. In this scenario, the attacker can go as far as stealing the ID document of the victim or even coercing the victim into performing the IDV flow.

When the victim is not physically present, the fraudster will have to rely on a *spoof artefact* to impersonate the identity. A popular spoof artefact is a custom-crafted 2D or 3D mask of the victim. A cheaper option remains simply to display a photo of the victim on a monitor.

Targeted attacks are typically harder to detect because of their level of sophistication. Should it be said, it is illusory to think that machine learning and AI is, at time of writing, robust enough to catch *all* fraud (especially spoof artefacts that have never been seen before) all whilst ensuring the high genuine pass rates that businesses require today. Robust mitigation strategies can however be put into place if we cleverly combine engineering expertise and AI expertise. In this regime, missed fraud can be quickly identified, labelled and used for machine learning. A handful of samples are enough to update the algorithm, show its increased effectiveness and deploy it to production.

So far, we have only mentioned the protections that the back-end can offer; irrespective of the large-scale or targeted nature of the fraud. But the front-end should not be left out of the discussion. For businesses, finding the right balance between fraud protection and user experience (UX) is very important, as 43% of customers admit they would abandon a sign-up process if their expectations aren't met at the first impression. So the goal for companies like ours is to maximise the ratio of fraud fiction by genuine friction. A given UX will offer a certain level of friction for genuine users, but will also impose a certain level of friction for fraudsters.

Photo or Selfie based experiences offer the lowest friction from a user experience perspective, so fraudsters may also assume they offer minimal defence. However advances in AI, mean that sophisticated passive models include texture analysis and other targeted features that provide very high fraud protection.

Where a business wants to provide extra protection against fraud, we believe that a well crafted video-based, active experience can bring the best ratio of fraud-to-genuine friction. The very nature of video makes large scale attacks almost void (video automation software is still hard to come by and increases compute requirements) and seriously complicates the life of a targeted fraudster.

Ultimately businesses need to craft a user experience that for them provides the right balance between reducing fraud and friction. The choices they will make are very much dependent on factors such whether they are regulated or not or perhaps if they are incentivising customer adoption and therefore potentially also attracting fraudsters as well. If this is the case they should consider putting in place additional mitigation measures such as 1-n matching at the point of onboarding.

Regardless of this, Onfido (and no doubt other biometrics vendors) continue to invest so that we can provide protection against both large-scale and targeted attacks. We have spent years designing the machine learning algorithms, user experience and other infrastructure to be able to respond quickly to fraud. We offer both a photo-based and video-based experience to suit customer's needs.

Organisation: Onfido Ltd
Name: Sarah Munro
Telephone Number: +44 (0) 7930358401
Email: sarah.munro@onfido.com

11. Paravision: Future borders are digital: There are two sides to this coin

e-Gates and kiosks utilising ePassports and facial recognition have long been accepted by passengers at border control and immigration. Increasingly, the same technology is used to reduce bottlenecks in outbound airport traffic.

The success of these initiatives has prompted many governments to initiate and accelerate digital-first programmes. The UK government, for example, published its 2025 UK Border Strategy and has inaugurated the Border Vision Advisory Group (BVAG) to help deliver on this strategy, while the European Union has actively been developing its Entry Exit System (EES) and Advanced Travel Information Authorisation System (ETIAS).

The Global Guidelines for Safe & Seamless Traveller Journey (SSTJ) by the World Travel & Tourism Council (WTTC) paints a vision where passengers no longer need to stop multiple times during their journey to verify their documents and identity; they need to undertake this exercise once at the start of their journey, using their mobile phone, unlocking a fast, frictionless experience that begins at home.

The successful implementation of a frictionless digital border strategy must begin well before the physical border. The flipside to the coin of expedited, simplified passenger travel is the exporting of the border: obtaining accurate data about a passenger and making decisions about that passenger as early as possible, ideally before they start their journey. This allows border agencies to deal with issues less expensively before travellers arrive at the borders, and enables greater flexibility in assisting them at the border itself.

The good news is that there have been recent technological advances that allow what would not have been possible a mere few years ago. Significant amongst these are:

1. **Advances in facial recognition accuracy.** As demonstrated by ongoing testing by the US Government's National Institute of Standards and Technology (NIST), the accuracy of facial recognition has advanced at an impressive rate. As NIST conducts its ongoing Facial Recognition Vendor Tests, accuracy rates have continued to improve (in some cases, with five-fold reductions in errors since 2018). To put this in context, in February of this year, NIST published its second report on facial recognition for paperless travel, in which leading providers achieved better than 99.9% matching accuracy for airplane boarding, ranking #1 in the U.S. across all metrics. This level of accuracy was unheard of a few short years ago.

