COVID-19: Effective and responsible biometrics solutions and concepts in a time of pandemic – building a resilient response

May 2020

COVID-19: Effective and responsible biometrics solutions and concepts in a time of pandemic – building a resilient response

Contents

1. Introduction

As the world faces new and unprecedented challenges, opportunities arise. Building a resilient community and providing a trusted source of information is extremely important.

The Biometrics Institute membership represents over 240 member organisations from around the world with a network that is close to 10,000 individuals, many of them experts in their respective fields.

During April 2020, the Biometrics Institute launched several new initiatives to provide its members with that timely and trusted information. This includes a news digest to members – a compilation of national and international news stories that our expert groups monitor – and a short survey on contactless fingerprint scanners. We now have invited our supplier members to submit papers addressing, "Effective and responsible biometrics solutions and concepts in a time of pandemic – building a resilient response."

These expert papers have been compiled into a document that we can share with our members and extensive wider network and on our social media channels. This is likely to be the first of other publications the institute will collate for its members.

We focused the submissions on addressing critical questions organisations are facing at this time and explain how any available solution is effective in this crisis. As new products are often of interest, we have allowed our members to place an advert into the report.

Proposed themes for the report were:

- 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

Please note that the institute is not endorsing any of the submissions but is sharing them with its members for information purposes which may help generate important discussion at this challenging time. I would like to thank these members for their contributions.

If you have any questions about the content of the submitted papers, please contact the authors directly.

For anything else e.g. if you are interested to join one of our online meetings discussing these topics or to discuss a future publication, please contact me.

I hope that you are all staying safe and healthy.

Yours sincerely

Isabelle Moeller
Chief Executive
Biometrics Institute
manager@biometricsinstitute.org

2. Auraya: Voice biometric applications to assist in pandemic times

A pandemic can disrupt and alter the livelihoods of everyone. Lives and circumstances can forcefully and drastically change. We must adapt to minimise the danger and reduce the disruption to our complex lives. While no one wants to experience the devastating loss of life, economic hardships and inconvenience that the pandemic has thrust onto populations during these strange times can be a catalyst in introducing changes that otherwise could take decades. Perhaps we will never again be so open to changing habits. For years people have resisted the opportunity to work from home, and now that we have been forced to adapt, many now work from home where it makes sense! Another forced change is the use of video conferencing technologies to stay in touch with friends and family. This new means of staying in touch may bring families together long after the virus is defeated. Perhaps business travel will change with more virtual conferences instead of the overuse of big global conferences. Many technology solutions are being delivered to tackle practical living issues in the locked-down world we have been forced to embrace. From fast-tracking new ways to invent and test medicines and create personal protective equipment to online conferencing, home deliveries, and exercising without large communal gyms. People and organisations have proved rapid change is possible, given the right circumstances.

These changes also introduced a new era of trust and cooperation as perfect strangers adapt to new rules around social distancing and people are making personal sacrifices to ensure the safety of unknown community members. In this era of more trust, it is important to reduce the ability of ‘bad actors’ to take advantage. Voice biometrics provides a key element in enabling open and transparent trust to exist as, quietly and unobtrusively, bad actors can be identified and dealt with appropriately, during digital transactions and phone conversations, leaving the rest of us to get on in the new world with more confidence.

As we become more community conscious, we are prone to become more fearful and concerned about our privacy and security. Voice biometrics provides consumers with a simple yet secure and private way to confirm identity with government agencies and other organisations we have entrusted with our assets and personal data.

Auraya’s voice biometric technology is being used to ensure secure, safer and easier conference calling capability. Cisco’s WebEx conference users can have voice biometrics enabled to gain access to conference calling service on their computer or mobile device by simply saying their name. If their voiceprint has been previously enrolled; and they are invited to the meeting then authorised conference call attendees can gain access from any device. No complex number codes are required to be remembered or punched in. Every time someone speaks, their voice identifies them and their name is displayed. This security option also prevents unknown or unauthorised people from attempting to join conference calls just because they have the meeting room code. Conference hosts can search recorded conferences based on when a specific speaker contributes rather than which device was used, which is especially helpful where there are multiple attendees using one device. Educational institutions can ensure that students that participate in the conference are, in fact, the enrolled students and not a proxy.

Voice biometrics can be utilised in contact centres even when agents are working from home. EVA the Voice Biometric extension for Amazon Connect enables voice biometric solutions to be deployed in days using cloud based services. Voice biometric solutions can be added quickly and securely to existing Call Centres and ‘work from home’ Call Centres to improve efficiency and security, whilst ensuring regulatory compliance. As Call Centres and digital support services feel the pressure and stress of increased numbers of calls and messages seeking assistance, they are also having to cope with lockdowns in offshore Call Centre locations as well within their own cities. The increased demand in a time of constrained capacity is forcing organisations to adopt new processes and technologies.

Organisations can use voice biometrics to ensure that known or suspected fraudsters are identified and prevented in real-time from perpetrating fraudulent activity . Being able to quickly identify suspected fraudsters not only reduces fraud losses; but it also assists the organisation to efficiently deal with legitimate callers. Where the biometric technology is eliminating known fraudsters, then legitimate customers can be served with higher levels of confidence and with less friction caused by manual verification processes.

In addition to helping deal with fraudsters, voice biometrics can be used to confirm that the authorised Call Centre agent is engaged in every conversation with customers. Organisations can be assured that the authorised agent is the only person that can handle customer calls. Calls that require transferring between agents can also be transferred with confidence and regulatory compliance as each agent's identity is verified by their voice.

In addition to using voice biometrics to deliver improved efficiency and security in Call Centres, voice is being used in digital channels. For example, a new quarantine mobile app is being delivered in Latin America using Auraya's voice biometric technology to help enforce quarantine measures. The app uses geolocation technology to ensure that the smartphone remains in the designated quarantine location and random requests for the quarantined person to verify their identity using their voice from the device ensures that the person subject to a quarantine order is with the device at the right location.

This quarantine mobile app can also be used to manage the crisis that exists in some correctional facilities worldwide. The COVID-19 pandemic has raised concerns about the vulnerability of inmates to the disease once it infiltrates correctional facilities. There are calls for a temporary release for some inmates to reduce the danger. The voice biometric mobile app combined with the smartphone geolocation technology can assist in monitoring the locations of inmates that are released to home detention. This allows correctional facilities to implement temporary parole while using this voice biometric system to continually and accurately track their whereabouts.

Organisation:	*Auraya Systems Pty Ltd*
Name:	*Paul Magee*
Telephone:	*+61 418255938*
Email:	*paul.magee@aurayasystems.com*

3. Biometix: Ensuring effective COVID-19 biometric technology solutions through testing

COVID-19 is driving opportunities for companies to provide technology solutions that meet the challenges of our new reality. Some of these solutions are repurposing existing solutions for different environment, whilst others are completely new applications. In the rush to COVID-proof your agency or business, how do you know that the product or service you are purchasing will really meet your current and future requirements?

Examples of some of the technology solutions being offered in response to this include:

- Border control: The use of touchless technology, i.e. contactless fingerprint scanning
- Remote work: Remote authentication of users using biometrics
- Consumer Apps: Biometrics used for mobile onboarding
- Surveillance: Face matching despite the presence of masks
- Immunity Passports: The use of biometrics to demonstrate immunity status

Many of these changes are occurring in a rapidly changing environment and require the consideration of urgent action to address these new challenges. In these situations, it is vitally important to ensure the right questions are being asked during the planning and procurement stages.

The kinds of questions to be considered during the planning stages might include:

- Have alternative methods of meeting the desired goal been explored?
    - For instance, rather than changing fingerprint readers, can the surface be sterilised using UV light or a protective coating?

- What independent validation is there about any claims of the technology's effectiveness?
    - Tests undertaken in-house by the seller maybe small scale and not a reliable indicator of real performance.

- Are there hidden integration or other costs?
    - Will you need to re-enrol users? Could it be that this technology might fail with certain demographics or conditions?

- How have security and privacy concerns been addressed?
    - A very accurate solution for recognition is of limited use if there are major other security or privacy concerns.

- What interoperability considerations should be included?
    - Will this data need to be shared? Does it need to be compatable with existing database or storage solutions?

Once a technology, or groups of technologies, have been selected the next phase is to undertake testing to validate the technology in your environment. The following are some general considerations about testing your solution:

- How will your tests be structured to produce accurate and statistically significant results?
- Will the solution perform as well under poorer quality conditions, perhaps where people are less compliant, or the environment is more challenging?
- What vulnerability and penetration tests should be performed?
- If your solution involves biometric matching, liveness and document reading, how do all these parts work together?
- Have applicable international standards been followed?
- Has the usability and human factors been tested with your population?

Based on our experience, we know that independent assurance and accurate biometric testing are the keys to making sure any response to the current crisis will not only meet its COIVD-19 related goals but also leave a lasting positive impact on future technology infrastructure. Independent expert advice ensures users can get the best value and outcomes from all aspects of their biometric and identification systems, laying the foundations for the effective and responsible deployment of any new technology.

Organisation:	*Biometix*
Name:	*Ted Dunstone*
Telephone:	*+61 419990968*
Email:	*ted@biometix.com*

4. Facetec: Secure e-voting in a difficult environment

The ability to vote in free and fair elections is the foundation of democracy. But most modern voting procedures are based on very old processes and technologies. And with the advent of the COVID-19 global pandemic, weaknesses in our electoral systems have quickly surfaced.

The first major US election held after the onset of the pandemic took place in Milwaukee, Wisconsin on 7 April 2020. Typical politics notwithstanding, being unprepared for the new circumstances and stay-at-home orders, in-person voting still took place, and several related problems - such as voters not receiving ballots, and thousands of completed ballots had been assumed to have gone missing - clearly foretold troubles to come.

On election day, a *New York Times* headline read: *Wisconsin Primary Recap: Voters Forced to Choose Between Their Health and Their Civic Duty*. *The Times* considered it, "An election almost certain to be tarred as illegitimate", and further, according to *Time*, "Wisconsin Fears Spike in COVID-19 Cases After Mid-Pandemic Election". However significant the problems were, this was only a primary election. Since, several primaries have been cancelled and the future of trustworthy voting is now in question.

The virus is expected to recur near the time of the national US election in November 2020. The US, and any other democratic nation, cannot afford to experience the problems Wisconsin did. Since in-person voting and mail-in voting are clearly not up to the requirements of a presidential election, alternative approaches must be presently considered.

