COVID-19: Effective and responsible biometrics solutions and concepts – one year into the pandemic

April 2021

Contents

1. Introduction

In March 2020, just before the peak of the first wave of COVID-19 in the UK, we asked our supplier members to submit a paper outlining their biometric solutions to the pandemic. A year on, and our understanding of the threat and possible solutions to control it have changed. So we've gone back to our supplier members and asked them to update us. This report is a compilation of submissions from some of our supplier members who wanted to share their thoughts and ideas.

Last May we published the first edition of this report. Since then, it's had over 4,270 downloads and that number is still rising, so this is clearly an area where our network is still looking for answers. Thank you to everyone who has participated in both reports.

For this 2021 update, we asked our members to address the critical questions organisations are still facing and to explain how their solutions are effective. As new products are often of interest, we have also allowed our members to place an advert in the report.

Proposed themes for the report were:

- One year into the pandemic – what have we learnt?
- New technology solutions and what they offer
- Immunity passports
- Biometrics and hygiene
- Touchless versus touch technology
- Solutions for remote working
- Questions about self-enrolment and liveness
- How biometrics including face and iris technology can deal with masks
- Ethical sales at a time of crisis
- New policy or procedures at times of a pandemic
- Digital onboarding solutions

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. Biometix: The critical role of standards for the development and testing of vaccine passports

Vaccine passports, or certificates, apps will be an important part of the world's recovery from COVID. The development of these apps in a standards compliant manner will be critical to driving adoption as well as ensuring national and international interoperability. Standards should also leverage collective best practices and enhance privacy and security.

Reaching an agreement on the best global standards for these apps has been difficult. A variety of approaches are proposed, from leveraging internationally ratified ISO standards, industry-agreed protocols through to standardized open frameworks. Some of the leading contenders include the ISO18013-5 Vaccination Passport, the World Health Organisation (WHO) Smart Vaccination Certificate, the IATA Travel Pass and an extension of the Existing Passport Standard from ICAO called the Digital Traveller Credential.

Each of these standards enables apps to be rigorously tested for compatibility and provide a robust environment for the interchange and use of health related data. It is thus important to ensure that any adopted standard can be independently tested to ensure conformity. The need for testing and assurance of these applications is critical; a developer's simple assertion of compliance is insufficient.

Each standard specifies a different method, or set of requirements, for binding with identity. The approaches differ in how explicit they are about the role or application of biometrics. However, in all cases, the mechanism for binding to identity should be evaluated for standards compliance. Relevant international biometric standards include 19795-5 biometric testing and 30107-3 for presentation attack detection (liveness)

There is now a great urgency in determining the best way forward on these standards and in deploying applications, especially given the widespread use of vaccines in many countries. Despite this urgency, rigorous independent testing, as with determining the efficacy of the vaccines themselves, is critical.

All key stakeholders, from government to industry, need to consider independent testing as a key part of their role-out plans, this will enable them to identify issues early and hence to ensure effective delivery, both on time and first-time.

Our collective return to "normalcy" may be dependent on the adoption of these apps, and this can only properly be supported by the integrity that is provided by independent standards adoption and certification.

Organisation:	*Biometix*
Name:	*Ted Dunstone*
Telephone:	*+61 419990968*
Email:	*info@bixelab.com*

3. Brands Australia: ICAO MRTD Image Capture Compliance & Seamless Self ID Enrolment options

As we come out of the COVID pandemic and international borders again re-open, the need to ensure ICAO Compliant & High Quality images on the enrolled country databases are within ISO / ICAO Standards is more crucial than ever. The need for broader level FRT matching remains important. There needs to be assurance in the matching of live capture images at the Smart Gate with the enrolled image within the country level MRTD databases. This is needed both now and into the future.

The concern remains how do we achieve this with the present COVID risks? High quality image capture is needed at the enrolment level to avoid hold-ups at the Smart Gates, thus ensuring seamless travel. This is balanced against needing to keep staff, who are involved in image capture with the public, safe from potential COVID exposure.

Whilst there are a number of countries that already comply well to ISO Standards 19754-5 -2005, there are many that don't. This will become increasingly apparent in time as gates reopen globally. Live images will miss match against the enrolled database, thus increasing failure rates.

For those Governmental and retail outlets that take passport photo images that are public facing, the issue of how to take the images in a safe and contactless way to protect staff is key. Is it possible to do this using current methods and equipment?

The answer is yes. The operator needs to keep a 1.5 metre distance from the subject (which is about the normal distance from subject to camera) and wear safety equipment including a face masks and gloves. Using alcohol-based wipes in chairs & equipment is also necessary. People awaiting the service need to be queued 1.5 meters apart.

The other option is Self ID Capture systems. These systems require the applicant only and no operator. It still remains important that the booths, particularly the chairs and touch-screens, are cleaned with alcohol-based wipes between applicants but does reduce the interface. It's also important to note that these systems will from time to time require some staff involvement, yet are proving a viable option to reducing staff exposure.

Organisation:	*Brands Australia*
Name:	*John Rule*
Telephone:	*+61 417 5532856*
Email:	*john.rule@brandsaustralia.com*

4. Dermalog: Why iris recognition could be the future of contactless biometric identification

Biometrics companies have to react to the urgent need for change in identification methods during the COVID-19 pandemic. Long-established solutions like touch-based fingerprint recognition represent a risk in the context of infection spreading. The pandemic-related requirement to wear face masks brings new challenges to facial recognition systems.

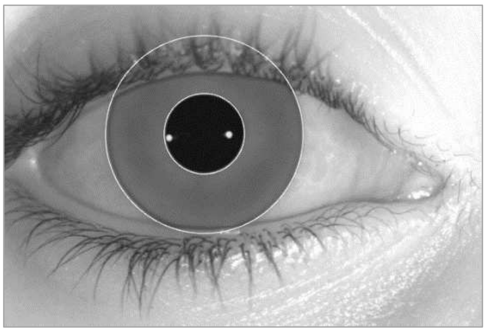
Given the new market requirements for biometrics, iris recognition is coming into focus. Iris technology is a promising field in biometric identification. This paper discusses why iris technology could be the future of contactless biometric identification and how it works.

A CLOSER LOOK INTO THE EYE

The complex and random patterns of an individual's eyes are unique and stable. The iris is a thin, circular structure in the eye, responsible for controlling the pupil's diameter and size and thus the amount of light reaching the retina. The iris texture, due to its intricate structure, constitutes a powerful biometric characteristic. Iris recognition achieves robust resistance against false matches and excellent recognition accuracy, enabling reliable biometric identification in large-scale systems.

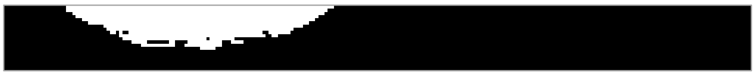
Feature extraction aims to precisely extract any discriminant iris biometric information from the acquired iris image and keep it compactly a biometric matching template. The feature extraction process in iris recognition is divided into four steps:

STEP 1 **Pupil and limbus segmentation**: Pupil (inner iris boundary) and limbus (outer iris boundary) are detected.

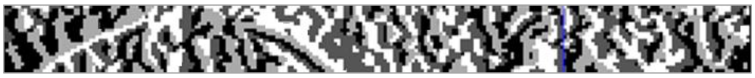


STEP 2 **Rubber-sheet transformation:** The annulus-shaped iris in Cartesian coordinates is transformed into polar coordinates. The so-called rubber sheet is calculated through a linear combination of pupil and limbus boundary curves.

STEP 3 **Mask derivation:** The eyelid, eyelashes, and cornea reflections (very bright spots) are excluded for a biometric comparison. Otherwise, they usually cause a lower comparison result. For this purpose, such a noisy region is localized as a mask.



STEP 4 **Iris code calculation:** Gabor and DCT filters are applied to the iris texture in the rubber sheet, resulting in an iris feature map. Finally, the so-called binary iris code is calculated from the feature map.



One approach to iris feature extraction is to combine high-precision image processing algorithms with cutting-edge artificial intelligence technologies. The feature extraction algorithm should be robust against various biases and variability from the image acquisition, such as different iris camera sensors, different light levels, spectacles, contact lenses, and even makeup (false eyelashes or heavy mascara). For security reasons, the templates should be stored in a different database, separately from the iris images. The iris image cannot be retrieved from the corresponding template and is not necessary to perform an iris matching.

NIR LIGHT FOR HIGH IMAGE QUALITY

Image acquisition plays a critical role in iris recognition since poor imaging conditions negatively affect the systems' recognition accuracy. Iris recognition requires an iris camera with active illumination in the near-infrared (NIR, 700 nm - 900 nm wavelength) and sensors with daylight cut-off filters capturing iris images with sufficient resolution. The NIR light's main reason is that it reveals structural patterns even for strongly pigmented irises in contrast to the images acquired under visible light. Furthermore, the subjects can participate actively in iris image acquisition: Human eyes are relatively insensitive to the NIR light.