2. **Ubiquity of NFC enabled smartphones.** The NFC capability is now available across most Android and Apple mobile devices, allowing governments to validate the authenticity of a passenger's travel documents remotely, from a distance and before travel, using nothing more than their mobile phone and ePassport. Additionally, it allows the accurate capture of the passenger's biographic data from the document's chip and, importantly, a face image that has been assessed by the issuing government to comply with the International Civil Aviation Organization (ICAO) photograph guidelines. With ICAO's recent publication of the standard for a Digital Travel Credential (DTC), there is also the option of storing a derivation of the ePassport's chip directly on the passenger's mobile phone.

In addition to being able to validate the document and accurately capture the passenger's details from it, the combination of the above two mentioned advents allows two key benefits specific to facial recognition:

1. Verifying document ownership. Utilising highly accurate facial recognition to match the ICAO compliant face image obtained from the chip against a liveness-verified selfie image determines that the applicant is using their travel document and not somebody else's.

2. Capturing a high-quality ICAO-compliant reference image. Obtaining the ICAO-compliant enrolment image from the chip of the ePassport allows the construction of high-quality reference datasets that can be used in passenger facilitation solutions when the passenger physically arrives at a border.

The two sides of this coin, therefore, can broadly be categorised as:

1. Digitally Exporting the Border Away from the Physical Border

The benefits of exporting the border are significant:

Reduced Friction and Cost

Reducing friction and cost in interacting with travellers, and a significantly enhanced, expedited, and improved customer experience by enabling self-service digital channels, reducing the reliance on costly physical Visa application centres (VAC).

Enhanced Security through Early Capture of Data

Capturing accurate, secure, and verified data, including biometrics, earlier, before the visitor arrives at the border and leaves their country of origin. This can be undertaken via pre-enrolment for any number of digital programmes, including:

- applying for an eVisa
- registering for an electronic travel authorisation (eTA)
- enrolling into a trusted traveller border facilitation programme for returning citizens or beneficiaries of a free travel zone.

Digital onboarding into relevant programmes has progressed to the point where Digital Permissions are becoming the norm. Physical tokens and vignettes will no longer be required to assert rights and statuses, and officials need only access your digital records.

2. Digital Transformation of the Physical Border

Onboarding into the appropriate digital programme or channel before a passenger arrives at a physical border significantly enhances the flexibility in processing arrivals. Advance analysis of biographic and biometric data and cross-referencing against the appropriate datasets allows maximum flexibility in granting permissions and segmenting passengers.

Whilst eGates have become common at most countries 'borders, they will increasingly be augmented by additional channels accorded to returning citizens, citizens of other nations participating in a freedom of movement treaty, and optionally eTA applicants or travellers enrolled in a trusted traveller scheme. Expedited and freer-flowing channels can consist of biometric corridors, where passengers can be matched against lists of pre-enrolled and pre-approved applicants. Digital permissions coupled with the ability to process ePassport DTCs can minimise the number of times passengers need to have their physical documents examined and their identities verified.

Collaboration is Vital

It's crucial to recognise that no organisation holds all the answers. To successfully meet the challenges of delivering the border of tomorrow, we must actively seek collaboration between end users, integrators, and best-of-breed technology vendors in order to couple suitable expertise in machine learning with thoughtful visions of future borders.

Future borders are digital and frictionless, and the benefits can be realised today.

Organisation: Paravision
Name: Carl Gohringer
Telephone number: +1 917 893 0037
Email: carl@paravision.ai

12. Reason360: Biometrics x Service

The delivery of customer service occupies a great deal of resources in many consumer-facing organisations – especially in those with enduring, account-like relationships with their clients. When such relationships are involved, a considerable part of the challenge in delivering great service revolves around identity – both from the customer's perspective and that of the organisation.

Digital identity and biometrics can help both parties with this challenge. Done well, organisations can save money and reduce risk, and customers can save time and feel confident in the security of their information. But these outcomes are not a given: much better results arise when identity elements are connected to customer service with careful attention to the details, to ensure that both the organisation and the customer are getting the most from the customer service experience.