It is important to use proven, robust Liveness Detection and official IDs to authenticate voters.

The US Congress has suggested a major shift to remote voting, with mail-in ballots as the most considered option. While mail-in will work for many voters, it was demonstrated to not be the most secure and trustworthy answer. But if an e-voting system is enabled, it must recognize without any doubt that only the correct person is casting a ballot and has direct access to it.

Voting is complex because of the logistics required to manage millions of people at thousands of locations, all on the same day. Bypassing all the physical challenges, and voting from voters' own devices, makes the process far more manageable, secure and cost effective.

Typical biometrics only compare two or more digital representations of human traits. For secure remote voter authentication, just "comparing traits" isn't enough. It must also concurrently measure "life," and to do that, robust Liveness Detection is needed.

Liveness Detection is truly the first principle of secure biometrics. But for a highly sensitive application like e-voting, the Liveness technology must be certified by a sanctioned third party, have years of commercial deployments to millions of users, and needs to be backed by a public spoof bounty, the only way a front-line application can stay ahead of the increasingly sophisticated and resourced attacks. Baseline testing in a lab is necessary, but cybercrime moves too quickly for testing organizations to keep up. Bounty programs are successful in the software industry, and the benefits of speed and transparency for biometric software are exactly the same.

FaceTec's system compares the user's newly collected 3D FaceMap with the government's on-file 2D photos of the correct voter. It then verifies that the 3D FaceMap was collected directly from a live, physically-present user – and not from a spoof artifact – with an exceptionally reliable Liveness check.

To illustrate, the entire process looks like this:

- A voter downloads the election app or visits the website.
- They enter a unique identifier, like their driver's license number.
- The camera on the voter's device is used to take a two-second video selfie.
- A 3D FaceMap is created from this video, encrypted and sent to the server.
- The voter's 3D FaceMap is checked for Liveness to ensure they are not a "spoof."
- The system looks up their unique number in the Government database, (like the DMV database), and compares the new 3D FaceMap to the ID photos on file.

  - If the 3D FaceMap and the 2D DMV photos match, the votes are counted.
  - For additional security, the Unique Identifier of the voter is run through encryption making it “hashed”, and the hash is stored on the server.
  - If a voter wants to ensure their vote was counted, they can re-enter their PII, it is re-hashed, and if there is a hash match in the database, then the vote is confirmed counted. The stored hash also prevents voting multiple times in the same election, and stores each vote anonymously.

The system can use existing election software that counts and anonymizes votes, like Microsoft’s ElectionGuard, currently being integrated by Neuvote. And by adding immutable blockchain technology, confidence can be increased that the votes are being cast and counted correctly.

Liveness Detection mitigates distrust in the remote election process. When voters prove their own Liveness and their identities, they will know every other voter has done the same, and, as long as the other components of the voting system are audited, that the results can be trusted.

Organisation:	*FaceTec, Inc.*
Name:	*John Wojewidka*
Telephone:	*+1.415.997.9235*
Email:	*johnw@facetec.com*

5. G+D Mobile Security: Biometric technology at the forefront of customer experience, security and privacy amidst COVID-19

BACKGROUND

The COVID-19 global pandemic has created a new normal for the world, which includes a low touch economy. With damaged trust in the hygiene of people and products, people are much more careful about who and what they interact with. Preference for contact free deliveries and payments prevail, in fact contact free payments have risen by 40% globally for Mastercard in the first quarter. Australia, along with many other countries, has increased the contactless limit, from $100 to $200.

The widespread use of biometric technologies in current COVID-19 responses, especially in the area of tracking and surveillance, has raised serious concerns about the violation of a user's privacy and security. However, biometrics can also be effectively applied in other areas. When biometrics are deployed in conjunction with existing security technologies and systems, they can help to prevent infection as well as enhancing overall security and usability while protecting user privacy.

Biometrics can improve user privacy and enhance the security of existing applications with minimal changes to existing infrastructure and systems.

One established and proven security technology that has received worldwide adoption is smart card based technology. This technology has been embedded in various form factors and devices that function through a variety of communications protocols, such as contact and contactless or near field communication (NFC), Universal Serial Bus (USB) and Bluetooth Low Energy (BLE). In recent years, smart card technology has emerged in new innovations across multiple industries. Biometrics should leverage smart card technology to facilitate higher usability, improved user experience and enhanced security and privacy.

STANDARDS & INTEROPERABILITY

The success of the smart card is underpinned by the support, collaboration and oversight of international and industry bodies in defining standards such as ISO (International Organization for Standardization), Global Platform, ETSI (European Telecommunications Standards Institute), EMV (Europay Mastercard Visa), FIDO (Fast Identity Online) and compliance to GDPR (General Data Protection Regulation) and PSD2 (Revised Payment Services Directive) regulations. All these work together to provide interoperability, competition and cost efficiencies while benefitting the public with a variety of choices. Users across different industries that adopt these standards can find multiple suppliers and don't have to rely on a single provider.

BENEFITS

Integrating a fingerprint sensor on a smart card has some clear advantages, benefits and value over a biometric fingerprint reader, including:

- The user's fingerprint template is securely stored on the smart card instead of the reader or a centralised biometric database.
- The fingerprint never leaves the smart card.
- The fingerprint matching is performed on the card, preventing the user's fingerprint template from misuse as well as protecting the user's privacy.

One important and everyday area for the potential application of biometrics is in financial services. A study conducted by Mastercard and the University of Oxford found that users have a high preference for biometrics.[1]

Overall, users believe that biometric authentication is more secure (83%) and more convenient (92%) than passwords.

PAYMENTS

The spread of COVID-19 has encouraged a shift away from cash to contactless payments. A biometric payment card can effectively work with existing Point-of-Sale (POS) infrastructure and addresses both the issue of PIN entry at the POS as well as the greater financial risk associated with the higher payment limit. With no PIN entry, the user can have a 'zero contact' seamless and secure payment experience. As the card is only enabled with a valid fingerprint (tied to the card), the unique fingerprint securely protects the card from use when lost or stolen. In terms of privacy, the biometric card can be PSD2 compliant.

An actual example of the everyday use of biometric cards is at Credit Agricole in France[2]. A more recent example of payment via a biometric Key Fob (device) is the Royal Bank of Scotland, in the UK.[3]

HEALTHCARE

The use of biometrics in Healthcare for user verification, physical and logical (computer and network) access and in securing medical transactions, presents an ideal area for multi-functional smart card biometrics. Additionally, a personal biometric card allows healthcare subsidies to be provided to the intended beneficiary.

Entry into restricted areas, especially those that already use smart cards, can be further strengthened with a biometric fingerprint device linked to an authorised user. This can prevent unauthorised entry into restricted healthcare facilities from a lost or stolen access device.

The biometric device can complement the user's authentication to healthcare IT systems (local and online) and support the organisation's Identity and Access Management (IAM) policies. User authentication based on Fast Identity Online (FIDO) specifications[4] provides a much simpler and far stronger security mechanism (than password-based authentication), and is designed with privacy compliance in mind for open and scalable systems across websites and apps.

The biometric device functions as a single authenticator with multiple applications.

With the inherent cryptographic capabilities in smart cards, the biometric device can also be effectively and securely used by healthcare practitioners to sign documents and perform medical authorisations electronically.

CONCLUSION

Biometric (fingerprint) capable cards and devices will play a major role in complementing the efforts of government and industry responses to COVID-19 by helping to prevent its spread and enhancing overall safety, while providing superior customer experience, security and privacy protection. These relatively new cards and devices are being trialled globally and expected to see a quick take-up to support the need for secure authentication and payments. This growth will inevitably also see the cost of these devices come down to a point where carrying a biometric card or keyfob in your purse or wallet will become as common as your traditional payment or ID card.

Organisation:	*G+D Mobile Security*
Name:	*David Tharm*
Telephone:	*+61 401 988 133*
Email:	*david.tharm@gi-de.com*

[1] https://newsroom.mastercard.com/news-briefs/overcoming-mobile-biometric-challenges-mastercard-and-university-of-oxford-collaborate-on-new-research-initiative/

[2] https://pressroom.credit-agricole.com/news/credit-agricole-tests-out-biometric-bank-cards-4da1-94727.html

[3] https://www.bbc.com/news/uk-scotland-scotland-business-50644378

[4] https://fidoalliance.org/

6. ID R&D: How biometrics enable a new and improved normal

In his book, *The Art of Winning in an Age of Uncertainty*, behavioural strategist Max McKeowen writes "All failure is failure to adapt, all success is successful adaptation." Across the world people are adapting to change in the midst of COVID-19. Consumers have altered everything from the way they shop, bank, and learn to how they seek medical advice. Likewise, businesses are reprioritizing, transforming, and rethinking ways to better serve their customers and employees, not just right now, but moving forward.

We can only speculate on the long-term impact of the current crisis but it will surely reshape society and business in lasting ways. Things that seem strange to us today, will seem normal in the future. Consider the fact that an 18 year old in the United States only knows post 9/11 airport security rules. The memory of walking a friend or family member to their gate is non-existent. Will the next generation have no nostalgia for greeting a new acquaintance with a handshake? Time will tell but one thing is certain, our resilience will result in innovation including ways to maintain business as usual – even when it's everything but.

Biometrics are among the technologies experiencing accelerated adoption in response to the pandemic. From enabling contactless access to validating digital identities and remote authentication, biometrics not only offer a way to cope with the current situation but also introduce advantages in the form of improved security, safety, and usability.

Three use cases that are better with Biometrics

1. Digital Onboarding

   Consumers have long shown an increasing desire for mobile and online banking options. However many financial institutions struggle to deliver effective Digital Onboarding processes for opening new banking and loan accounts. And banks are not alone as consumers look to sign up for a variety of services online -- from setting up new mobile service to replacing or boosting income in the sharing economy. Whether the business driver is compliance with Know Your Customer (KYC) and Anti-Money Laundering (AML) regulations, stopping repeat fraud, or ensuring a safe and secure marketplace, identity proofing is imperative.

   Biometrics improve security while simplifying digital identity proofing in a quick two-step process that has historically required human involvement. Face biometrics ensure that the photo on a government ID matches a selfie of the person who is signing up. Passive facial liveness detection prevents spoofing via the use of photos, cut out masks and video in the process.