Cameras could enable non-contact, automatic capture of multiple biometric features for safe operation, detecting face and iris from a distance of up to 2 m. The cameras also measure body temperature using integrated thermal sensors. As a result, the solution achieves exceptionally high accuracy for biometric identification and provides additional health protection.

TEMPLATE STRUCTURE ENABLES FAST MATCHING

Biometric matching is the process of comparing two biometric templates (e.g. iris templates) to receive a value of similarity (score). The key advantage of iris biometric comparison is a binary fixed-length template. The simple template structure and the binary form help to achieve high comparison speeds. A fractional Hamming distance is calculated as a measure of the dissimilarity.

DERMALOG's iris matching for example reaches a comparison speed of up to 25 million eyes per second. The software exploits the advantages of modern CPU intrinsics (e.g. SSE/AVX) while still being compatible with various CPU generations. Supplementing this, the iris recognition technology achieves a very low false match rate (FMR) and a very low false non-match rate (FNMR) simultaneously.

The solutions should address:

- Tolerating low-quality images: Reliable feature extraction and comparison
- Speed and accuracy: High matching speed and low failure rate
- Stability: The unique pattern of the human iris remains unchanged throughout one's lifetime
- Uniqueness: The probability of two irises producing the same iris code is nearly impossible
- Device independence: Compatible with professional NIR iris cameras
- Flexibility: Integration into existing security infrastructure or operating as a standalone solution
- Full compliance with ISO standard on iris image information (ISO/IEC 19794-6:2011)
- Full compliance with ISO standards on iris image quality (ISO/IEC 29794-6:2015)

Organisation:	*DERMALOG Identification Systems GmbH*
Name:	*Sven Böckler*
Telephone:	*+49 (0)40 413 227 - 0*
Email:	*marketing.de@dermalog.com*

5. FacePhi: Biometrics – A human Technology for Bank Digitalisation

Biometrics is the technology most intimately connected with people, since it is based on the analysis of our behavior and physical features to verify our identity. In this way, our face becomes a unique and inimitable password that allows us to use digital services using our most human side. Thanks to their ease of use and security, these biometric identity verification systems have spread strongly in the financial sector and become a clear example of technology with a positive social impact with the arrival of Covid-19.

Throughout 2020, we have had the opportunity to turn our biometric solutions into useful tools that have guaranteed access to services for thousands of people, despite the confinement and social distancing that have occurred throughout the globe. In April of last year, our facial recognition system reached the healthcare sector for the first time, thanks to its implementation in the Kangbuk Samsung Hospital in Seoul. With this innovation, patients were allowed to carry out different procedures, such as requesting medicines or their next doctor's visit, after validating their identity by recognizing their face on a screen, without the need to use cards or interact with anyone. Shortly after, we developed an improvement in our algorithms so that they were able to recognize faces with masks, adapting our technology to the new requirements imposed by Covid-19. The need for a secure and contactless society encouraged us to continue working on new applications for our biometric software.

As a result of this work, we began to develop together with Supervielle, one of the main private banks in Argentina, a biometric recognition system that would go beyond improvements in security and user facilities, becoming one of the most important success stories in the field of the Silver economy. A development that advances towards the future of biometrics as an inclusive technology accessible to anyone, regardless of age and previous ability in the digital environment.

This success story is based on Argentina's own financial regulation, where it is mandatory for older people to provide "proof of life" in person at bank offices to collect their pension. It is an uncomfortable and inflexible system, since it forces many elderly people to travel and imposes a face-to-face procedure that is repeated on a monthly basis. At the beginning of 2020 we achieved a milestone in the Argentine banking: our facial recognition solution now allowed them to proof life and collect their pension with just a selfie from their mobile application.

In the months following its implementation, this facial recognition system focused on the senior user grew at a remarkable rate. The health crisis forced in Argentina one of the longest confinements in the world, which kept its citizens for more than 7 months with hardly any possibility of carrying out procedures outside their homes. In this complex context, our technology had a positive social impact, being able to protect the health of more than 38,000 older users who began to monthly proof their lives without going to a bank branch. The social impact of this project has opened the door to a whole universe of digital services adapted for the senior user, such as checking the date of receipt of their pension or withdrawing cash by identifying themselves with their own face, without the need for passwords or complicated procedures.

But, what does the future hold for us? Beyond its social role during the toughest moments of the pandemic, our facial recognition system represents a first step towards a new way of understanding digital services and the relationship with all types of users. In the near future, this technology will give rise to multiple uses due to its great scalability, completely replacing the use of passwords by a simple facial recognition process in any financial operation and linking to different touch points in the branches, in order to facilitate the completion of procedures.

In short, the use of biometrics has already become more than just a technology that allows a safe and practical relationship between banks and their clients. The digital transformation is a fact, with a near horizon in which companies, institutions and citizens will interact, mainly, through digital platforms. In this context, from FacePhi we are committed to ensuring that this transition is inclusive and broadens to all types of people, including senior users and groups at risk of exclusion due to their lower capacity to operate in these environments. We want biometrics to bridge the digital divide, and to consolidate the most humane way of relating to Artificial Intelligence.

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

6. IDEMIA: Traveling despite COVID – How to regain confidence

The Covid-19 pandemic has created substantial global disruption. This year has taught us humility, and the need for the industry in general to be flexible in order to adapt to any change. Whether this be changes to:

- the virus and its variants
- the health situation
- our economies
- the psychology of global populations pertaining to their life, work and consumption habits

After a year of health crisis, more than ever we must put in place solutions to a potentially long-lasting issue and rebuild trust among all stakeholders.

Governments, as well as the entire travel industry, have mobilized to find urgent solutions to resume travel and safely reopen borders. To ensure a global response, a combination of solutions are considered in order to comply with the new paradigm with regard to air travel. The solutions proposed include **contactless technologies, health pass and risk analytics**. Not only will they limit interaction, but they will also help governments to implement long-term risk mitigation strategies at borders by integrating a new factor: health data.

Improving hygiene at airports with contactless technologies

Among the many initiatives deployed, two stand out the most; remote services and touchless technologies. Through the use of remote services, travelers can start their journeys from the comfort of their homes. For example, they can confidently complete their biometric check-in securely using the airport/airline's app on their smartphone thanks to the integration of robust presentation attack detection.

There is also an increasing interest in contactless biometric technologies, as they will play a key role in reducing the spread of the virus, as well as regaining the confidence of travelers. But these are not just 'simple touchless technologies', they are innovative touchless devices that identify travelers on the move, enabling greater efficiency and a better user experience, while respecting user privacy.

If biometrics allow travelers to securely go through any airport touchpoints in a contactless way, then touchless interaction with the equipment (ie: the screen) is also needed. Among the various touchless solutions being offered, the use of smartphones is key. At the kiosk, by creating a mirror image of the information presented on the screen, travelers can use their smartphone to interact with the airport/airline's touchpoint without touching the actual screens.

Even passports are about to be digitalized, so that they can be securely stored and used through the traveler's smartphone with the same level of security and interoperability as the physical document. This is called Digital Travel Credentials (DTC).

Health Pass solutions supported by Governements

Due to the pandemic, further checks may be required in addition to what is currently being done. We can reasonably assume that the new checks will be related to the health status of travelers.
In order to permit cross-border travel, travelers will have to prove that they are healthy or vaccinated. Therefore, travel documents such as passports, visas, electronic travel authorizations or even a new 'sanitary passport' may incorporate health status data.

Various health certificates can be issued to verify the traveler's health status and should be considered to be a legitimate method of health verification. Health Pass solutions should enable secure storage of all types of certificates, from PCR tests to proof of immunity or vaccinations.

The industry is searching for an interoperable solution that can be issued securely while preserving privacy and ensuring data protection of all, including biometric, biographical and health data. The establishment of a trusted Health Pass is a key step toward regaining the confidence of governments. The level of trust associated with the Health Pass is a key consideration as they will be shared among various stakeholders. Governments, as trusted actors, are in the best position to guarantee the authenticity of the health certificates. They can also leverage the existing Public Key Infrastructure (PKI) for the issuance of the ICAO Visible Digital Seal which is an internationally recognized standard of a 2D bar code. This can be updated to meet the current requirements of the health certificates for travel-related purposes. This issuance can be adapted to the specific needs of each country while complying with international standards.

Additional screening and mitigation strategies

All this valuable data could be integrated into the existing border control systems, as well as the interactive Advanced Passenger Information systems or Passenger Name Record analytics solutions. This would allow the relevant government agencies to perform the necessary traveler checks in advance, enabling them to welcome bona fide travelers or implement appropriate measures as necessary.

It could be valuable to know if a traveler has flown from, or transited in, a ‘high-risk’ area before arriving at their final destination, or if they were close to infected passengers on a plane. As usual, an appropriate balance between security and privacy must be actively maintained.