When designing identity mechanisms for customer service, some processes are well understood. The assessment of levels of security for different types of service delivery usually involves bringing together the right parts of the organisation to agree on a model. This can be challenging – in part because of the radically different perspectives and language used in different functional siloes – but it is not unfamiliar to most organisations. However, navigating these conversations with the subtle statistical variations associated with biometric technology adds a new level of complexity to the dialogue, and it often helps to have independent expertise in the room to ensure all parties reach both a common understanding and the best possible outcome.

But beyond this, some intersections between identity and service can present more thorny problems. Often these problems come to life with scale: an issue mildly impairing the experience of 5% of customers may be overlooked in a small organisation, but at large scale may present a considerable improvement opportunity worth chasing.

Consider, for instance, the basic flow of much service delivery, especially online: customer logs in, selects desired service, performs action, ends interaction. Which security level should we choose for the login? We don't yet know what service the customer wants – they choose that at the next step. Maybe we aim for the lowest level, knowing we can always step up later. But what if 40% of people need the step-up? Now we have quite a disjointed identity experience for a significant portion of our customers.

Faced with this, maybe we would consider re-ordering the sequence to one commonly used in telephone service: customer selects desired service, logs in, performs action, ends interaction. Now we know what the customer wants, so we can choose exactly the right security level to hit in the login process. And for customers arriving to receive service having found it using a search mechanism – all too common! – their experience is much neater. But now we have a new problem: for the other customers who start from scratch it's impossible to present a menu of services for each –we don't know who the customer is, so we can't do any tailoring to individual circumstances.

These challenges are compounded in modern service delivery that leans on adjacent technologies such as machine understanding of natural language. Just as in biometrics, great strides have been made in the performance of such systems. But, just as in biometrics, they are not perfect. Some portion of the time our service delivery machine will get things wrong, and our customer will be asked to verify their identity based on what the machine *thought* they wanted, when in fact the customer needed to be verified to a much higher level.

Of course, there is the possibility that the customer too can make mistakes with similar results. A type of service might be mistakenly identified, leading to an incorrect assessment of security level, or an identity might be inadvertently asserted, leading to attempts to verify details – or attempt biometrics matching – against the wrong person. ('Uncommon!' you might think, but it happens surprisingly frequently.)

So how should these various options, challenges, opportunities for mistakes, and potential to add value to all parties be traded off, and done so mindful of other organisational issues such as digital identity reuse, technology investment, availability of resources, and capacity for change? How can options be generated, and decisions made, that get the best outcome both in today's circumstances and those reasonably foreseeable?

One helpful yardstick is time. The overall time expended, across all relevant parts of the experiences delivered, averaged out across all the various scenarios, and considered for both customers and the organisation, can form a useful way to think about the ramifications of different options and choices across the impacted stakeholders.
Determining all the necessary input factors and assessing likely outcomes is not a trivial exercise, but not impossible either; and provides concrete data that supports decision-making and education of executive stakeholders about the trade-offs being made on their behalf. This should not be underestimated in importance: justification of decisions in service delivery is all-too-often based on gut, which commonly leads to change based on whim rather than evidence.

It's possible to do all this work alone, of course – internally, with the people already tasked with thinking deeply about service improvement. But it is often the case that additional expertise in the field at hand – *'biometrics × service'* if you will – can help bring teams together, provide counsel, and offer concrete insights to make it easier and quicker to deliver excellent experiences for customers and greater benefits for the organisation.

While the opportunities for adding value through responsible use of biometrics in service delivery are enormous, getting great outcomes is not easy. With careful thought about the experiences our customers have, the challenges that they will have during their different journeys as customers, and the organisational context in which service is delivered, great outcomes can be brought to life.

Organisation: Reason360
Name: Brett Feldon
Telephone number: +61 457 817 326
Email: brett@reason360.com.au