   Why it's better with biometrics: *According to Deloitte, 38% of customers say user experience (UX) is the most important factor when choosing a digital bank. Biometrics make digital onboarding more secure and technologies like passive facial liveness remove friction from the process to improve usability and decrease abandonment in onboarding. Another advantage is lower costs by bringing automation to a previously manual process.*

2. Authentication for Remote Workers

   COVID-19 will lead to better preparedness to "go remote" — enabling many businesses to maintain productivity without face-to-face meetings, travel, and brick and mortar hours. With the right procedures, processes and tools in place, we can expect to see this trend stick in the form of greater work-at-home flexibility.

   Of course, security is a top concern for many companies who suddenly have the majority if not all of their employees working remotely and unprecedented stress on IT staff. More than one-third of senior technology executives surveyed by CNBC say that cybersecurity risks have increased with stay at home orders. Biometrics such as voice and face offer strong authentication for replacing traditional passwords all together, or as a second factor.

   Why it's better with biometrics: *Traditional passwords are easy targets for hackers, can be shared between employees, and are a frequent source of frustration for both users and IT staff. Biometrics with anti-spoofing offer a significantly more secure, yet frictionless form of authentication that employees can't forget or share.*

3. Contactless Secure Access

   A study in the *New England Journal of Medicine* found that COVID-19 can live two to three days on plastic and stainless steel. What started with wiping down grocery cart handles has progressed to a hyper awareness of the many things we come into contact with when we leave our homes. Keypad payment systems, self-service kiosks, and protected physical locations still largely require authentication via something we know, like a PIN, or something we have, like an access card -- and these things require hands-on interaction.

   Biometrics, including voice and face, offer a contactless way to verify a person's identity. In the current environment, this technology could help reduce virus spread in business offices, hospitals, airports, and other secured locations which often rely on fingerprint readers, card access, and or manual identification checks.

   Why it's better with biometrics: *Limiting physical interaction with high-traffic devices is one way to help reduce virus spread. Biometrics also improves security by protecting physical access based on something you are vs something that can be lost, shared, or stolen.*

These are just some of the ways that biometrics can help businesses and consumers adapt to the current reality and long-term change caused by COVID-19. In many cases businesses are accelerating their digital transformation and security initiatives, as well as coming up with new innovations that will position them for future resilience and growth.

Organisation:	*ID R&D*
Name:	*Kim Martin*
Telephone:	*+1 407-928-3320*
Email:	*kim.martin@idrnd.net*

7. Ideco: Biometrics and hygiene – protecting your customers' existing investment

Since touch-based biometrics was first introduced for access control or time and attendance purposes, hygiene was frequently raised as a concern. Labour unions specifically objected against the use of biometrics on the basis of hygiene, but completely ignored that during a normal day in our lives one would touch numerous objects, whether intentionally or not. These may range from door handles, shopping carts, elevator buttons, parking ticket dispensers to POS terminals where you need to enter your pin number to complete a transaction.
With the global outbreak of the COVID-19 pandemic, these hygiene concerns have again been pushed into the spotlight, especially with the virus being spread via particles left on surfaces. It is therefore important to realise the risks and address it in a responsible manner that alleviate the current fear and panic in using touch based biometric solutions.

For obvious reasons manufacturers globally are touting touchless biometric solutions as a replacement of their touch-based siblings. Even though these touchless technologies may work in most use cases, replacing the current deployment will have a massive economic impact on organisations who are already financially distressed. With the current economic crises due to lockdown regulations, most organisations will put hard brakes on the re-investment of infrastructure or enhancements especially where the current infrastructure is still operating and performing the function it was initially invested for.

Make them safe to use

This raise may valid questions amongst customers. How do I protect my current investment and safeguard against the COVID-19 virus or any other communicable diseases? Is washing or sanitizing hands before and after using the fingerprint biometric terminal feasible and will it impact the user experience negatively? How often do I clean the biometric reader and what do I use to disinfect it? What will the long-term effect be of alcohol-based sanitisers on both the reader and the user's fingerprints? What next then?

The CDC (Centre for Disease Control in USA) has released a list of registered products tested and approved for disinfection of hands and equipment as well as the destruction of COVID-19. Straight alcohol is not sufficient as it evaporates from the skin within 15 secs and needs at least 1 minute to be effective. Alcohol based sanitizer with added biocide at 5000ppm (generally known as Quaternary Ammonium Compound) leaves a layer of biocide on the skin, which then has time to destroy the fatty shell and hence the virus.

The World Health Organisation and many other medical research institutions have also done extensive research on how to kill viruses and bacteria in other ways than the traditional methods mentioned above. These include the use of O_3 (Ozone gas) in a closed system guaranteeing no escape of the Ozone gas for the treatment of many diseases including SARS and AIDS and the use of ultraviolet light or UV light. Many of these solutions are now being applied in medical environments to sanitise the environment or has been deployed by city authorities in China and South Korea to sanitise public transport, in example.

Germicidal UV light (also referred to UVC with wavelengths less than 280nm) is used in hospitals and medical centres to clean rooms and equipment, but it's generally regarded a health hazard to humans as continuous exposure may cause skin irritation and eventually skin cancer.

Dr David Brenner, director of the Columbia University in New York Centre of Radiological Research, has been studying how to use UVC to prevent the spread of diseases for years. Brenner's team has since tested UVC against two seasonal coronaviruses, and is now testing the strain responsible for the pandemic, SARS-CoV-2. "We saw we can kill 99 percent of the virus with a very low dose of UVC light," Dr Brenner told ABC News " and there's no reason to believe it's going to be different for the novel coronavirus".

Disinfect readers, don’t replace them

Based on this research, Ideco Biometrics has patented and developed Steri-C, a device that can be retrofitted to most existing fingerprint readers. Steri-C uses UVC to burst the surface area of a touch based fingerprint reader directly after every use and then goes into safe mode to limit any potential risk of exposure. A dose of no less than 2,0 mJ/cm^2 is the calculated exposure that will result in a fractional survival of ±10^{-2} based on the Influenza A virus (H1N1). All reports indicate that the Covir-19 virus is in fact not as tough as the H1N1.

Although the UV exposure is extremely low, directed and fully controlled, Steri-C also employs an industrial processor to strictly manage the proximity sensor to switch off the UV when a finger approaches the fingerprint sensor.

As with any other product of this kind, Ideco cannot give a 100% guarantee that all microorganisms left on the surface area of the biometric reader will be destroyed. There is however sufficient scientific proof that the correct dose of UVC will kill bacteria and viruses. These solutions need to be adopted to current infrastructure to allow for the safe and continuous use of the enormous investment already made in touch-based biometrics.

Steri-C - Ultraviolet disinfection to ensure the safe use of your fingerprint reader

- Easily mountable on existing fingerprint readers.
- Controlled exposure to minimize risk of irritation.
- No adverse impact on operations or accuracy.

* Steri-C = Patent pending

☎ +27 (0)12 749 2300 ✉ sales@ideco.co.za

Organisation:	*Ideco*
Name:	*Francois Vermeulen*
Telephone:	*+27 12 749 2300*
Email:	*francois@ideco.co.za*

8. IDEMIA (France): Is a change of paradigm to be expected in air travel?

Since COVID-19 hit our world, the latter has been heavily impacted on an unprecedented level, particularly from a health point of view. Large parts of the economy have also been severely affected, and the global aviation industry is no exception with flights down by 80% by the end of April.

Even if our way of living has been drastically impacted during the last few weeks or months, our desire to travel, to discover the world will remain. However, once the current crisis has passed, as we all hope it will, new expectations will arise and a new paradigm will no doubt emerge.

Taking this shift into account, what will this “new normal” look like, especially when it comes to travel?

No one has certainties. But this new normal may be two-fold:

- More contactless and hygienic processes to safeguard both travelers and personnel
- Additional health screenings or health status checks in order to guarantee that those who travel are safe and are not putting the country they visit at risk

Contactless processes coupled with biometrics could pave the way for a more hygienic airport journey

The passenger journey within an airport is currently made up of various so-called “touch points”: check-in, baggage drop-off, security screening, border control, boarding for instance. The “touch point” terminology may not be adequate for a sanitary crisis like COVID-19, but it reflects the challenge that airports are facing.

Before the COVID-19 crisis, the International Air Transport Association (IATA) had already launched the OneID initiative, which aims at providing a seamless, self-service experience for passengers, and where biometrics is the key token to get through all these touch points by replacing documents such as boarding passes or passports.

This initiative is needed now more than ever, but should be reinforced by taking into account the new sanitary concerns. Passengers do not just want self-service or fast processing now, they will be required to not touch anything, be it a screen on a self-service kiosk or a boarding pass scanner at the boarding counter.

As equipments such as self-service kiosks are set to remain in the future, for legal or practical reasons (including the automation it allows, thus enabling social distancing), it will be key to find new ways to interact with such equipment, other than using touch screens that are touched by hundreds of travelers every day. Various ways to reach this touchless interaction are possible. Voice recognition, eye tracking and gesture recognition for instance are obvious candidates, though they might come with ergonomic challenges to be really inclusive of all types of travelers. Other innovations are therefore to be expected soon and should now be proposed by the industry and tested by the airport stakeholders to define those which are the most relevant.

Beside these interactions such as voice, eye tracking and gesture recogniton, and as pushed by IATA, biometrics can obviously play a critical role in achieving a 100% contactless passenger experience.

Face recognition is by definition contactless, and so is iris recognition with new generation technology. Indeed they can be performed at a distance and already meet the expectation for a touchless process. Face recognition with sanitary masks, however, can only be ensured by a handful of leading biometric providers, and even with the best-of-breed algorithms will always be a compromise compared to recognizing an unobscured face. In this context, iris recognition potentially coupled with face recognition such as in the OneLook™ equipment developed by IDEMIA and already in use in some major airports, is a good candidate to help achieve this 100% contactless passenger experience.

When it comes to fingerprints, the legacy biometric modality of choice, it is generally assumed that such a technology requires to physically touch a sensor. However, the latest developments clearly show that a 100% contactless experience can also be achieved for fingerprints: IDEMIA’s Morpho*Wave*™, which enables travelers to be identified by a simple wave of the hand in front of the sensor, or IDEMIA’s DirectCapture™ technology, which can be simply deployed in a smartphone or tablet app making the most of their embedded camera to check fingerprints, show that this biometric modality is also already part of this new contactless reality.