The current risk assessment solutions will have to be adapted in order to integrate new business rules that take into account epidemic (and pandemic) threats such as COVID-19. These business rules and processes will have to integrate data that can be shared prior to travel, or collected at the arrival destination. For example data on immunity testing, which is gaining an increased interest.

It is time to start planning how travel will resume: expectations are high, but there can be no such resumption without strict control of the health risk and trust from the community. All in all, the industry is working on a wide range of solutions. These encompass the collection and processing of health certificates, the border risk assessment itself and solutions supporting a touch-free and hygienic end-to-end passenger experience, as well as the collection of digital health information. Future technologies including biometrics are also part of the response to the current health crisis.

Organisation:	*IDEMIA*
Name:	*Nicolas Phan*
Telephone:	*+33 7 63 14 32 58*
Email:	*nicolas.phan@idemia.com*

7. Innovatrics: Presentation Attack Detection (PAD) – the case for passive liveness

There's been a lot of fuss in the identity world about so-called liveness detection. In fact, there's even confusion over the correct terminology; the National Institute of Standards and Technology (NIST) categorizes liveness detection as a subset of Presentation Attack Detection (PAD) and defines it as follows:

"The measurement and analysis of anatomical characteristics or involuntary or voluntary reactions, in order to determine if a biometric sample is being captured from a living subject present at the point of capture."

Early PAD "Active Liveness" technologies focused on instructing users to carry out voluntary reactions to prompts, such as tilting their head a certain way or following a randomly moving object with their eyes (this was the method used in early iterations of Innovatrics Digital Onboarding Toolkit). These methods, while effective to a point, can be outsmarted with a little effort and ingenuity.

More recently, technology vendors have come up with more advanced methods of detecting presentation attacks. These new methods fall under the category of "Passive Liveness", as they do not require the user to carry out any actions in order to allow the algorithm to calculate their liveness score. This is where things start to get interesting.

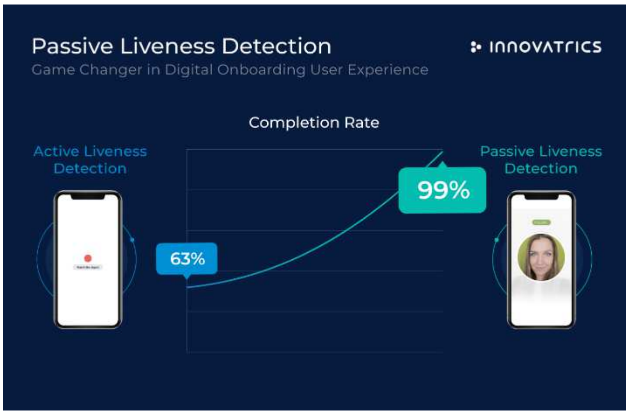
Passive liveness uses image recognition deep learning techniques to tell a real face from an image (e.g. perspective distortion, involuntary eye movement or facial muscle twitching). The training set contains many different spoof vectors: printed photographs, printed masks, screenshots from mobile or PC screen.

The passive liveness developed in Innovatrics runs in the background of the face capture process; only need one frame to tell if the person is real and alive. In order to succeed different use cases and conditions, it runs also completely on-device utilizing the power of neural networks compressed into a lightweight mobile component with same performance as the server-based solution.

So which approach is better in real world applications such as remote onboarding? The evidence we've gathered from dozens of deployments is conclusive. One of our early-adopter customers initiated their project using Active Liveness, then took the decision to upgrade to Passive Liveness in 2020. The result?

Active Liveness: 63% of customers successfully completed this step, taking an average of 13 seconds

Passive Liveness: 99.9% of customers successfully completed this step, taking an average of 1 second



What's more, when we ran the Passive Liveness algorithm over their existing database (of over 30 million onboarding images), we found that approximately 1% of all previous onboardings had been completed with the help of a presentation attack. Armed with this information, our customer was able to close down these accounts and protect their business from potential fraud.

By introducing Passive Liveness, we simultaneously improved the user onboarding experience and increased the overall security of the application.

Another strong argument supporting Passive Liveness is the fact that there is an ISO standard (30107-3), which sets out principles and methods for performance assessment of presentation attack detection mechanisms. A testing lab named iBeta, based in Denver, Colorado was the first to carry out testing according to this ISO standard in two levels; iBeta Level 1 PAD and iBeta Level 2 PAD.

In 2020, Innovatrics achieved Level 1 PAD accreditation and we are currently preparing our submission for Level 2 PAD. We also keep an open mind to new testing bodies which may emerge. Biometric benchmarks are useful to a point, however, I always recommend that organizations test biometric technology on their own data against two main criteria; speed and accuracy. If it's very fast but not accurate, you can't use it. If it's very accurate but not fast, you shouldn't use it either.

And most importantly, if vendors claim to be "iBeta Certified", "3D Certified", or "Level 4/5 Certified", do a little more research. No such independent certifications exist.

Organisation:	*Innovatrics*
Name:	*Donal Greene*
Telephone:	*+421 2 2071 4056*
Email:	*Roman Sevec, roman.sevec@innovatrics.com*

8. Jenetric: Fingerprint readers are dead – aren't they?

No doubt, the Corona pandemic, with all its implications, challenges the biometrics industry to a considerable extent. Of course, as in any other industry, economics, supply chains, physical conferencing and working from home are the obvious implications. However, there is a more important question to answer: Will this pandemic change the way biometrics, and fingerprint scanners in particular, are used in the future?

If there was one buzzword that characterized the last 11 months in the biometrics community, it was "Touchless." Whereas in the pre-pandemic era, the use of biometrics was focused on "Seamless," today almost every conference and webinar focuses on the use of biometrics in a "Touchless" approach. From April 2020 to the present, there have been about 25 press releases from academia, industry or the media related to touchless biometrics. Suddenly, and for understandable reasons, facial, iris and voice biometrics have become much more relevant.

Almost one year ago the death of fingerprint scanners was predicted. Low-end single-finger readers, which are mostly used for authentication, will fall off the cliff due to the pandemic. According to the forecast, within 2-3 years, four-finger readers used for more sophisticated law enforcement and border control applications will be replaced by smartphones and their contactless biometric capabilities (fingerprint or other modalities). Along the way to this transition, more stringent disinfection solutions and antimicrobial measures will be applied to these four-finger readers.

Ten months after the death of fingerprint readers was predicted, it's time for an interim update. The introduction of FACE ID by Apple with the iPhone X in 2017 was done for a variety of reasons, but certainly not for pandemic or sanitary reasons. Very soon, other smartphone manufacturers followed this move from finger to face.

Contactless fingerprint capture via the phone's camera has been around for a while, and there were and are pilot studies ongoing. Here, hygienic concerns are not the driver for this approach, but rather the convenience of using the phone instead of a separate fingerprint reader. Compared to a report published seven years ago, progress in contactless fingerprint solutions has been reported in 2020. Whether considering more advanced touchless fingerprint readers or smartphones, images taken with most readers today do not represent a 3-dimensional structure of the ridges but rather a 2D image. This approach has been shown to cause issues in accurate fingerprint capture due to distortion, deformation of the finger's skin, low contrast and in correcting the distance between the finger and the camera. Therefore, efforts in research on touchless fingerprint capture technologies are still needed before contactless fingerprints are fully accepted for more advanced fingerprint applications by certification bodies or governments.

Be safe with JENETRIC's fingerprint scanners
Now available:
Antimicrobial Coating
- Effective against bacteria and viruses
- Nontoxic and non-sensitizing to human skin
- No loss in fingerprint quality
- Durable and robust against abrasion and cleaning
sales@jenetric.com

Not surprisingly, all manufacturers of touch-based fingerprint readers provided protocols and instructions for sanitizing their products. Although the risk of infection by touching a surface is much lower than from airborne transmission, regular disinfection helps to reduce the risk of infection even further. In real life, disinfecting is inconsistent (not following the rules, lack of disinfectant availability, etc.) and therefore sophisticated solutions beyond regular disinfection, such as antimicrobial coatings or disinfection by UV for fingerprint readers, were introduced. Surely more smart solutions can be expected in the coming months.

Are fingerprint readers dead?

The pandemic has clearly focused attention on hygiene and fingerprints, much more than in previous years. However, whether customers are ready to switch from touch-based to contactless solutions, or even replace fingerprints with other modalities, has yet to be answered. Many parameters other than just hygienic concerns, such as cost, ease of use, legislation, and backward compatibility to existing data sets or accepted standards determine the penetration of new technologies. Finally, at this point it is not clear how long the pandemic will continue to affect the biometrics industry in the near to long term. So maybe after "Seamless" and "Touchless" the next big thing will be "Faceless", because facial masks will certainly be around for quite a while.