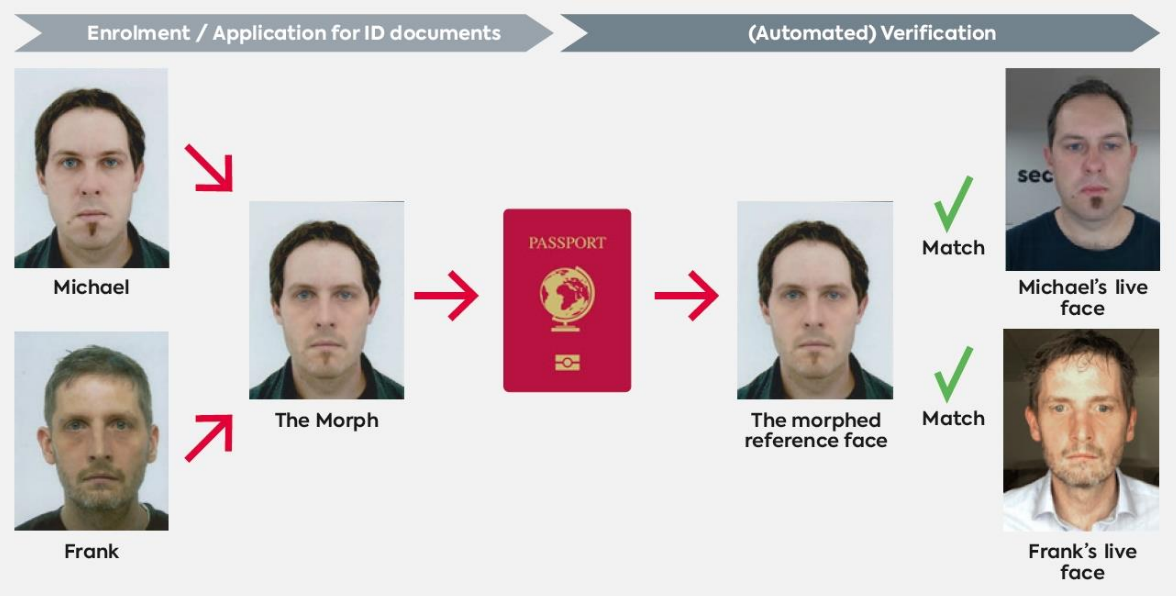
13. secunet Security Networks AG: Man or morph?

Introduction

Biometrics and facial recognition have made border control more efficient and secure. However, there are types of fraud that still pose a challenge, both for border control officers and automated border control systems. These notably include so-called morphing attacks, in which fraudsters make use of ID photos assembled from the facial images of more than one person. Now there is an algorithm that can reliably recognise morphs like these.

Fictional impostors Michael and Frank use powerful image editing software to merge their biometric passport photos into a single image. The result is an image that resembles both men. Michael then uses this manipulated image for his new passport. Superficially, he's recognisable as the person in the picture, so the officials don't suspect anything when they issue the passport. Frank then goes to the airport with the new identity document. As the morph is executed well, facial recognition software – or the officer at the border control counter – mistakenly recognises him as the person in the picture, thus identifying him as Michael, the passport holder. In the worst-case scenario described here, Frank can therefore cross the border under a false identity.

The impostors in this story are fictional, but the crime is very real. Public authorities from various countries, including the Slovenian Police Force, for instance, have already reported scams involving morphing. The likely reason for this prevalence is that morphs are easy to implement. They don't require any special expertise; a commercial image editing program and a little talent are enough.



THIS IS HOW A MORPHING ATTACK WORKS.

The human security factor

Reports of detected morphs show that perpetrators predominantly target automated border control systems. However, this type of fraud also poses a challenge to humans. Research shows that, on average, people only recognise about 60 per cent of the morphs they are shown compared to a trustworthy image. However, people who take part in such a test seem to perform better and better in the course of the examination. So those who specifically deal with the subject sometimes recognise more morphs later on.