This is a major improvement that could enable authorities, especially Border agencies that require the use of biometrics, to continue operating the way they want, by capturing any combination of biometric data they request, while being able to offer a contactless experience.

Additional health screenings and health status checks to ensure everyone can travel safely?

The new paradigm resulting from the COVID-19 crisis might also require additional controls compared to what is currently being done. And these controls may be related to the health status of each passenger.

In order to be able to travel, passengers will possibly have to declare or prove that they are healthy safe. It may thus be expected that the required travel documents, such as passport, visa, electronic travel authorization or arrival cards, will integrate some data related to the health status. Additional documents which can potentially take the form of a sanitary passport could also be requested by authorities.

And all this valuable data could be integrated into the existing border control systems, as well as the interactive Advance Passenger Information systems or Passenger Name Record analytics solutions, so as to allow relevant government agencies to perform the necessary controls in advance, welcome those who are identified as safe and take appropriate measures for others.

In addition, this data could be used by some risk assessment tools that could also support authorities in spotting travelers that might represent a level of risk. Understanding the complete travel history in order to see if the traveler has not flown from or transited in an area at risk prior to their arrival at their final destination, or being able to target all the passengers that were sitting on a plane close to a potentially affected person could be of interest, although an appropriate balance between security and privacy will always have to be examined carefully.

These risk assessment solutions that are already designed to perform similar targeting will possibly have to adapt to integrate new business rules that take into account epidemic threats such as COVID-19.

Now, if these measures may prove to be valuable, they will probably have to be complemented by other elements such as in-situ temperature checks when passengers present themselves at the airport. Among various health checks temperature checks, as they have started to occur in some places since the crisis emerged, might help the authorities in detecting passengers that are potentially ill.

This process was already implemented years ago in African airports, when the authorities were fighting against the Ebola virus, and have proven to be efficient and one of the most pragmatic ways to ensure safety for everyone. As stated above, they can also be coupled with other measures.

Various technologies can be used to measure the temperature with varying accuracy and levels of cost, but also requiring different set-ups possibly coupled with biometric checks occurring at existing touch points.

In this regard, one can expect technology providers to continue to support the air transportation industry in meeting the challenges they face by proposing relevant and effective solutions, while still paying close attention to the recommendations that will come from the competent authorities such as the World Health Organization.

All in all, these additional screenings coupled with an even more contactless biometric experience will be key in reducing health threats and enabling the air transportation industry to regain the confidence of the general public. This contribution is essential to making the whole industry resilient, and it is critical to ensure the safety of citizens and travelers alike, while ensuring a smooth journey through airports.

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

Access Granted

9. IDEMIA National Security Solutions (USA): Contactless identification in a time of pandemic

Novel coronavirus 2019 (SARS-CoV-2) has upended the world, including the identification world. So far as we are able, we now minimize contact with people, surfaces and avoid the exchange of paper. In the biometrics community we immediately think of our first biometric, fingerprints. The "gold standard" in fingerprinting, for over 100 years, has been the tenprint. That is to say, a nail-to-nail rolled impression of all ten fingers, coupled with plain impressions of the four fingers joined of each hand, and the two thumbs.

Done well, even done poorly, capturing the tenprint extends over about ten minutes and entails close contact between the subject and an operator. Fingerprint impressions are made by papillary ridges on the fingers and thumbs. Until about 1990 fingerprints were captured with ink on special cardstock. Cleaning the fingers afterwards was an unpleasant task. Today prints are primarily captured with various live scan technologies, optical being most common. Pores, irregularly spaced about the fingers, secrete a tiny amount of sweat when we grasp something hard and smooth, which helps in grasping. It also leaves smudges on sensor platens requiring cleaning.

Of course, the fingers are three dimensional objects. Collecting impressions in two dimensions introduces nonlinear distortion in the images due to skin plasticity. Uneven pressure in the fingers during rotation, dryness of the skin, sweat, dirt, grease, humidity and other factors result in non-uniform contact with the sensor platen and noisy images. So no two tenprints will be exactly the same.

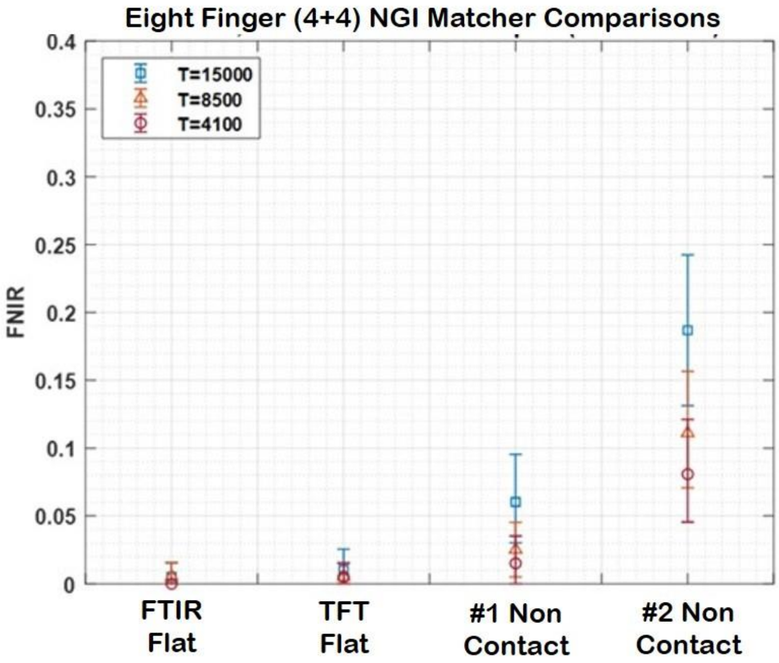
Disadvantages of close continuing human contact, long capture time, and inconsistent resulting images are long known. Readily acceptable for criminal justice purposes, tenprints have proven problematic for other applications, such as international arrivals, where even seconds of additional delay impact queuing time. Now, we have learned from the pandemic that viruses linger on surfaces, at infectious titer levels, for days.[1] Touching the same surface, unless cleaned after every use, is a disease vector.

Yet we cannot move away from fingerprints, as was done with Bertillonage a hundred years ago, for identification. Many applications require positive identification. Facial recognition, despite tremendous progress, did not reach that level of accuracy before we entered the age of widespread use of masks. It will take time, if ever, before periocular, eyebrow, forehead, and ear based identification can rival fingerprint accuracy. Iris identification certainly has adequate accuracy. However high cost, a tiny installed base, failure to capture issues, coupled with miniscule existing reference galleries make iris an unlikely replacement for fingerprinting in the foreseeable future.

While the pandemic brings a new sense of urgency, issues with contact fingerprinting were long known. In 2004 a fast capture effort, across the US Department of Justice, launched with the objective of capturing ten rolled-equivalent fingerprint impressions within 15 seconds. Between 2006 and 2008 the National Institute of Justice with several federal partners made four R&D awards and during 2007 to 2009 led to prototypes which while not ready for operational use did advance the state of the art. In 2015 the National Institute for Standards and Technology (NIST) announced a Contactless Fingerprint Capture Device Measurement Research Program. Work under that initiative continues to the present, supported by federal departments, with active industry participation. Both specialized fingerprint capture devices and applications using conventional digital camera for image capture continue to be studied. In 2017 the Intelligence Advanced Research Projects Activity (IARPA) issued a prize challenge for a nail-to-nail "live fingerprint capture device that does not require a human operator, [is] capable of biometric recognition as good or better as the existing standard, and does so in the same or less time as the existing approaches." Eight challengers responded and while the requirements for the Grand Prize were not quite met, when prizes were awarded in 2018, the state of the art again advanced.

The Biometrics Institute conducted a survey, finding as of May 2020 that two commercial contactless capture devices are available with a third in development. Three Smartphone camera based applications are available with a fourth in development. The NIST research program has examined the contactless capture devices and found performance roughly comparable to existing optical and capacitive flat fingerprint capture devices.

[1] Aerosol and Surface Stability of SARS-CoV-2 as Compared with SARS-CoV-1, The New England Journal of Medicine, March 17, 2020, https://www.nejm.org/doi/full/10.1056/NEJMc2004973, and Persistence of coronaviruses on inanimate surfaces and their inactivation with biocidal agents, G. Kampf, et. al., Journal of Hospital Infection, January 31, 2020, https://www.journalofhospitalinfection.com/article/S0195-6701(20)30046-3/fulltext



Traditional tenprint performance, especially for latent fingerprint matching, has not yet been achieved. For criminal justice use more work is required. However, in the United States 60% of fingerprint checks against the national criminal history files are for non-criminal justice purposes. The commercial non-contact devices have both been certified for personal identity verification (PIV), but for technical reasons cannot be certified under Appendix F of the Electronic Biometric Transmission Specifications (EBTS). Yet, they demonstrably work well enough for operational use. The need is real, and urgent, in this time of pandemic. Time will tell if processes can rapidly adapt to allow their use.

Organisation: *IDEMIA National Security Solutions*
Name: *James Loudermilk*
Email: *jim.loudermilk@idemia-nss.com*