Organisation:	*JENETRIC*
Name:	*Roberto Wolfer*
Telephone:	*+39 3641 32199 50*
Email:	*sales@jenetric.com*

9. Jumio: 5 ways to keep AI bias out of online identity verification

When bias becomes embedded in machine learning models, it can have an adverse impact on our daily lives. It's exhibited in the form of exclusion, such as certain groups being denied loans or not being able to use the technology. As AI continues to become more a part of our lives, the risks from bias only grow larger.

In the context of facial recognition, demographic traits such as race, age, gender, socioeconomic factors, and even the quality of the camera/device can impact software's ability to compare one face to a database of faces. In these types of surveillance, the quality and robustness of the underlying database is what can fuel bias in the AI models. Modern facial recognition software uses biometrics to map facial features from a photograph or video. It then compares the information with a database of known faces to find a match (this is known as a 1:n match).

In 2018 the American Civil Liberties Union found that Amazon's AI-based Rekognition facial recognition software falsely matched 28 U.S. Congress members with a database of criminal mugshots and that nearly 40% of the false matches were of people of color, even though they made up only 20% of Congress.

Demographic bias is also an issue for facial authentication which relies on an individual's unique biological characteristics to verify that she is who she claims to be.

Facial recognition and facial authentication, however, are two very different kinds of animals.

Most leading identity verification solutions leverage AI and machine learning to assess the digital identity of remote users. Unfortunately, these algorithms are also susceptible to demographic bias. But, this type of bias has nothing to do with the underlying database because this type of authentication doesn't perform 1:n-type searches against an established database of images.

It's a whole different kind of AI that is used to solve a very different business problem — if the person is who they claim to be when creating new accounts online.

AI algorithms are used to compare the selfie of a customer with the photo in their identity document, and bias can creep into algorithms in several ways. AI systems learn to make decisions based on training data, which can include biased human decisions or reflect historical or social inequities, even if sensitive variables such as gender, race or sexual orientation are removed.

Here are five critical questions to ask solution providers to determine how well they are addressing demographic bias:

1. How big and representative is your training database?

Machine learning models use AI training datasets to learn how to recognize patterns and apply technologies such as neural networks, so that the models can make accurate predictions when later presented with new data in real-world applications. When it comes to AI, size matters. The larger and more representative the training data set, the better its ability to withstand the introduction of demographic bias.

2. Where did the data come from to create the training data sets?

When companies don't have enough of their own data to build robust models, they often turn to third-party data sources to backfill this gap, and these purchased datasets can introduce unintentional bias. For example, a dataset of images of ID documents captured under perfect lighting conditions with high-resolution cameras is not representative of ID images that are captured in the real world. Not surprisingly, AI models built on unrealistic models will struggle with IDs that were captured in dim lighting. Algorithms that were built with real-world production data, on the other hand, will contain documents with real-world imperfections. As a result, these AI models are more robust and less susceptible to demographic bias.

3. How are the data sets labeled?

In the context of identity verification, labeling is how the ID documents are tagged. If the photo of the ID has been manipulated, then the document will be tagged as fraudulent with photo manipulation. If the picture of the ID has excessive glare, then the label should reflect this characteristic. If the wrong labels are used when tagging individual identity verification transactions, the AI models will bake that information into the algorithms, making the models less accurate and more subject to bias.

Some solution providers outsource or crowdsource the tagging exercise while others insource it to experienced agents who are instructed how to tag verification transactions to optimize the learning curve of the AI models. Naturally, the insourcing models generally result in more accurate models.

4. What type of quality controls are in place to govern the tagging process?

Unfortunately, a lot of this bias is unconscious because many solution providers do not necessarily know when they're making the algorithm that it's going to make incorrect outcomes. That's why there needs to be some quality control injected into the process. In the identity verification space, there's no substitute for having a trained crew of tagging specialists who know how to accurately tag individual ID transactions and auditing processes in place to check their work.

5. How diverse is the team developing the algorithms?

Reducing bias is also about the people who are developing the AI algorithms and tagging the datasets. It's not unfair to ask about the composition of the AI team. Ideally, the AI engineers and data scientists come from a variety of nationalities, genders, ethnicities, professional experiences and academic backgrounds. This diversity helps ensure that different perspectives are brought to bear on the models being created which can help reduce some demographic bias.

There is a growing concern that demographic bias in a vendor's AI models could reflect negatively on a company's brand and possibly raise possible legal issues, especially when economic decisions are dependent upon the accuracy and reliability of those algorithms. Believe it or not, these algorithms can result in some types of customers being unfairly rejected or discounted, which translates to lost business and downstream opportunities. That's why it's increasingly important to understand how vendors measure demographic bias and what measures they are taking to address it.

Organisation:	*Jumio*
Name:	*Claire Galbois-Alcaix*
Telephone:	*+44 020 7031 6004*
Contact:	*www.jumio.com*

10. Laxton Group: A new dimension for biometrics: Hygiene safety management integrated in elections

Early 2020 it felt like the world came to a standstill. And yet, for those of us in the biometric space, it was as if the opposite resulted. Suddenly, we had to adjust our biometric solutions and leapfrog into a new era: one where biometrics are intimately coupled with hygienic procedures like social distancing and sterilization. While much of the world did slow to a halt, elections clearly could not. The effect that a National Election and voting have on the lives of millions of people is significant, and ultimately, it's their right. Thus, extreme flexibility and well-thought-out solutions were required to ensure that safe and secure elections continued without delay.

The National Election in Ghana led us to re-think how we provide end-to-end solutions in these special times. To ensure the election happened on time, hygiene challenges were re-evaluated when dealing with supply-chain, production of equipment, training of election officials, and mobilization of voter registration. We needed to ensure that documentation could be verified safely, voter registration could occur without worry, and more importantly that voter authentication was still possible.

We took this as an opportunity to relook at our end-to-end solutions, adapt our technology, and integrate this type of hygiene-focused thinking into the future of our devices, services, and procedures.

Safety First - Social distancing, disinfecting, and unique training methods

When you need to ensure that in 10 weeks, 8500 biometric registration kits are set up, 76,000 Biometric Voter Verification handhelds are deployed, and countless elections officials are trained during a pandemic, you start to think creatively. 17 Million voters were counting on it.

Democratic elections matter. For many Ghanaian's voting means traveling long distances and facing difficulty authenticating their identity. The Electoral Commission of Ghana worked with Laxton to help bring stability and confidence to the electoral voting process and to help mobilize it so that more Ghanaians than ever before could cast their vote. When COVID-19 hit, these voters required a solution that had to consider the now added importance of their health.

The elections team at Laxton was able to innovate and adapt our processes to better suit the changing needs of the world when it comes to hygiene first.

We integrated change solutions into our end-to-end process to ensure safety, and for hygiene to be a priority in working together. This included social distance working methods, private charter flights for our teams and quarantine setups for those landing in the country, COVID-19 testing, changing of masks every 2 hours, and handwashing and sanitizing stations to allow for the continuous production of the kits without added risk. We developed training methods for the election workers to keep them safe and reduced numbers by doing stakeholder meetings virtually, prepared training videos to share using a designated What's App training channel and held one-on-one training with significantly scaled-down numbers.

Without normal options available, we had to reconfigure how the biometric kits were assembled and how training was completed.

During the preparations for the election, COVID-19 suddenly changed the dynamics completely. Besides registering voters in remote areas, it also had to be done during a brutal pandemic with limited travel options, while keeping social distancing and new hygiene protocols. We observed that COVID-19 brought a fast shift toward "touchless". In this situation, we recognized that we could continue to rely on our well-tested, rugged equipment, and instead, adapt how we used the equipment as opposed to adjusting the equipment itself. The appropriate measures were put in place to combat any risk of an increase in infections.

With careful changes to hygiene protocols, we kept focused so that the project and implementation of it would not be a cause for a rise in COVID-19 cases in Ghana during this election.

Elections go on

In 2019 nearly two billion voters in 50 countries around the world participated in elections. More than ever before. The UN and World Bank envision that by 2030 every individual in the world will have a digital identity. Digital ID promises to transform Africa's economic and political landscape. It means having a voice, and it means being able to democratically vote.

New insights gained beyond elections

We have adapted our devices in instances where it contributes to reduce the risk for communicable pathogens.

We adapted our mobile handheld device, the Chameleon 5L to include a temperature sensor that "alerts" the operator of individuals with increased body temperature. Leveraging incredible camera technology and SDK's for improved readability, we were able to eliminate physical contact and still ensure secure, accurate authentication. This for example allows a passport photograph to be scanned using the camera technology instead of a person having to place their actual passport down on a device. Authentication and verification can continue without the security and the quality of the data being compromised.

Our Biometric kits have a uniqueness that allows for a 90-degree rotation. This deliberate rotation allows citizens to have no physical contact with the kit operator. Kits are sanitized, and people can stay 6-feet-apart and still ensure accurate authentication and verification. This type of thinking is one-part hardware design and one-part operational design. We think about our end users all the time. Furthermore, we consider how to keep both their identity and their health as a priority without ever sacrificing security and accuracy.