Supervised registration

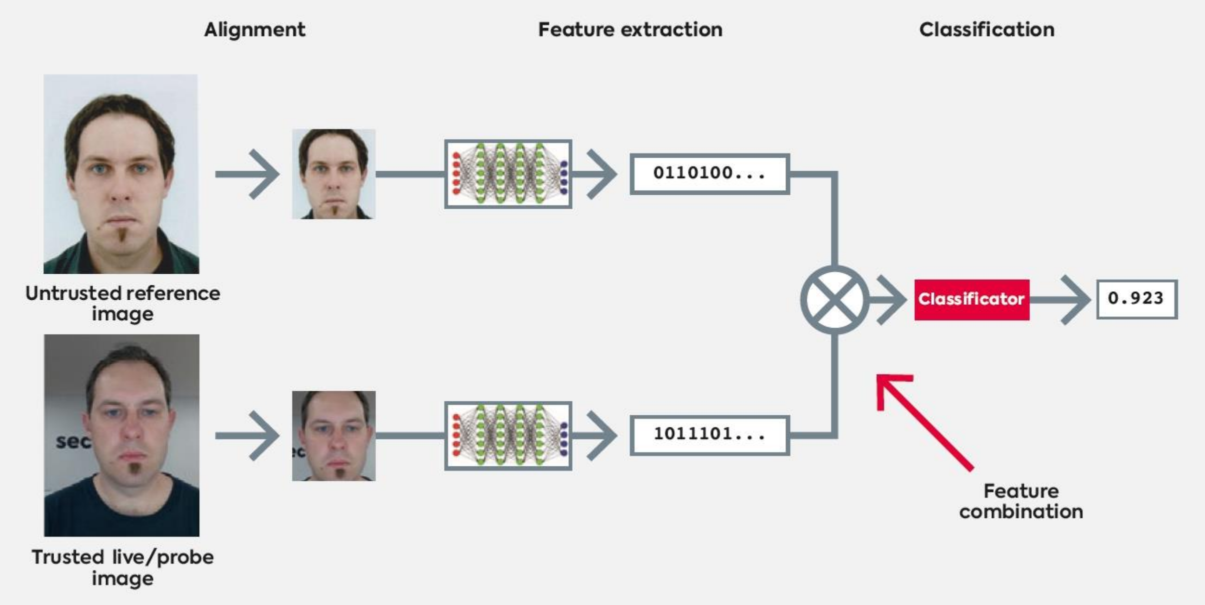
Training border control officers is therefore one way to deal with the morphing problem. Another is so-called "live enrolment". In order to prevent the forgery of personal images in identity documents at the issuing stage, authorities could no longer consider photos provided by applicants themselves. Instead, only images taken directly on-site under the supervision of the authorities would be acceptable. This would ensure that no more morphs find their way into identity documents. The problem with this is that even if all European countries were to agree on such a procedure in the future, there will probably always be countries around the world that accept images taken at home for official documents. Consequently, live enrolment alone will never truly overcome the morphing challenge.

Nevertheless, the coming European Entry / Exit System (EES) is expected to herald improvements in this area. When entering Schengen countries in the future, third-country nationals will have to register with four fingerprints and a facial image – directly at the border via live enrolment. When these individuals re-enter the Schengen area, not only the image in their identity document will be available, but also a trusted facial image in the EES database. If high-quality equipment, like the height-adjustable facial image camera secunet easytower, has been used for image capture, the result will be ideal for EES-compliant border control.

Smarter software

Another security measure is software algorithms that recognise facial morphs during automated border control. secunet's experts have been working on morphing attack detection (MAD) for several years. Strictly speaking, we are talking about "differential" MAD in this context, whereby a facial image is checked through comparison with a second, trusted image. A trusted data source is always present in the automated border control process, because this process always involves capturing a live image. This image is then compared to the image in the traveller's electronic identity document. At this point, the algorithm intervenes and detects any discrepancies. A vital prerequisite is that the live image meets high quality standards.

In partnership with the Darmstadt University of Applied Sciences, secunet has now developed a new, even more effective algorithm[1], which has already proven itself to be suitable for everyday use. As with other algorithms like this, a threshold value can be used to fine-tune the algorithm. If set to a false positive rate of 2% (meaning two out of every hundred facial images are misclassified as morphs and have to be manually verified), the algorithm will spot 85–88% of all genuine morphs. This is very good compared to both human test subjects and previous algorithms.



THIS IS HOW MORPHING ATTACK DETECTION OPERATES.

Morphing detection: today and tomorrow

The new algorithm has allowed MAD to take a decisive step forward within a very short period of time. Despite this progress, morphing attacks will likely remain a challenge for the foreseeable future. The algorithm must therefore be continually improved, extended and retrained to further reduce error rates going forward. In addition, software-based MAD can only be part of the solution; its other cornerstones are live enrolment and the training of border control staff. After all, combatting morphing is as much about people as it is about machines.

[1] The methodology was first described in the following publication and was subsequently developed further by secunet: U. Scherhag, C. Rathgeb, J. Merkle, C. Busch: "Deep Face Representations for Differential Morphing Attack Detection", in IEEE Transactions on Information Forensics and Security (2020).

Organisation: secunet Security Networks AG
Name: Alina Kadelka/ Michael Schwaiger
Telephone number: + 49 (201) 5454 3888
Email: alina.kadelka@secunet.com

14. Secure Logistics B.V: A trusted digital identity combined with an on-card biometrics solution

Facial Recognition on Card solution

With digitalization increasing at a high speed throughout all industries, a trusted digital identity is key to success. It requires a proper verification and registration of one's identity for it to be authenticated, be it human-to-machine or machine-to-machine.