10. InnoValor: The importance of NFC-based remote identity verification in a resilient society

Abstract

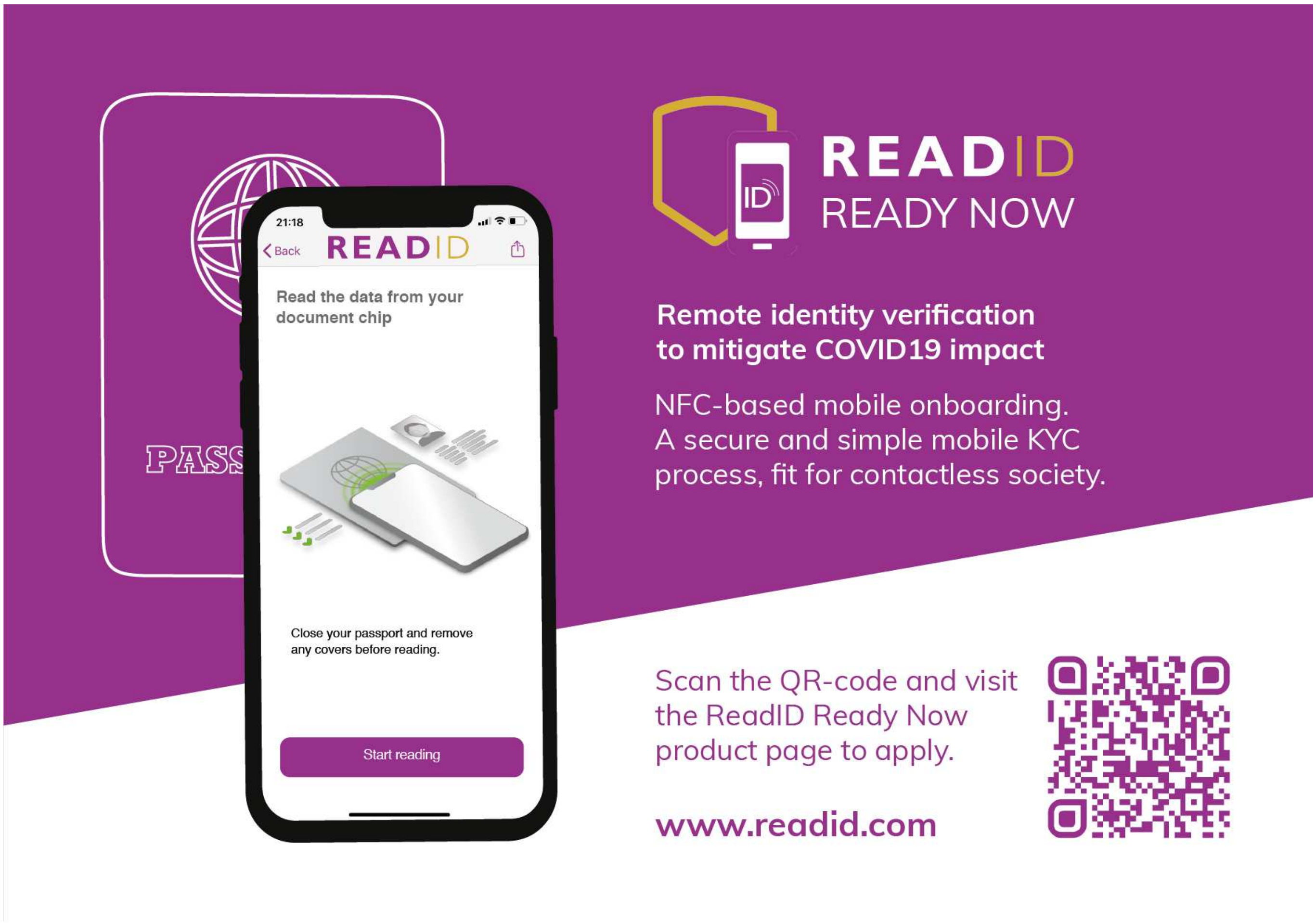
The shift towards a contactless society has increased pressure on organisations to loosen their KYC restrictions in order not to block transactions. This increases the risk of identity theft, which criminal organizations are actively exploiting. This paradox can, however, be resolved: NFC-based mobile onboarding makes it possible to bridge create a secure and simple mobile KYC process, fit for contactless society.

The trust paradox

Identification, typically, required physical presence: checking the identity document and verifying the holder is actually holding it. And many transactions require identification because of regulatory reasons and/or to reduce risks. The COVID19 pandemic created a shift towards a contactless society, hampering secure identification, blocking transactions that require Know Your Customer (KYC). Pension funds need *attestae de vitae* for their customers, healthcare institution need to know who they are dealing with, notaries must ensure correctness of real-estate transactions, and schools need to know who has passed the exam remotely. Organisations can lower their identification restrictions, increasing the risk of identity theft, or stop their businesses. An impossible dilemma, so it seems.

This dilemma, however, is not a dilemma by a paradox that can be resolved through technology that is widely available: electronic identity documents and smartphones with NFC capabilities. The same NFC chip in mobile phones that enables payment, also enables mobile identity verification. NFC can be used to enable remote verification with a smooth customer experience, with a high level of security at a lower cost.

This approach is not new. It is used increasingly in, for example, mobile onboarding for banks, moving into 24x7 digital services. Traditionally, KYC comes with visits to branch offices. Time consuming, costly and limited to office hours. Nowadays, if a bank cannot deliver fast enough or creates, in the eye of the customer, unnecessary hurdles in the process of becoming a customer, a digital competitor is virtually around every corner.


PASS
21:18
Back
READID
Read the data from your document chip
Close your passport and remove any covers before reading.
Start reading
ID
READID
READY NOW
Remote identity verification to mitigate COVID19 impact
NFC-based mobile onboarding. A secure and simple mobile KYC process, fit for contactless society.
Scan the QR-code and visit the ReadID Ready Now product page to apply.
www.readid.com

At the same time, regulatory pressure increases: anti-money laundering legislation has led to substantial fines already in the financial industry. The importance of high-quality KYC processes is higher than ever. Digital solutions for KYC have been in the market but have their disadvantages. Optical solutions using photos of identity documents are not secure, video identification solutions in which customer wave their identity document in front of a camera are invasive and costly. Both have a poor conversion and take too long.

How does NFC work in remote identity document verification?

Modern passports are great; they are equipped with a NFC chip following the ICAO 9303 standard. This chip contains similar information as is printed on the passport, but with a number of crucial differences. First and foremost: all information is digitally signed and encrypted and cannot be manipulated. Also, the face image is available at a high resolution, without any additional watermarks. Therefore, they are much more suitable for face matching than the printed face image (look-a-like fraud). Finally, a copied chip can be easily detected. Also, most modern ID cards have the same chip, the EU even has a regulation mandating this for new ID cards.

The big breakthrough in this technology came with the availability of smartphones with NFC. Basically, all modern smartphones are equipped with NFC, often used for mobile payments. A smartphone can be used to read and verify the chips in identity documents, without the need for expensive additional hardware. This is a great opportunity: leveraging two things everybody has – a passport and smartphone – identity verification can be done remotely, with a great user experience and a high level of trust. For Android this was already possible for several years, and since September 2019 also iPhones can do this.

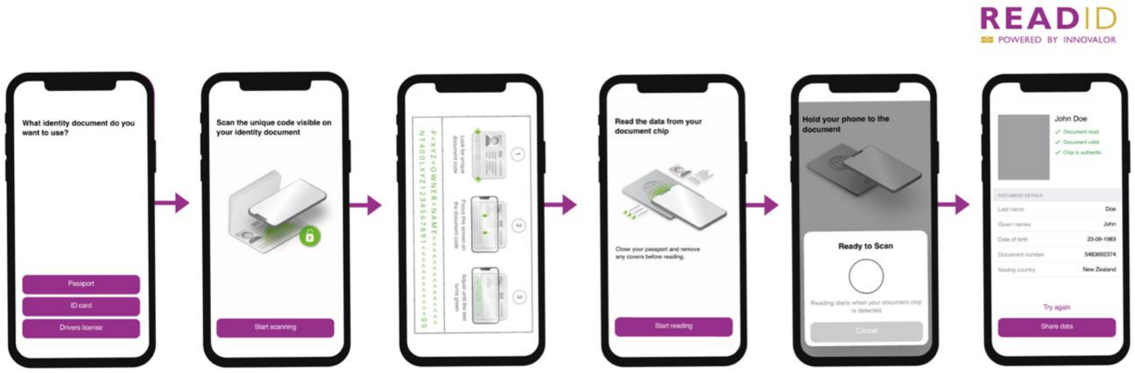

READID
POWERED BY INNOVALOR
What identity document do you want to use?
Passport
ID card
Drivers license
Scan the unique code visible on your identity document
Start scanning
P<XYZ<OWNER<NAME<<<<<<<<<<<<<<<<
NT400LXYZ123456789<<<<<<<<<<<<00
1 Look for unique document code
2 Focus the screen on the document code
3 Adjust until the text turns green
Read the data from your document chip
Close your passport and remove any covers before reading.
Start reading
Hold your phone to the document
Ready to Scan
Reading starts when your document chip is detected
Cancel
John Doe
✓ Document read
✓ Document valid
✓ Chip is authentic
DOCUMENT DETAILS
Last name Doe
Given names John
Date of birth 23-09-1983
Document number 5483692374
Issuing country New Zealand
Try again
Share data

Figure 1. User flow for remote verification with ReadID.

Our software product ReadID allows to do NFC-based mobile identity document verification (Figure 1). The app is used to read the chip, and our software at the server is used to do all kinds of verifications and send the validated information to our customer. For remote identification we cannot trust the smartphone, since an attacker can easily manipulate the smartphone. Verification therefore need to be done in a secure server environment which we provide as SaaS. ReadID can be integrated into customer apps, through an SDK, but is also available as a ready-to-use app, not requiring any form of technical integration. This is important to allow for a quick adoption in smaller organisations or NGO’s fighting the consequences of COVID19 that do not have the resources, or time, to do an integration.

A resilient KYC process

Reading the chip digitally allows to verify the validity of the identity document and read the customer information without the risk of any OCR or typing mistake. An important first step and sufficient for many processes. In a KYC process this can be extended with holder verification: we can also verify that the person owning the passport is currently holding the passport. This is done through face matching, including liveness check, as a second step.

Large banks such as ING, Rabobank and DNB Norway use our solution. The UK home office has incorporated our technology in their app for the EU Settlement scheme, allowing EU nationals that as a consequence of Brexit need a residence status to apply for this online. More than 3.3 million EU nationals already successfully went through this process. Not only large companies and governments use ReadID, for example, small notary offices use our solution to check identity documents without physical contact.

These use cases show that the trust paradox can be overcome. NFC-based identity document verification creates a smooth customer experience, combined with the necessary level of trustworthiness at a distance, at affordable cost. Using NFC is the way forward in resilient KYC processes.

Organisation:	*InnoValor/ReadID*
Name:	*Maarten Wegdam, Wil Janssen*
Telephone:	*+31 6 22403433*
Email:	*readid@innovalor.nl*

11. Innovatrics: Challenges for contactless access control

As one of the major providers of automated fingerprint identification systems, we have assessed that the coronavirus pandemic has accelerated the demand for face recognition modality based on the number of our clients and partners who upgraded their systems. As existing AFIS platforms can be extended quite easily with facial modality, a lot can be learned from the several challenges we have encountered when designing a fully contactless, automatized, and flexible solution that smoothly works with existing access control systems.

Accuracy

For a truly seamless functioning access control based on face recognition, accuracy is paramount. Low accuracy corresponds to more manual interactions and overrides and more attempts to gain access even by authorized people. Given all the hassle, seamlessness can't be achieved. High accuracy, however, means better security, as gaining access without authorization is unlikely.