Biometrics and hygiene – A relationship that will continue

The risk of communicable diseases was always considered, but never as top of mind as it is today. Our experiences in 2020, and into 2021 have expanded our insight. Those in the area of biometrics are working with changing requirements and exploring alternatives for even better solutions. New features and product designs, combined with increased hygienic procedures bring the overall biometric solutions to a new era toward secure, safe, and hygienic authentication.

Organisation:	*Laxton Group*
Name:	*Nick Perkins*
Telephone:	*+31 702 505 600*
Contact:	*https://laxtongroup.com/*

11. Phonexia: The pandemic has uncovered the need for frictionless voice biometric authentication

It has now been more than 12 months since our society began its fight with the coronavirus's infamous worldwide spread. Long-established communication patterns over the phone, Internet, and other channels have been turned upside down and shaken heavily. Never before has humanity experienced such an intense information overload as during these unprecedented times.

As it seems that the battlefield dust is finally settling down globally, due to the many creative processes put in place, it is now an ideal moment to revisit the weak points that affected organizations' abilities to interact with people efficiently over the phone and other voice channels.

Bottleneck #1: Long authentication process

Contact centers of banks and other security-driven commercial institutions always did their best to verify a person reaching out to them remotely. An account breach is unforgivable these days, and with cybercrime methods advancing quickly, the number of security checks is growing.

This, however, prolongs the authentication phase of each call, as the organizations' employees need to ask many security questions before they can even start discussing what they were originally after.

Before 2020, people were fine with waiting in a queue to talk to an agent on the other end of the phone line. Customers' calling patterns repeated year after year, and organizations knew what to expect. If a sudden surge in calls happened, people simply waited a bit longer.

2020 was different. The coronavirus had suddenly forced millions of people to stay at home, and instead of interacting with their banks, insurance companies, and other utility providers face to face, they switched to the phone.

Not accustomed to an authentication process over the phone, many didn't remember their security questions, had forgotten their PIN codes, and got frustrated for not knowing the second and seventh number of their contract's number.

Bottleneck #2: Limited workforce

Lengthy authentication processes amplified yet another bottleneck—a limited workforce.

As the number of people reaching out to institutions over the phone multiplied massively within an extremely short time, the precisely calculated (but limited) workforce of call centers struggled to meet the entire demand.

Hundreds of people were forced to wait in a queue to talk to a person who could help them with an inquiry they would otherwise have solved in person. But as branches were closed, there was simply no other option. For people accustomed to discussing matters in person, phone communication was a natural and instant choice.

Even though the Interactive Voice Response (IVR) systems and voicebots played an important role in easing the workload, lengthy authentication based on various security questions was still a frustrating bottleneck for many "newcomers".

Bottleneck # 3: Agents working remotely

As if the limited workforce wasn't bad enough, home office requirements and forced quarantines further lowered the number of available employees who could respond to the people's requests over the phone.

Companies that used to manage their call center employees on premise had to quickly adapt their internal processes so their agents could work from home seamlessly. This has been extremely challenging for institutions working with sensitive customer information. Not only do these companies have to be sure about the identity of the person speaking to their agents, but they also need to ensure that a verified agent is talking to a person on the phone.

It is relatively easier to supervise agents if they work in a company's building than managing agents who work from home. Cybercrime and social engineering are advancing fast, and a remote work infrastructure is an attractive way for fraudsters to overcome security measures.

When agents work from home, it is much harder for organizations to control whether the agent who has just logged into the company's system is still the same individual who is speaking to a person on the phone only a few moments later.

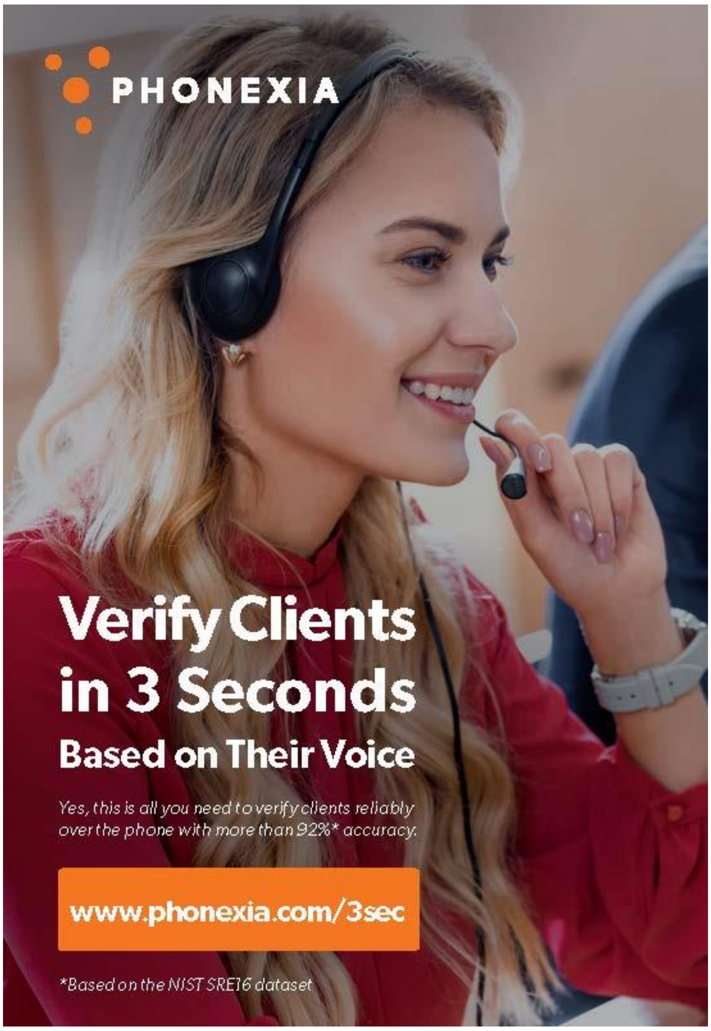
The need for frictionless voice biometric authentication

The current massive shift toward remote working and digitalization has changed the way people are interacting with organizations. What would have been solved in person just a year ago is now approached with a "remote" mindset first.

This significant behavior change has uncovered an immense need for frictionless authentication that verifies a person over the phone as seamlessly as possible.

As the most natural part of every conversation is voice, passive voice biometric authentication is an ideal candidate for frictionless verification of a person's identity over the phone. Especially if voice biometric authentication is truly passive—the person who is being verified can speak freely without the need to repeat any specific phrases.

The passive voice biometrics approach enables organizations to shorten the authentication phase significantly (bottleneck #1), which in turn allows agents to respond to a much larger number of calls (bottleneck #2), and ensures excellent customer experience while keeping fraudulent behavior at bay (bottleneck #3) with continuous passive voice biometric verification running in the background of a call.


PHONEXIA
Verify Clients in 3 Seconds
Based on Their Voice
Yes, this is all you need to verify clients reliably over the phone with more than 92%* accuracy.
www.phonexia.com/3sec
*Based on the NIST SRE16 dataset

Organisation:	*Phonexia*
Name:	*Miroslav Jirku*
Telephone:	*+420 734 466 400*
Email:	*miroslav.jirku@phonexia.com*

12. TECH5: Exploring innovative biometric-driven solutions for proof of vaccination

As we approach the one year anniversary of the World Health Organization's declaration of a global pandemic, the number of people to have been infected with COVID-19 exceeds 132 million, and more than 2.8 million of these people have died. The response to this health crisis has been the development and approval of several vaccines with unprecedented speed to combat COVID-19.

Although access to vaccination can translate into more freedom of mobility and conducting business, without the ability to verify one's immune status in a secure and indisputable manner, increased immunity does not in and of itself reduce these restrictions. In order to bridge the gap between immunity and the return to normalcy, several private and public organizations are rapidly implementing proof of vaccination solutions to track an individual's immunity status, which, in turn, will not only reduce restrictions on business and travel, but also serve as an aid to limit the spread of the virus.

The purpose of this article is to explore global technological readiness for proof of vaccination solutions. We will discuss the advantages and disadvantages of the different types of vaccination certification, the main features of each as well as the manner in which they could be implemented.

What do the Latest Solutions for Proof of Vaccination Look Like?

1. **Printed Certificate**

   The most immediate and readily available solution for certifying vaccine status is the printed certificate. Such a solution requires that a health official issue a document proving vaccination status immediately after vaccination.

   The most obvious disadvantage such insecure certificates face is forgery. Consequently, any printed vaccination certificate that does not include on it some sort of visible and/or invisible security features can be easily forged or altered.

   Even if the document is legitimate and contains the necessary safeguards to prevent its forgery or adulteration, it is still necessary to verify that the person presenting the document is the person named in the certificate. Therefore, the second disadvantage of standard printed documents has to do with the absence of an inherent quality that allows for the immediate and foolproof verification of the identity of the holder of the certificate.