For more security demanding environments however, the digital identity can be enriched with biometric data. Naturally provided the applicable laws and regulations are complied with. However, privacy is always a challenge: where do you store this privacy-sensitive data and how do you prevent its misuse? Facial recognition on a card is a solution. No storage of photos in a central database, but only a biometric template on the chip of a smart card. The user always has a say in where he or she shares this data. The facial recognition on card solution is suitable for both physical as well as digital environments. Thanks to the 1-to-1 comparison instead of the 1-to-many comparison, the process is fast, secure and privacy friendly.

Why is this special?

Almost all biometric face verification techniques are based on a 1-to-many comparison. This creates the risk of data falling into the wrong hands and being misused. By placing the template on card and only verifying it at the time of presentation, a closed and secure process is created. The use of facial authentication for access to locations, systems and/or devices via the on-card technique is a so-called self-sovereign solution; the user decides where, with whom and when this template will be used.

To ensure a stable performance in in- and outdoor environments, the facial recognition on card solution has been extensively tested. Scenarios tested:

- Port areas with storms, salty rain, pollutants
- Different nationalities
- Person to be recognised from truck (angle camera), with face masks, safety helmets and goggles
- The speed of reading a file from a smart card (photo on card)
- Liveliness detection.

Why a card instead of a smartphone?

In contrast to e.g. biometrics of a phone, where multiple faces can be enrolled, the facial recognition on card solution only allows for one biometric template.

What are the benefits?

Facial recognition on card combined with a trusted digital identity, makes contactless biometrics possible in demanding in- and outdoor environments. For outdoor environments the location that has to secure the terrain, this means unmanned access gates in combination with 100% personal identification. For the user of the smart card with the biometric template, this means faster access to the site, without having to hand over a privacy-sensitive identity document.

Organisation: Secure Logistics B.V.
Name: Frank de Krou
Telephone number: +31 10 463 77 77
Email: fh@secure-logistics.nl

15. SISSA Integral Monitoring: Personalized biometric solutions: the importance of technology integration

If the COVID-19 pandemic taught all professionals involved in the security sector anything, it is to appreciate the benefits that contactless biometric technology has to offer today and in the years to come.
However, something that is just as essential to learn but, for some reason, has not been conveyed with the same success, is the importance of engaging the services offered by biometric (and non-biometric) technology integrators for the creation of fully customized solutions.

Customized solutions for particular challenges

A technology solutions integrator can improve the value chain and boost the return on investment of its customers by developing solutions that meet their specific needs, thus contributing to the fulfillment of their business objectives.

To this end, the offer of a high-level technology integrator must include the following five services:

1. Specialized consultancies

The starting point should be a risk analysis to identify the real needs of the organizations and, in this way, present solutions that generate value and return on investment through the integration of various innovation technologies.

2. Design and executive project

Afterwards, the technological solutions must be designed and projected through the elaboration of plans, diagrams and work plans that support and guarantee the success of the project to be developed.

3. Supply, installation and start-up

A high-level technological integrator must be capable of implementing and integrating different components (devices, platforms or applications) independently and from different brands to create unique solutions, which are fine-tuned in accordance with the standards established for the optimization of organization operations.

4. Managed Services

In addition to creating unique solutions from components of different brands, what gives value to a high-level technology integrator is its ability to monitor and manage the operation of the solutions supplied to provide comprehensive maintenance and make continuous improvements to maximize their life cycle, thus ensuring their proper operation and ensuring their proper coexistence with the pre-existing technology and infrastructure.

5. Training

Finally, a high-level integrator must enable organizations on the correct use of the solutions provided, training them for their free and responsible handling, allowing them to take full advantage of their benefits.

Integral services for turnkey projects

Although these services can be contracted separately, it is always recommended to do it in an integrated manner. In this way, the integrating company will be able to develop a turnkey project that, in addition to representing an economic saving for the contracting organization, will be executed with greater speed, will be better controlled and will have coherence and efficiency in each of its phases.

Integration of biometric and security solutions

Now, speaking specifically of biometrics in the security sector, technology integrators must have business alliances with the best manufacturers in the market that allow them to supply, implement and customize biometric solutions of last generation in terms of access control and people management.

These alliances will facilitate the work of the technology integrator when designing and implementing a solution that meets the specific needs of the organization in question, which could include anything from a biometric selfenrollment app (biometric check-in), to devices that allow automatic verification and authentication of documents or identification of people by contactless biometrics.