The US-based independent institution, the National Institute of Standards and Technology (NIST), regularly conducts tests to benchmark accuracy. Face recognition vendors from all over the world submit their algorithms to establish their competency in the Face Recognition Vendor Test (FRVT), wherein 150 algorithms were tested in the last one.

To further improve the quality of detection, a number of improvements can be made. Innovatrics, for example, offers the ability to automatically add a new picture to an employee database such as instances when the individual gets a haircut or wears a mask.

Speed

Speed goes hand in hand with accuracy. For access control purposes, face identification has to be performed almost instantly. In high-volume periods such as morning peak hour, it makes a huge difference if your system supports this feature. Low speed would create bottlenecks, leading to inconvenience.
Like accuracy, speed is easily gauged by NIST FRVT results. Depending on the use case, it is useful to see how fast the algorithm is in different scenarios and database sizes. When scaling your access control system, it's important to know if your algorithm maintains its speed as the database increases - something Innovatrics has long been known for.

Access Logic

A fast and accurate algorithm is a sound foundation for a good seamless access control system. To be functional, it has to provide a clear set of rules to prevent mishaps. They have to be extensive to account for most case scenarios.

These scenarios include everyday occurrences such as entering and turning around (e.g. to greet a colleague), which could trigger an access control camera. The system should be able to follow recognized faces in a stream and correctly predict whether they are approaching an access point. Moreover, it should be able to quickly separate authorized persons from the unauthorized to prevent tailgating and the like.

The aim is to have a system that is as automated as possible. Manual override should rarely happen; receptionists should mostly enroll visitors. Even this can be replaced with automized self check-in via the app.

Robustness

A seamless access control system should be able to handle peaks without any hitches. Processing high data throughput should not bring the system down to its knees, even when it has to process a large number of faces.
A good face recognition solution processes a raw video stream directly without recoding or pre-processing. It detects faces, attempts to recognize them, and sends appropriate commands to the rest of the system. Many systems currently work with still image-based recognition, which takes up processing time and slows it down to less than real-time processing.

The robustness lies not only in handling high data throughput, but also in adding more cameras without compromising performance. In some solutions, a system can be tied to a single camera or a preset array of cameras. Although having more increases computing power, such a setup can be costly. It is therefore advisable to rely on systems that are able to add cameras even without hardware upgrade.

Easy Integration

Most organizations, who want to add seamless access control based on face recognition, already have a number of interlocking systems in place – usually video management and data control systems with appropriate access control already tied in. As such, integrating the face recognition solution into the existing network should not be an issue. Needless to say, API and support of industry standards (such as Wiegand protocol) are a must.

Not all solutions work in cohesion with the existing system, requiring extra wiring, redundant data input, and synchronization. In these cases, personal data has to be entered twice (into the main system and face recognition system), adding extra complexity to the system and opening possible security holes.
As the complexity and number of interlocking systems increase, the ability to seamlessly integrate them becomes all the more necessary.

Flexibility

Apart from being robust for scaling purposes, the system must also be flexible enough to accommodate necessary changes to access the control setup. Ideally, it should work with most cameras that are connected, operating in different viewpoint and lighting positions. Technically, this means that the user should have control over a number of settings, including detection thresholds and even different detection algorithms depending on the type of deployment and required accuracy. These should be easy to set and test (and reset) in a ready-to-use interface. Since biometrics can be confusing for a non-expert user, it's ideal if the settings are easy to understand.

Enrollment should be flexible, wherein the system is capable of accepting input from a concierge desk (e.g. via tablet), and also from a user-held smartphone. In both cases, it must be able to take high quality pictures to enter into a watchlist.

Organisation:	*Innovatrics, s.r.o.*
Name:	*Robert Izak*
Email:	*info@innovatrics.com*

12. Jenetric: Hygiene and fingerprint scanners

This paper focuses on background information, technical and market aspects as well as recommendations with regards to hygiene and fingerprint scanners. Neither are other biometric modalities discussed nor are political motivations for implementing fingerprints as a proof of identity considered.

1. Background information

The vast majority of fingerprint scanners used today contain touch-based sensors. The fingerprint capture surface of those systems consists of metal (capacitive sensors), glass (prims or TFT-based sensors) or plastic (electroluminescent sensors) materials. The SARS-CoV-2 virus can survive on various surfaces between a few hours (copper) and a few days (plastic)[2]. However, these investigations were done under laboratory conditions only. No information is available yet on how the Coronavirus survives under real-world conditions at various temperature and humidity levels, on different surfaces, etc.

It is known that due to the morphology of the corona viruses that these microorganisms can be disinfected rather easily[3]. Using disinfectants with 62-70% alcohol and an exposure time of at least one minute will inactivate or kill corona viruses effectively.

2. Touch-based systems

As a matter of fact, capturing a fingerprint by using a touch-based system requires touching the capture surface which might be a risk to transmit viruses from one user to another. Besides the obvious measure to reduce the risk by applying disinfectants, there are other technical means possible. Studies have shown that the SARS corona viruses could be effectively inactivated by heating the surface to 56°C[4]. Also, the irradiation with UV for a short period of time will reduce the viral infectivity to an undetectable level. These technical means have not been applied to fingerprint scanners today but can be developed rather easily. However, applying these methods will require a modification to the standard operation procedures in the field.

3. Touchless systems

There is no doubt that due to the nature of the scanning principle, touchless systems reduce the risk of transmitting microorganisms from one user to the other significantly. Whereas some single finger systems have been on the market for many years, systems for capturing multiple fingers in one step have been introduced only recently.

3.1 Speed performance

Technically touchless systems provide a short fingerprint acquisition time[5], particularly multiple finger systems. However, the overall time that it takes to capture fingerprints needs to consider the usage of those systems as well. Finding the correct position, holding the fingers at the correct angle, holding all four fingers parallel and within the field of depth is not necessarily easier than touch-based systems. In fact, for some systems it is even more complicated and requires training. In addition, due to the fast capture time, there is no possibility to dynamically correct the fingerprint position during the capture process. That means that only after the fingerprint image has been captured, the result will become available. In the case of low image quality, the capture process must be started again.

In summary, although touchless systems have a high image capture speed, a well thought out user guidance that indicates where, how, when, for how long and at which speed the fingers are applied to the scanners is key for a successful fingerprint acquisition.

3.2 Image quality

"Images produced by a contactless device are fundamentally different from conventional scanned ink and livescan fingerprints. They differ in both distortion characteristics and image sensor characteristics."[6]. The major difficulties

[2] https://www.nejm.org/doi/full/10.1056/NEJMc2004973?query=featured_home
[3] https://www.journalofhospitalinfection.com/article/S0195-6701(20)30046-3/pdf
[4] https://www.ncbi.nlm.nih.gov/pubmed/14631830
[5] https://www.iarpa.gov/challenges/n2n/n2n.html
[6] https://www.nist.gov/programs-projects/contactless-fingerprint-capture

for acquisition of fingerprint images acquired by touchless systems compared to those captured by touch-based systems or by ink are finger distortion, low signal-to-noise ratio, and the risk of motion blur during the capture process. A prerequisite for comparing touchless fingerprints with traditional fingerprints is to generate a true 3D-relief that needs to be converted into graylevels.

LIVETOUCH
Flipcase
The most easy way to scan fingerprints mobile – anytime, anywhere.
www.jenetric.com
T: +49 3641 3129950 - M: sales@jenetric.com

For the development of the image fidelity of contactless fingerprint scanners including testing methods and metrics and artifacts, NIST started the research program CRADA[7]. As of today, there is no certification procedure and standard available that allows the use of touchless fingerprint systems for one-to-many comparisons, i.e. a standard that matches the requirements of FBI EBTS Appendix F. Two of the commercially available touchless systems are certified for one-to-one comparison (FBI EBTS PIV certification) with explicit information, that these systems shall not be used with the US CJIS system[8].

4. Commercial aspects

Although a lot of research and development effort for touchless technology has been invested over the last 10 years, only a few touchless systems have become commercially available. The main reasons for this lack of commercial success are:

a) The high costs of R&D (and the resulting products) compared to the most important criteria in government RFPs: price. As long as price is the determining factor for government applications (which requires the highest image quality standards) the return on investment can’t be justified.

b) The missing international image quality standard. Developing fingerprint systems without knowing the required performance and testing methods causes risky investments in research and product developments to be made.

5. Recommendations

For systems in the field:

- Use those fingerprint scanners that can be cleaned with easy to purchase and non-vendor-specific disinfectants, e.g. alcohol wipes or cleaner.
- Provide these disinfectants for users after the fingerprint capture.
- Disinfect the scanner regularly according the vendors guidance.

For proving scientific data concerning the impact and risk of hygiene and fingerprint scanners:

- Initiate large-scale studies on the risk of transmission of bacteria and viruses with fingerprint scanners under real-world conditions.

For increasing the number of touchless systems:

- Strengthen the efforts for the development of an image quality standard for fingerprint images from touchless systems. Include institutes, universities, standards bodies and agencies from a global base and not just the US (e.g. RCMP, BKA, BSI, Interpol, STQC).
- Start international performance comparisons for touchless systems comparable to the Nail2Nail challenge from IARPA or the biometric rallies from DHS.

Organisation:	*JENETRIC GmbH*
Name:	*Roberto Wolfer*
Telephone:	*+49 3641 3219950*
Email:	*r.wolfer@jenetric.de*

[7] https://www.nist.gov/tpo/partnerships/cooperative-research-and-development-agreement-crada

[8] https://www.fbibiospecs.cjis.gov/Certifications

13. Peoplekey: Fear not thy biometric

Disclaimer: My role is as a CEO, not an expert in Viral medicine, thus I state that my works contained here cannot be relied on as expert opinion. I am informed as many of us are from sources readily available to all of us, internet mostly. I do apolgise if my statements here are not absolutely accurate, any lack of truth in my statements comes from a lack of knowledge rather than ill intent, forgive me if you will.

Introduction

As human beings, we really are a touch odd. We have a global pandemic, this becomes front line news so we all buy toilet paper. That creates more news and then a complete panic buying frenzy followed by no toilet paper anywhere. There were other items effected, not because they would normally run out but simply because of panic buying. Whilst the toilet paper fiasco is amusing on one level, it represents the truth of what people will do. What people believe is the truth is the truth to them. The truth to them is all that matters. So in order to examine contact or contless biometrics we really need to look at various aspects of the truth. The actual truth, the varying circumstances and indeed, the truth that people believe. All are different.