   Finally, it may be difficult or impossible for a printed certificate to be easily updated or replaced.

2. **Technology-based Solutions**

   Several health and government authorities as well as some large industry players are currently commencing the implementation of new solutions that provide proof of vaccination. These solutions have been provided to the authorities as mobile applications that can be used for issuance of vaccination passports to citizens.

   Despite the obvious benefit and ease that such solutions provide, several difficulties associated with implementation and usage of some of these solutions have emerged.

   The most pressing concern associated with these applications has to do with issues of Privacy both in terms of keeping an individual's identity safe and the ability of the application to collect personal data not relevant to the verification of one's vaccine status. Furthermore, for existing solutions that provide proof of vaccination, most applications require linking vaccination status to a citizen's ID.

   Another issue related to the use of a mobile application solution for vaccination status has to do with implementation time. In general, the implementation of complex technological solutions takes months at a minimum.

   Also, the solution should also not be limited in its ability to establish identity and authenticate it. In other words, the optimal solution should easily and securely 1) verify the genuineness of the issued vaccination certificate, 2) indisputably authenticate the identity of the person presenting the vaccination certificate (if required by the use case), and 3) confirm that the person is indeed the owner of the certificate. Additionally, the solution should be flexible enough to manage the issued vaccination passport. In other words, the solution should allow for easy update of stored data.

   Finally, a limitation that is of particular importance to a mobile application is internet connectivity. Specifically, online solutions require the internet by definition, and mobile solutions exclude citizens without smartphones. The optimal vaccination passport, therefore, will be one that also allows completely offline authentication of the information it contains.

Rethinking the Approach to Proof of Vaccination

Given the needs and limitations for a mobile solution that can provide each individual with the ability to confirm their vaccination/immunity status securely and authentically, we took an initiative to conceptualize and design a technological solution that can facilitate the next critical phase of the post COVID-19 world, which necessitates bringing life back to the new, required normality.

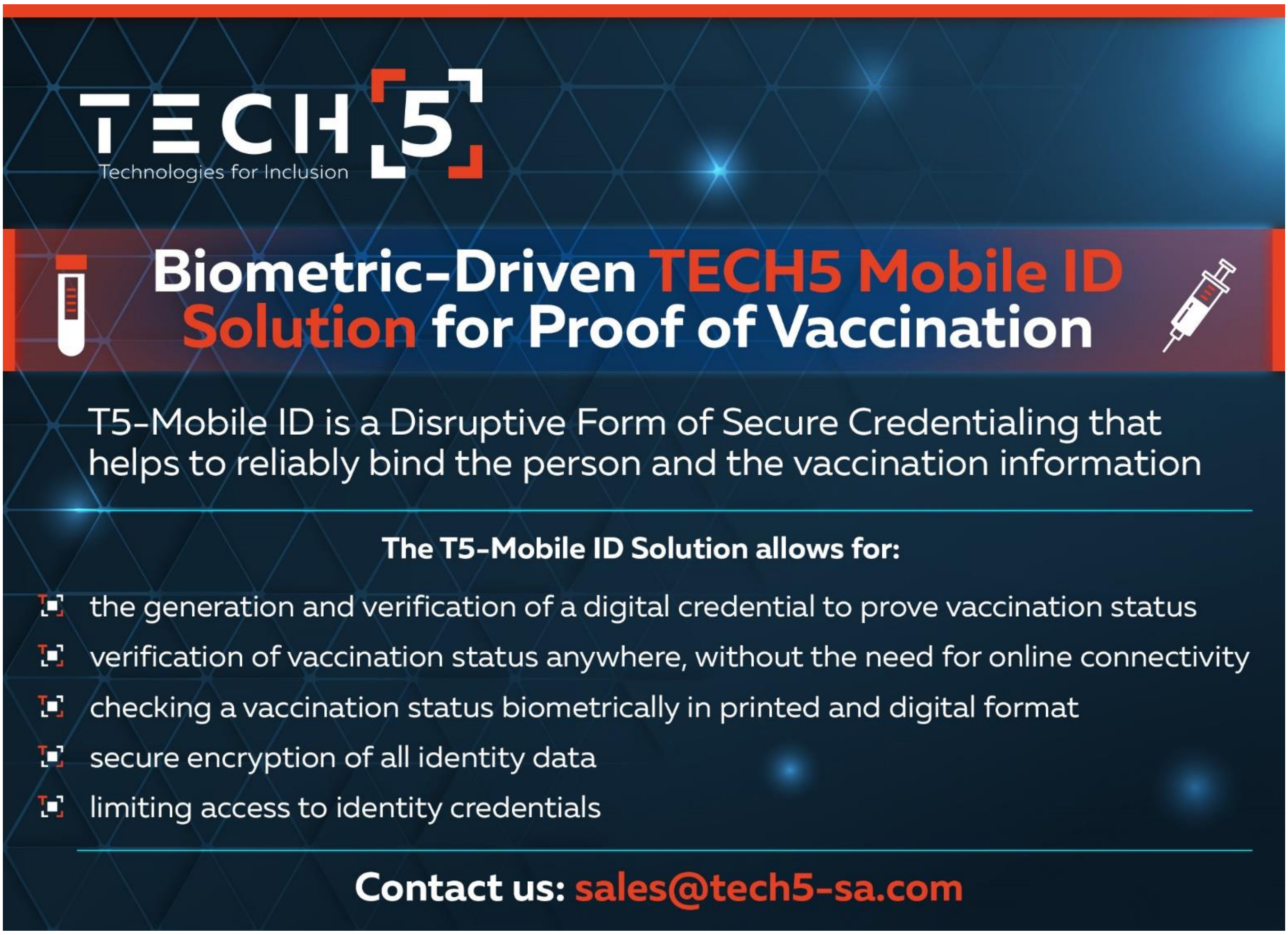
Uncoupling vaccination status from a citizen's ID

In order to avoid such types of problems as endangering the personal data or limiting the access due to absence of Internet connectivity or a smartphone, the objective of proof of vaccination needs to be addressed differently compared to previously described solutions.

The solution should allow vaccinating entities to provide each vaccinated person quickly and easily with a biometrically-verifiable credential. The credential should contain the vaccination date and status, as well as biometrics, for example, face biometric template, all encrypted securely. The credential then should be presented, on a smartphone or in printed form, to any verifying organization that has downloaded the verification software, which can run on a smartphone or other mobile device, to verify that the person presenting the credential is the true owner. The verification should be based on biometrics, but require no third party verification, and so, the biometric data itself will stay with the owner and under the full control of the owner.

Such a solution will solve all main problems of the existing solutions as it is inclusive and links the vaccination status to its holder in a secure and private manner, preventing forgery and allowing to boost the fight against pandemic.

Organisation:	*TECH5*
Name:	*Yulia Bibikova*
Telephone:	*+7 926 666-10-22*
Email:	*info@tech5-sa.com*



Biometric-Driven TECH5 Mobile ID Solution for Proof of Vaccination

T5-Mobile ID is a Disruptive Form of Secure Credentialing that helps to reliably bind the person and the vaccination information

The T5-Mobile ID Solution allows for:

- the generation and verification of a digital credential to prove vaccination status
- verification of vaccination status anywhere, without the need for online connectivity
- checking a vaccination status biometrically in printed and digital format
- secure encryption of all identity data
- limiting access to identity credentials

Contact us: sales@tech5-sa.com

13. Thales: How biometric technology can protect and improve the future of sport

One year on from the start of the COVID-19 pandemic and the long-term effects of the virus are still visible in the sports and leisure industries. Despite the fact that football matches, Grand Prix, and Superbowls are - for the most part - now back on television, sporting events have been just as much at the mercy of this unpredictable and ever-changing health crisis as any other segment of life.

With data now showing dwindling audience viewing figures for major sports events, organisations are looking for innovative ways to help welcome fans back to stadiums, and soon. But how exactly can this be achieved in a way that protects the health and wellbeing of athletes and fans alike? Well, to quote soon to be basketball Hall-of-Fame inductee Kevin Garnett, with the help of technology, 'anything is possible!'

Facial Recognition for socially-distanced access control

Equipping stadiums with biometric gates can provide a fast and secure contactless experience for supporters. The principle is simple and transparent; a person is given a unique temporary ID when they 'check-in' to the event from home. This number then becomes the identifier for that fan throughout the event, with facial recognition cameras confirming that the face verified during check-in is the one entering the grounds. This data is anonymised so that the person is only ever associated with a number, not their personal data, and is deleted once the event is over. With hygiene concerns still at the forefront of people's minds, these gates can eliminate touch points facilitating the spread of the virus, provide less contact with stadium staff and reduce queuing time.