However, the work of a high-level technology integrator is not limited to the integration of solutions in a single area. These professionals must be able to integrate technological devices of different nature that can interact with each other and respond according to the characteristics, processes and business rules of each organization.
Among the different solutions that a high-level technological integrator must be able to integrate and make them coexist with each other, the following stand out:

- Video surveillance with analytics
- Pedestrian and vehicular access control
- Biometric identity management systems
- Automated and remote opening and closing of doors
- Physical perimeter security
- Alarm and fire detection

Organisation: SISSA Integral Monitoring
Name: Isaac Valencia Trejo
Telephone number: +52 55 1228 4507
Email: isaac.valencia@sissamx.com

16. SITA: Digital identity and travel

Frustrating, Fragmented, Fraught

For many years the Air Travel Industry campaigned for a digital transformation that would alleviate increasing pressures on infrastructure and resources caused by continued growth in international travel[1]. Industry and travellers needed everything about travel to be faster and more efficient.

Some evolution towards the vision of swift and seamless travel where your face is your passport has progressed within airports through the use of check-in kiosks, eGates, and other self-service options. However, important upstream and downstream parts of the journey are not joined up, causing gaps in the chain of trust between the various authorities involved in approving travel, as well as confusion, repetition and delays.

Authorities still check identity and documentation manually as part of passport and visa issuance, using processes that rely heavily on individuals' skills in comparing faces and in detecting fraudulent documents. Border control officers undertake further checks when people present at the busy physical border, but too often their critical work relies on systems holding biographic information of variable quality, supplied through various channels, and interpreted differently under different national, cultural and linguistic traditions.

From the moment someone commences their plan to travel internationally, critical information is collected separately by different authorities in different ways, and it is stored in different systems and formats. Similar information is collected for passport applications, visa applications, passenger declarations and landing cards, and it is often submitted directly by travellers themselves who are not experts in the relevant conventions, underlying data standards or checking processes.

Continuously supplying and capturing this information is cumbersome, and it is essential for travellers to safeguard all their critical documents proving who they are and what permissions they hold, for repeated inspection.

None of this became any easier with the introduction of new requirements related to COVID test results and vaccination certificates. Despite the need to drastically cut costs during the pandemic[2], more forms and manual checks were added for industry to manage, causing massive delays[3] and major inconvenience to passenger processing and operational schedules.

Reform

The pandemic massively accelerated digital transformation as the need to accurately identify people remotely for access to services became an imperative, and as the world embraced digital health credentials. Governments, companies and standards bodies have been working hard to create the next generation of self-service travel infrastructure, where our mobile phones are the remote control for an entire journey, in a new paradigm underpinned by digital identity.

Importantly for international travel, international standards have appeared for verifiable digital vaccination certificates[4], digital visas[5], and digital passports[6], connecting and providing integrity across the spectrum of processes involved in the travel continuum.

Mobile apps and digital wallets have changed how we engage with services. Today, we expect the convenience of access to services from our devices. We expect that we can easily prove who we are and what we are entitled to, without having to carry an abundance of paper documents or plastic cards. We expect that there is an app for all of this.

[1] See: ACI World publishes annual World Airport Traffic Report - ACI World

[2] See: Economic Impacts of COVID-19 on Civil Aviation (icao.int)

[3] See: Digitization needed for smooth restart of travel | Airlines. (iata.org)

[4] Eg: Digital documentation of COVID-19 certificates: vaccination status: web annex A: DDCC:VS core data dictionary, 27 August 2021 (who.int)

[5] See: Digital Travel Authorizations. (New).pdf (icao.int)

[6] See: ICAO-TR Digital Travel Credentials, Guiding Core Principles DTC (icao.int)

The Future of Travel

We are finally at the point where we can implement joined-up digital travel across the entire journey. Using digital credentials and mobile device-based capabilities including biometrics and liveness detection, our border, airport and airline authorities can accurately verify identity and authorise travel for many travellers remotely, and confirm that travellers hold a valid passport and a verifiable digital visa. By submitting their digital credentials to border and travel authorities directly, travellers can easily confirm their vaccination and health status.

Once credentials are verified a person can elect to seamlessly pass through all the usual airport and border processes using just their face as the token, replacing passports and boarding cards for the entire journey. Should someone lose their passport, the single most important item needed for international travel, they can produce an authoritative digital backup of it.

This digital travel model dramatically reduces the need to handle and verify physical documents, freeing up time for immigration and border officers to undertake higher-value investigative work. It strengthens assurance in relation to identity, nationality, health and travel authority, ensuring that decisions are based on reliable information about the right person, that has not been altered. It opens up end-to-end seamless travel and off-airport self-service opportunities, reducing the crisis of airport congestion with fast and accurate processing that commences before a traveller enters an airport.