The actual truth

Coronavirus is NOT actually spread through the skin. Touch what you want, contact what you want, biometric or not biometric, coronavirus will not infect a person via skin contact. I quote the Queensland Government here.

Coronavirus IS spread via the mucus membranes or wet parts of your face (eyes, nose, mouth and inhaling). The important actions needed for the Coronavirus issue are social distancing and sensible hygene, not so much what you touch. You have more danger from Coronavirus by being too close to an infected person for too long than by using a contact biometric that they used before you.

So why are we considering that there is an issue with contact biometrics? Yet, here we are.

What people believe

Biometrics has always had it's fears and controversy. People believe what they want to believe, biometrics or not. Contact Biometric devices being "unhygienic" was a concern long before coronavirus arrived, so why? Biometrics was also feared as "big brother", the collector of fingerprints and faces, and still today, privacy issues abound with facial images. So why is biometrics the bad guy here? A persons full image in any or every detail is free to be published anywhere with the person who's image has been captured being, unable to do anything about it. An Australian cricketer called Shane Warne will attest to that. Freedom of the press. No privacy for the person concerned, absolutely none. Where is freedom of biometrics? This is the human perspective.

Some people will buy lottery tickets and smoke cigarettes at the same time despite the chances of cancer being higher than winning. Fear leads to logical reasons why the "thing that is feared" should be avoided and the "thing that is loved" is OK.

So what drives the fear? Many things and we are all subject to it. Typically, that which we know, that which we do not know and that which we think.

What provides a reverse force of this fear? It is education / reassurance or motivation. The biometrics industry has been educating people since inception. The Biometrics Institute's primary directive.
Motivation comes from the desire of the user.

- Put a biometric lock on a beer fridge. Everyone wants to use it, no privacy issues here.
- Controlling and reporting on who took what, that's a privacy issue.

So what should we do?

That which is not quite true and the resulting fear factor that people feal are certain extremely important. We should never ever ignore this. People will do incredible things based on what they believe absolutely, true or not. Biometrics is not the issue here, fear of a contact biometric is. The fear has been born of coronavirus with the distortion of the real risk being transported into the fear of a contact biometric as well.

My estimate is that if a true comparison between transmission rate of Coronavirus were made between contact and contactless biometrics, there would be very little difference. Couple that with the actual recovery vs sickness rates, it would probably show the risks to be far higher in many other places, activities and circumstances that we all are exposed to in our every day lives. Despite all of this, we in the industry must absolutely and deeply understand the fears that people have, justified or not.

It is my recommendation that the industry offers re-assurance to all users of biometrics that;

- Contact presents little greater risk than non contact.
- Good practice and social distancing is paramout.
- Contactless technology is available for those with advanced levels of concerns.

We realise that users of Peoplekey hardware have been seen kissing our products and for good reason. Peoplekey regards this as a possible health risk and will request users to cease and desist.

Organisation:	*Peoplekey*
Name:	*Frank Bruce*
Telephone:	*+61 410 690570*
Email:	*frank.bruce@peoplekey.com.au*

14. Phonexia: Identity verification struggles at a time of pandemic

The infamous and now notorious Covid-19 has put our society to the test on many levels, hitting the healthcare, hospitality, and travel industries the hardest. Thanks to the myriad of hygiene measures put in place to cope with this unprecedented pandemic situation, the question of safe, reliable, and efficient biometric authentication has been raised.

Just a few months ago, no one would have worried about using their fingerprint to verify their identity on their smartphone. No one would have thought twice about unlocking their smart device with their face. However, a pandemic knows how to turn our lives upside down.

Putting a mask on your face and wearing gloves to limit the further spread of the coronavirus may be unpleasant for many of us, but it is absolutely circuit-breaking for a biometric verification technology that relies on a fingerprint or facial recognition.

Given the fact that people in distress prefer to call rather than type in, remote communication with the clients of banks and other institutions has become a true challenge due to a significant increase in the number of incoming calls. On the one hand, a client's identity needs to be verified quickly over the phone so that other clients who are already waiting in a queue can be served as quickly as possible, while on the other hand, the use of fingerprint verification via a client's smartphone needs to be reduced to a minimum to limit the potential spread of the virus further.

And for obvious reasons, depending on the location of a person (whether they are at home without a facemask or somewhere in public with one on), facial recognition is not always a viable option either.

When all the limitations and health-propagating enforcements are taken into account, all that is left to a person to verify their identity conveniently and reliably is either using the uniqueness of their voice or iris. These are the only touchless biometric technologies that are currently broadly available for public use.

However, iris scanners have not yet been widely adopted among the public, and frankly, it is neither time-efficient nor user-friendly to ask a caller to first scan their iris with a smartphone to prove their identity

Therefore, the only widely applicable biometric verification that can be used instantly and within the framework of reducing the spread of the virus is the one based on a person's voice.

Not only is it a natural part of every spoken communication, but it is almost always available to verify a person's identity. Combined with the other biometric aspects of voice, such as the estimation of a person's age group or the identification of their gender, the voice can be used to provide a huge variety of biometric information about a speaker

Whether pleasant or not, the current Covid-19 pandemic has uncovered the previously barely considered weak links of biometric verifications that depend heavily on fingerprint and facial biometrics recognition. Of course, each biometrics technology has its own unique place in our society, and most of the time works perfectly as intended.

It is however essential to be aware of their strengths and weaknesses, so that when the next unprecedented event occurs in the future, we will all be ready to interact freely, safely, and quickly thanks to our verified identities, in order to put the world back into balance.

Organisation:	*Phonexia*
Name:	*Marketa Lorinczy*
Email:	*marketa.lorinczy@phonexia.com*

15. Regula Baltija: Forthcoming trends: Touch versus touchless technology

Over the recent months of uncertainty the world had to reestablish itself by moving most of its operational processes online. The world has changed and consequently our reliance on innovative technologies has increased. This is a massive trend as we've seen many organisations around the world now obliged to move from desktop to mobile solutions in order to minimise human contact to help reduce the spread of COVID-19.

This has resulted in the demand for all sorts of digital technology, including online ID verification solutions. The increased use of online tools has led to a rise in fraudulent activities (e.g. account scams, phishing, identity theft, mortgage and credit card fraud). For customers and businesses alike the need to stay constantly vigilant is high as identity theft could potentially be the first step to launching online fraud attacks. Therefore, the implementation of touchless online ID verification solutions should be at the top of all businesses' wish-list.

It is now more important than ever that online ID verification solutions, such as Regula Document Reader SDK for mobile and web applications are expanding the capabilities of document authenticity verification. What seemed impossible just a few years ago has become a reality thanks to such mobile solutions. They are as quick and secure as traditional hardware devices whilst minimising the human contact in today's global health crisis.

A good example of how online ID verification may help during the pandemic crisis is evidenced in the very recent Regula collaboration with the Spanish social startup KUVU and the development team SQUAREETLABS. Spanish developers have integrated Regula Mobile SDK into their free app COVIDA, designed to help the elderly in need of food, medicine and other necessary products. Regula Mobile SDK provides online authenticity verification of the volunteer's ID at the first stage of the registration process. By verifying the volunteer's ID, the service guarantees safety and security of its users.

The demand for digitisation has been growing steadily over the past few years, but now due to the global health crisis, the growth has expedited. Just before the COVID-19 outbreak in Europe and the US, the intergovernmental organisation Financial Action Task Force (FATF) had published a guideline report on digital ID, where they

DOCUMENT READING AND VERIFICATION IN YOUR APP

Regula forensic science systems

- Extract data from identity documents
- Fill in digital forms automatically
- Verify authenticity in real-time

Regula Document Reader SDK for Mobile & Web apps: requires no extra human contact, implementing full **#socialdistancing**.

mobile.regulaforensics.com

estimated that 60% of the world’s GDP would be digitised by 2022. It is now obvious that COVID-19 has made an indelible impact on the digital world. The onboarding process is to be streamlined as businesses look to proceed with contactless technology as the new norm, even after COVID-19 to ensure passenger safety.

Etihad has recently developed sensors in their self-service touch points to create touchless technology at airports with the ability to evaluate the temperature of the travellers at a distance. The touch points also include a camera that reads document data without the need for placing it down on the device. This technology further minimises the potential risk of any viral or bacterial transmission by avoiding manual processes in order to put the staff out of the harm’s way. Although this crisis will boost the shift towards digitisation in the short-term, the overall approach to technology will not immediately change straightaway. Therefore, current methods will remain despite the interest in touchless technologies. Traditional desktop document verification devices will still be the mainstay as in many industries there is a particular need for tangible desktop technology, such as in the hospitality and medical sector (at the reception desks), border control, immigration services, law enforcement, as well as in embassies and consulates. These spheres are expected to make a shift towards digitisation, or at least investigate its probable benefits. We will see this happening steadily without fully abandoning touch hardware solutions.

The aviation industry has been particularly impacted by the global effects of COVID-19 health crisis and has been repositioning itself on how it operates to answer the health concerns of the public. According to Future Travel Experience: “even once the demand for travel is fully restored, the end-to-end experience may have forever changed, and it is likely that social distancing will become a longer-term feature in our lives”. Therefore, businesses will have to adhere and adapt to new trends as well as forthcoming changes.

There is a growing demand now for airports to move away from touch points to touchless solutions by adopting and extending automated ‘hands free’ technologies. Those technologies will enable touchless use of self-service devices through voice recognition and biometrics, answering passenger health safety concerns and reducing unnecessary queues. It does however, have its drawbacks which somehow must be addressed. One of them is e-passport verification by reading the RFID chip. The other is dealing with civil liberties associated with biometric data collection and use of cameras. All this combined must be balanced with the passenger experience. This is the challenge that we face today.

Organisation:	*Regula Baltija Ltd.*
Name:	*Anastasiya Lvovskaya*
Telephone:	*+375 17 224 66 44*
Email:	*anastasiya.lvovskaya@regula.by*

16. TECH5: The potential of touchless biometric technologies and solutions for COVID-19 management and the post-pandemic era

The global impact of the dangerous new coronavirus, COVID-19, has led to the rapid development of new technologies and solutions that allow for the collection of data to monitor the spread of the virus. Several health and government authorities have already begun implementing biometric-based Quarantine Management Systems.