What's more, as wearing a mask, or some sort of face coverage, is likely to remain a requirement during big sporting events (particularly those indoors) for some time to come, facial recognition cameras are now compatible with the use of PPE. Indeed, data from the National Institute of Standards and Technology has shown the technology can still provide excellent accuracy in recognising masked faces.

Smart gates for contactless temperature control in crowds

One of the major challenges sports organisations face when it comes to the virus, is dealing with the sheer number of fans needing to be processed and be deemed fit to enter the event. While it is clear that fans are keen to start experiencing live sport again, they also need to trust that organisations are doing their best to minimise the virus spread. What's more, this needs to be executed in such a way that it doesn't dramatically increase venue queuing times or have a significant impact on how convenient it is to enter the grounds.

This is where smart gates can help. By adding thermal imaging and artificial intelligence to smart gates at sporting venues, sporting staff can use this contactless technology to quickly and easily see which people in a crowd may be running a temperature, one of the COVID-19 symptoms. In turn, this allows them to determine the risk factor of allowing this person into the event and take precautionary action, if deemed necessary.

Digital Identity Verification for contactless authentication

The pandemic has highlighted the need to reduce contact points with objects and people as much as we can to decrease the spread of the virus. When visiting a stadium, however, this is currently quite difficult as fans need to pass multiple ticket checks in order to verify they have the right to watch the event, and that the tickets they hold are legitimate. This is where digital identity verification can play an important role – authenticating each person through automated ticket terminals in a seamless and fully self-serviced journey.

In practice, this works by fans verifying that their ID online matches the name on their ticket before they enter the arena. This can be achieved by matching the biometrics on their ID document photo with a selfie, just like when using some elements of online banking. Once this has been approved, a unique identifier is created for the person in question in the form of a 'live' QR code. With the identifier in place, the fan can proceed through all ticket terminals simply with a contactless scan of their own device.

Digital Identity Wallets for Health Passes

As vaccination programmes gather momentum, many governments are looking to so-called health passes (aka vaccine passports or certificates) as a potentially powerful asset to secure international travel.

However, even if just deployed at the domestic level, health passes are a useful tool to verify your health status at sporting events and venues. This would give supporters a means of providing trusted proof of the results of PCR or antibody tests, or of their vaccinated status, while reassuring stadium staff that the credentials being presented have been issued by a legitimate authority.

Using a Digital Identity Wallet, it is possible to provide a secure, fully interoperable and standards-based environment for encrypted credentials (health pass) all within the holder's smartphone. A virtual wallet also ensures that credentials are inextricably linked to the holder's identity.

For sports enthusiasts, the spread of the pandemic has dramatically transformed the fan experience that has long been an ingrained part of the weekend routines for friends and families. While the inability to visit stadiums, the introduction of invisible crowd noises, and the stringent COVID protocols enforced on athletes have reshaped the way we experience sport events, the health and safety of fans and athletes is rightly being prioritised.

It's our hope that with the help of the technologies mentioned above, the whole industry can start to return to a sense of normality in the coming months. Not only will event organisers be able to feel confident about getting fans back into stadiums in the safest manner possible, but fans can also rest assured that the risk to their health is minimal.

Organisation:	*Thales*
Name:	*Kadie-Ann Fyffe*
Telephone:	*+ 33 1 55 01 54 26*
Email:	*kadie-ann.fyffe@thalesgroup.com*

14. Veridas: COVID passport as a tool for economic growth

The global state of alarm caused by the coronavirus pandemic has altered our lives in many ways.

We have all had to modify our routines, even the most deeply rooted, to effectively combat this virus that has caused such an economic impact.

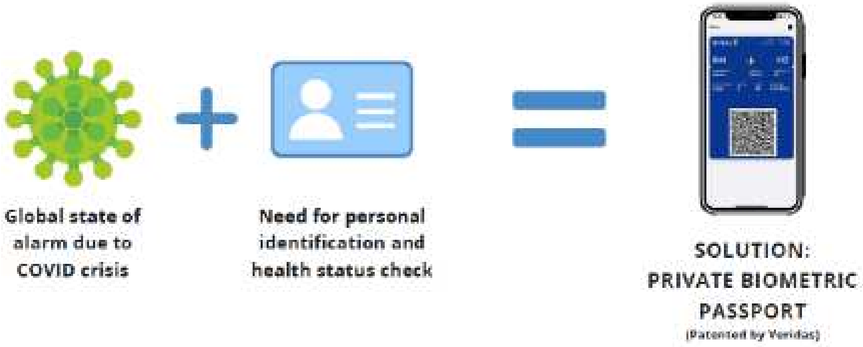
One of the main consequences of COVID-19 has been both global and local mobility reduction. Since the beginning of the pandemic, tighter border controls and limitations have been a must to avoid the expansion of the virus.

With the arrival of the vaccines at the end of last year, we glimpsed the return to normal life, however, maintaining a high level of security is still and will be vital to achieve this. Not only for personal or mental health wellbeing but also for the creation of the required environment for the economy to start recovering or even thinking of potential growth.

In this sense, one of the main levers of economic recovery for specific countries is the possibility of relaunching tourism, undoubtedly one of the most affected economic sectors. It should be remembered that foreign tourism accounts for a large part of GDP in most European countries, such as Spain, where it represents 6%, Croatia, 20%, or Portugal, with 10%.

Having this in mind, a Covid Passport project has been forged within the European community with information on vaccinations received or tests performed by the carrier. But, is this enough? How will we know that the passport corresponds to who it claims to be its rightful owner? Without including additional security measures, could this passport become a safe-conduct for people who are not vaccinated? How are the authorities able to assess the validity of a PCR test performed by a foreign entity or clinic?

A private biometric passport, that includes information on our vaccination, will allow for an efficient and secure way to gradually open borders with the confidence that the virus will not be massively spread again.


Global state of alarm due to COVID crisis
Need for personal identification and health status check
SOLUTION: PRIVATE BIOMETRIC PASSPORT
(Patented by Veridas)

Biometric passport: private and irreversible

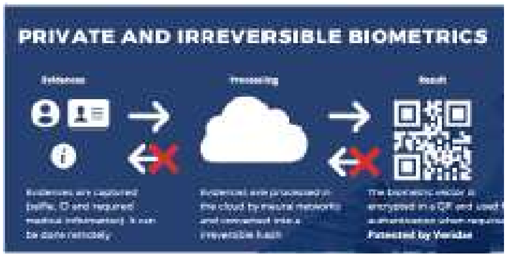
A biometric passport will provide security and privacy to citizens. It is critical to reinforce security controls while keeping an eye on usability if Europe wants to achieve a great adoption of this new proposal by the general population.

The use of facial biometrics technology should be considered to associate each health passport to a natural person through their biometrics in a completely private way and easily verifiable by the authorities.

Through a simple onboarding process, performed remotely and where all the evidence (selfie, ID & required medical information) is captured, an irreversible biometric vector would be generated and encrypted into a QR code. The credential, like an ID card, will only be in the hands of the patient, and will not need to be stored for verification by the authorities. Instead, verification could be carried out with a mobile device by scanning the QR code and taking a picture of the owner to compare the information.

This process of transforming evidence into a QR code, making sure that individual carrying that ID is who they say they are, will be carried out by cloud-based neural networks, converting all this information into an irreversible mathematical hash.

Veridas-FaceQR is a service offered and protected by patent PCT/EP2017/081317 owned by Veridas that enables the authentication of a person using facial biometrics. The biometric comparison process is performed between a facial image and an abstract representation of the person's face stored in a private, biometric QR format.



It is worth mentioning that this entire process is certified regarding security and privacy at all levels e.g. through iBeta certification for ISO 30107-3 for advanced liveness detection capability and management system is fully certified under the ISO 27001. This solution has been built under the most strict data privacy requirements.

Health certificate Process

Veridas suggests the following two steps for the generation and subsequent verification of the biometric passport:

Health certificate generation

Health professionals working for certified health organizations are allowed to generate health certificates. These certificates contain information about the traveler's health status, the health professional and organization issuing the certificate (employee & organization IDs), and the timestamp of creation.

Health status verification

The authentication of the Private Biometric Health Passport by using biometrics, provides evidence that health status belongs to the individual that is using it without any doubt, removing any fraud or impersonation risk.

Main advantages

Privacy

No data is stored in the provider's servers. The traveler is the only owner of his/her data. All data in the Private Biometric Pass is encrypted. This data can only be decrypted by Supplier's ' API, and only if a selfie of the legitimate holder is received in the request together with a PBP reading. Therefore, even the loss of a PBP does not expose any personal data. No person nor system, not even supplier's biometric engines, can reconstruct the facial image of the spectator from the PBP.

Security

Two-factor authentication, checking something the user has (PBP) and something the user is (face biometrics). The face recognition engine is subject to constant improvement in terms of precision and liveness detection and is presented to continuous evaluation by the NIST, assessed as one of the top engines in the world.