The model requires careful consideration of security and privacy controls, planning of alternative options for travellers who prefer or require traditional airport processes, and thorough testing and monitoring of solution quality and performance. It will not be perfect for every person and every condition, but it radically improves the quality of information and self-service opportunities associated with international travel.

Using the unparalleled opportunities for identity assurance, coordinated service delivery and customer engagement that are now available with modern mobile apps and digital credentials, digital identity is enabling the digital travel transformation, delivering more robust information to travel authorities and improving the experience for travellers.

Organisation: SITA
Name: Paul Cross
Telephone number: +61 491 154 064
Email: paul.cross@sita.aero

17. Veridas & dasGate: How a facial biometric system provides access to a Spanish Football League

Access the stadium quickly, comfortably, and securely without carrying a physical or digital (QR code) season ticket by simply using their face. The aforementioned is the objective of the new access system implemented for the first time in the Spanish first division, La Liga, specifically at El Sadar - Stadium of C.A. Osasuna -.

Club Atlético Osasuna, using dasGate's technology, has installed its identity and access platform as an alternative to entering the stadium to improve the experience of people visiting El Sadar, cutting queuing time and removing tickets and membership cards.

To enable the new biometric access system, two steps are required: firstly, each user must complete a simple registration that can be easily carried out remotely in less than one minute through their cell phone by taking a picture of both the membership card and the ID card and taking a selfie; remote registration with identity verification *"From couch to stadium"*. Then, once the activation process is completed, which is valid for the whole season, the member will be able to arrive at the stadium without the need to carry the physical or digital season ticket. By simply bringing their face close to the small screen on the gates-placed turnstiles, they will be able to open the barrier and enter the stadium automatically. The system recognizes that the subscriber's face matches the registered one, and the turnstile will open automatically. The process of approaching the terminal and opening the barrier takes less than a second, generating a more comfortable and agile access to the stadium

Recently gone live in LaLiga official matches, this new access system, already placed at 8 areas of the Stadium and available for all members, showed that it can provide access to more than 20 people per minute. An unprecedented number and performance that generated an exceptional user experience, as well as providing both the club and LaLiga complete confidence that the people who were accessing were the season ticket holders, maximizing security.

What are the advantages of facial recognition?

- Speed: FR enabled access gates allow passage in less than a second, reducing queues and avoiding delays caused by people who cannot find their season ticket or take a long time to get it read by the QR or barcode reader
- Convenience: there is no need to carry anything to enter the stadium, neither the physical season ticket nor a digital ticket on a mobile phone. Attendants will only need their face to enter
- Security: the event organizer can be sure that everyone present in the venue has the necessary permits
- Compliance: additionally, this new biometric access system can comply with the General Data Protection Regulation and is endorsed by La Liga
- Voluntary: attendants will always be able to choose the traditional forms of access to the stadium, with facial recognition access being another option they can enjoy. Its use is voluntary and does not replace any other forms of access that will continue to be available
- Easy to use and inclusive: this additional option to access the stadium is friendly and easy to use for everyone. Users do not have to worry about changes in their clothes, the use of glasses, scarves or any other physical change.The system is trained to recognize humans accurately despite these changes in appearance.

This technology allows anyone to operate securely in the digital and physical world by simply being themselves. It is important that the engine is recognized by the National Institute of Standards and Technology (NIST) of the United States (the primary reference for evaluating this type of technology), and it has certified anti-spoofing and liveness detection technology (compliant with ISO and iBeta Level 2 evaluation). Since 2017, more than 60.000.000 biometric enrollments have been performed worldwide in diverse sectors such as banking, insurance, telcos, mobility, and public administration. The technology is deployed with thousands of daily accesses.

Moreover, following our commitment to privacy, regulation, and compliance, all personal data is processed under the subscriber's express consent and under the guidelines of the Spanish Data Protection Agency and applying security measures audited under official certifications. The implementation of this access solution for El Sadar has been subject to a Data Protection Impact Assessment (DPA) by an independent third party. Veridas has obtained the ISO 27001 certification for information security management systems and complies 100% with the General Data Protection Regulation, the Organic Law on Data Protection and Digital Rights Guarantees, the Spanish Data

Protection Agency guidelines, and the rest of the Spanish and European regulations. In addition, it has joined the AEPD's Digital Pact, an initiative that works to create a healthy digital environment free of content that threatens the integrity and honor of individuals.

Organisation: Veridas & dasGate
Name: Sandra Marqués/ Carlos Arana Remirez
Telephone number: +34 605 326 112
Email: sandra.marques.intern@veridas.com