Global & accessible

The proposed solution to generate private biometric passes is cloud-based, fully international, and suitable for developed and developing countries. The private biometric passes can be presented in physical or electronic form to the biometric terminals.

Health safety

The proposed solution allows the creation of a private biometric pass that allows airlines and security staff to verify if a person has been qualified by a health professional as healthy, infected, immune. etc. This health information is univocally linked to the credential holder through face biometrics. The proposed solution allows each government and airline to use different travel rules depending on the country of origin, destination, as well as health check status and date. This technology can be used for the control of infectious diseases other than Covid-19.

Organisation:	*Veridas*
Name:	*Mikel Sánchez*
Telephone:	*+34 676 11 44 16*
Email:	*msanchez@veridas.com*

15. WorldReach: Digital onboarding after the pandemic: A checklist for success

As vaccination programs expand and COVID-19 cases drop, thoughts are turning to life after the pandemic. What will our new normal look like? What have we learned and what changes will persist?

One safe bet is that citizens will demand and expect remote, digital onboarding into both government and commercial services. The public appetite for sitting in waiting rooms and handing over paper documents – already waning before the pandemic – has gone forever. The post-COVID citizen knows that digital options are available, and expects service providers to offer them.

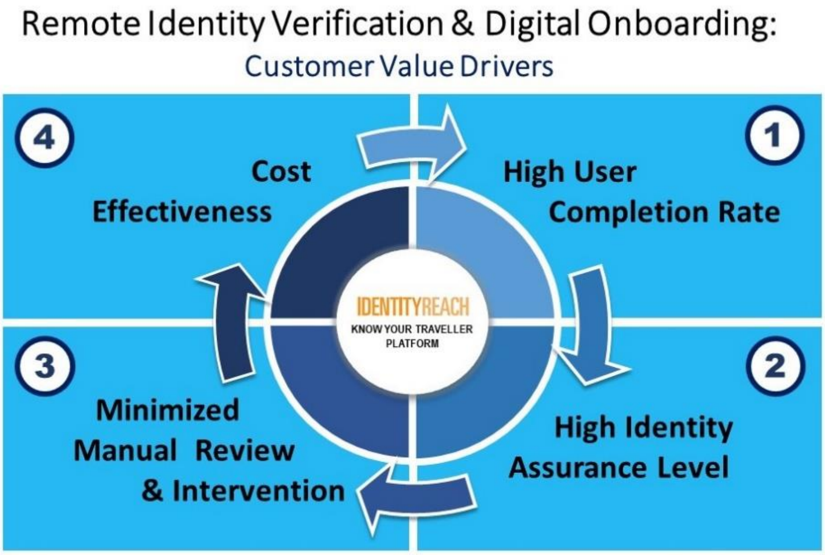
But this is about much more than buying some shiny new tech. To make a success of digital onboarding, service providers need to focus on the whole end-to-end process and the customer experience. For both government and commercial services, this is the only way to derive best value from digitization.

In the financial industry, the abandonment rate for digital onboarding is reported to be 63% (Signicat, *The Battle to Onboard 2020 – The impact of Covid-19 and beyond*). By comparison, in our work in government services, WorldReach has a successful user completion rate of over 90%. Why the stark difference?

At WorldReach, we are able to monitor telemetry data from ongoing usage (over 5 million transactions and counting), identifying opportunities for continuous improvement and examining the impact of subtle changes to see their results on the ground. As a result, we have developed a clear view about what works.

The diagram below summarizes our checklist for success: four key Customer Value Drivers that all service providers should consider when planning a move into digital onboarding and services.

We believe these four Customer Value Drivers can help agencies assess the impact of proposed designs, technology and user experience for each element of identity verification and digital onboarding:


Remote Identity Verification & Digital Onboarding:
Customer Value Drivers
1
High User Completion Rate
2
High Identity Assurance Level
3
Minimized Manual Review & Intervention
4
Cost Effectiveness
IDENTITYREACH
KNOW YOUR TRAVELLER PLATFORM

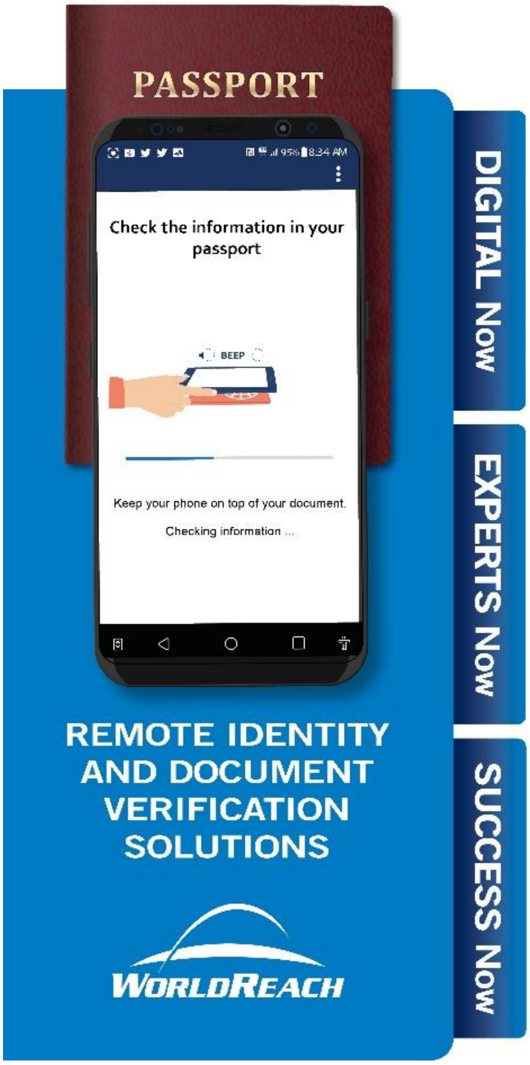
1. Achieving high user completion rates above industry norms: A service provider should offer high incentive or value to the end user to try the digital process. Once the end user decides to opt in to the digital channel, there should be a very high success rate of completing the process. This requires a logical workflow, clear user guidance, easy to use technology, and process innovation to ensure a good user experience. If these elements are all in place, service providers will minimize rates of abandonment, which provides no customer value and often creates a disincentive for others who may follow.

2. Achieving a high identity assurance level: This includes the level of verification of the e-chipped document and use of its secure facial images as a biometric reference, without having to gain access to a central database from the issuing authority. Many identity verification services rely primarily on optical scans/images of an ID document, with inherent security weaknesses for the verification process. It is difficult to obtain consistently high-quality facial images from a scanned or photographed document at the same level as a chip-stored biometric. This can cause repeated customer attempts, leading to abandonment and/or a low-quality image for the reference photograph. This, in turn, can lead to more attempts at manual confirmation. There is also a need to ensure the facial image meets appropriate criteria for 1:1 facial matching that is sensitive to the circumstances of the user. Liveness (or genuine presence) is a further example of the recommended security measures, along with corroborating information needed to achieve high identity assurance (e.g. see UK Good Practice Guide 45).

3. Achieving minimized manual review/intervention: The degree of success achieved on the above issues will greatly affect the ability to meet a threshold for automatic processing and so allow minimal manual human review and acceptance. Manual review, if used routinely, will slow the process to the point where end users may abandon and so will not be easily scalable or cost effective. There will always be instances where manual adjudication and approval is deemed necessary, such as suspected fraudulent activity, or other circumstances where it is not possible to meet typical criteria for an automated review. The key is to ensure these cases are the exception and not the rule.

4. Delivering high cost effectiveness: This requires an end-to-end focus on doing it right the first time, rather than incurring unsuccessful attempts to launch, which tends to create bad reviews and user scepticism. It's important for service providers to choose technology companies with significant experience of similar deployments at high volumes, in order to benefit from lessons learned elsewhere. A poor rate of completion, low identity assurance results or high manual interventions can contribute to poor overall cost effectiveness, even if most technical components are individually running well.

What works in a demo version or early prototype is not necessarily the same as a service that is scalable to millions of people and able to deliver high completion rates to a high level of assurance, meeting customer's goals. There is considerable complexity behind a large-scale production implementation that can run on global ePassports or citizen eIDs across their multiple generations, plus the wide range of smart phone models and operating systems in use by the general public.


PASSPORT
Check the information in your passport
BEEP
Keep your phone on top of your document.
Checking information ...
DIGITAL Now
EXPERTS Now
SUCCESS Now
REMOTE IDENTITY AND DOCUMENT VERIFICATION SOLUTIONS
WORLDREACH

Any agency or company looking to move into digital onboarding should carefully consider not just the tech but the totality of the business processes changes that are required for success.

Organisation:	*WorldReach Software*
Name:	*Gordon Wilson/Jon Payne*
Telephone:	*1 (703) 883-7022*
Email:	*Jon.Payne@worldreach.co.uk*