Although national lockdowns were the first necessary measure to control the spread of the virus, the consensus is that such extreme measures are not sustainable in the long run without the risk of pushing the world into the largest global economic crisis since World War II. What is clear, however, is that in addition to tending to those individuals infected with COVID-19, and hospitalizing those who are seriously ill, any plan to ramp up the economy and reduce losses must necessarily incorporate solutions to bring people back to the workforce in a safe and controlled manner. This means that it has also become essential to identify those citizens who have already been infected with the virus as well as the many individuals who carry the virus asymptomatically.

The approach of mass testing for COVID-19 antibodies, which in countries like South Korea has proven effective in combating the virus, not only documents a regional level of “herd immunity” to COVID-19, but can also provide an opportunity for the collection of individual citizen data. The use of such data in combination with the latest technologies can become an effective tool for countries to bring citizens who can no longer become infected with the COVID-19 virus, or infect others, to a normal life.

One of the most promising concepts in this context is the introduction of an “Immunity Passport” or “Immunity Certificate”. Many countries are defining this concept in a similar fashion. Namely, the data of citizens with a positive antibody test result are enrolled into a specific government database managed by the Ministry of Health or other qualified Government institution. Each individual registered in the database is then issued an "Immunity Passport". Holders of such “passports” will be allowed to end full self-isolation, get back to work, move freely around the country and return to their usual lifestyle.

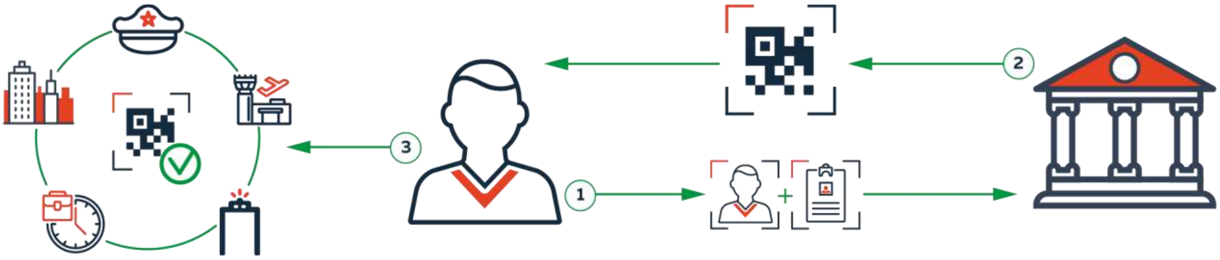
In order to implement such a strategy, it is imperative to keep in mind some essential ethical requirements, for example along the lines of those defined by the highly respected Edmond J. Safra Center for Ethics[9]. First, given that we live in a digital world, the "passport" should be electronic. This will allow for the document to be issued to a citizen by sending it to his/her e-mail and/or mobile device. Second, the data in the “passport” must be secured. Specifically, all stored information must be encrypted such that the data is kept private and accessible only to those authorized to verify the document. Most importantly, the power to authorize access to the data must rest solely in the hands of the owner of the data. In addition to a citizen’s test result and basic biographical data, the "Immunity Passport" should also store a unique identifier. This unique identifier could be a photo of the holder’s face; however for even greater security, access could be protected by one or more biometrics such as face, fingerprint or voice. Given that adequate Internet connectivity is not always available, authentication should also be possible completely offline. Third, the solution should be flexible and allow for easy update of stored data. Finally, the solution should be affordable for rapid implementation in every country, software-only, cost-effective and easy to integrate.

One solution could be an “Immunity Passport” that combines touchless biometric capture technologies with the use of high-density barcode storage, and meets the requirements described above. The steps for creating an “Immunity Passport” for a citizen could be as follows:

1. A citizen gets tested for antibodies at an authorized entity and receives the results.
2. The citizen submits the test results along with biographical information and a face photograph to an authorized entity to apply for an “Immunity passport”.
3. Biometric technologies allow the capture of biometric data without any purpose-built device or having to visit a registration office.

[9] The Edmond J. Safra Center for Ethics, COVID-19 Rapid Response Impact Initiative, White Paper 8: “Immunity Certificates: If We Must Have Them, We Must Do It Right”.

4. The authorized entity generates a high definition barcode that stores all gathered data encrypted with PKI to authenticate the barcode and make sure that only the authorized holder can unlock the data. This becomes the "Immunity passport" that is issued to the citizen and is protected by the citizen's biometrics.
5. The citizen can carry this "Immunity passport" on a mobile device or print it. Only the citizen can provide access to the "Immunity passport" to the person or entity of choice.



We believe that the post-pandemic era will become increasingly more digital. After weeks and months of quarantine in which day-to-day life was managed fully online, it is very likely that people will have changed their habits. As a result, more than ever there will be an increased need for a secure online environment as digital identity credentials incrementally replace physical documents. The eventual creation of "Digital immunity passports" governed exclusively by one's own biometrics could theoretically lead to the integration of other essential ID documents into it, ultimately leading to a single "Citizen's Digital ID", fully owned and managed by a citizen. In effect, identity will be moved from being housed in the external world to being retained in the safety of your own personal identifier.

Organisation:	*TECH5*
Name:	*Machiel van der Harst*
Telephone number:	*+41 79 615 46 37*
Email:	*machiel.vdharst@tech5-sa.com*

17. Trust Stamp: COVID-19 the fight for health, privacy and security

In response to the current pandemic crisis, we have seen a surge in biometrics-enabled solutions. These range from touchless biometrics and remote authentication to location tracking and contact tracing. Individuals need not only to prove who they are, but also now where they have been, and with whom they might have been in contact. While biometrics is unique in that it can irrefutably authenticate and identify the identity of an individual, their privacy should not be compromised; they should remain in control of their own personal data (including biometrics); and, only a minimal amount of their information needs to be revealed. The above needs involve not only individual-to-individual interactions (e.g., contact tracing), but also scenarios such as individual-to-organisation interactions (remote access), as well between two organisations.

In this paper, we advocate a biometric-enabled open identity management system (IdM) that supports selective disclosure of information or zero-knowledge proof queries between two parties, which has the following characteristics:

- **Anonymized**: Biometric references are transformed by an irreversible function using anonymization algorithms into a Irreversibly Transformed Identity Token (IT^2). This approach, which is known as cancellable biometrics, satisfies security requirements such as irreversibility, unlinkability (diversity), and revocability, whilst maintaining the level of accuracy of the native biometric reference.
- **Open**: The system is vendor-neutral and hence biometric modality agnostic. It promotes interoperability of biometric technologies and enables any standalone (siloed) IdM to securely exchange identity information in compliance with the general data protection regulation (GDPR) and best practices (Kindt, 2013).
- **Biometric functionalities**: The system supports identity query operations such as one-to-one comparison (authentication) and one-to-many comparison (identification) which supports database deduplication and watchlist operations.
- **Privacy by design**: The system is designed to reveal only relevant information following, inter alia, the data minimization principle, including a zero-knowledge-proof scenario where the response of the system is binary (e.g., delivering an answer to the question: Based on an individual's travel history, should the person self isolate).

A working MVP prototype can be found in www.Safe14.com. This system can minimize quarantine times for travellers and the need for economically destructive blanket bans, freeing front-line individuals to be where they are most needed. This is achieved without storing any sensitive information and without intrusive hardware such as "ankle bracelets". The proposed solution can work with existing biometric technology through a biometric reference conversion process if required.

Here's how it works:

1) Some information about the user is captured, including biometrics such as touchless fingerprint scans and facial biometrics. This data is enriched by auxiliary information such as geolocation, and even password or token as knowledge-based and token-based authentication, respectively.
2) Trust Stamp's artificial intelligence technology, including deep learning, converts this identifying data into an IT^2 token.
3) Upon successful matching with a genuine, live sample, an IT^2 has the ability to answer questions without revealing any additional information about the individual. This zero-knowledge-proofing property ensures that the individual is protected against personal data leaks, identity theft, and fraud.

Technically, an IT^2 is a cancellable biometric representation that is a result of blending biometrics and/or other identifiable information along with some random noise, the amount of which is controlled by the length of a nonbiodata key (including helper data). The irreversible property of the transform works in the same way as in lossy data compression whereby a lot less information is retained at the output compared to the input (see Fig. 1).

The one-way anonymization transform also satisfies two other security requirements, namely unlinkability (diversity) and revocability. Unlinkability means that two IT^2 tokens of the same individual in two unrelated applications appear to be very different from each other, e.g., an IT^2 stolen from one application cannot be re-introduced into another. Revocability means that an IT^2 can be revoked any time, e.g., upon the request of the individual, for any reasons, as required by GDPR and similar privacy regulations; or when the IT^2 is compromised or stolen.

An IT^2 is bidirectionally interoperable, meaning that any biometric reference of any biometric modality can be transformed into an IT^2; and any IT^2 can be processed by any third party-supplied SDK matcher. However, matching using Trust Stamp's 1:N identification SDK will be more computationally efficient in terms of speed and scale thanks to efficient implementation. Finally, using multiple IT^2 representations can improve the recognition accuracy over that achievable by its single-template native biometric representation counterpart (see Figure 2).

In a more advanced version of the system, using Trust Stamp's state-of-the-art key-binding sketch-based biometric template protection scheme, a cryptographic key is inserted into an IT^2 to generate a public token (also known as a Pseudonymous Identifier according to ISO/IEC 24745:2011), which is performed by an encoder during enrolment. Only a genuine, live IT^2 of the same individual can be used to unlock this public token using a decoder so that a private token is released and be consumed by a standard cryptographic framework which is linked to an Identity Management system.

Trust Stamp's anonymization-based biometric template protection scheme addresses a number of privacy concerns. First, a valid consent is given by the individual when they voluntarily provide their biometric scans, especially in the instance where touchless fingerprint technologies are being used. Second, since the IT^2 significantly reduces privacy and security risks incurred by either the data controller or processor. An IT^2 is, by definition, purpose-specific and furthermore, can be rendered time-limited. Moreover, in applications where an individual can carry a physical token, they have full control over how their data can be used. Thanks to the transformed nature of IT^2, two or more parties can now exchange information about tokens in a semi-trust manner, which is not possible without the one-way anonymization transform. The parties can set policies to strictly define the nature of exchange from a privacy perspective. In short, Trust Stamp's irreversible identity token solutions and similar biometric template protection schemes provide the tools and policies to support privacy by design, or privacy enhancing technology (PET).

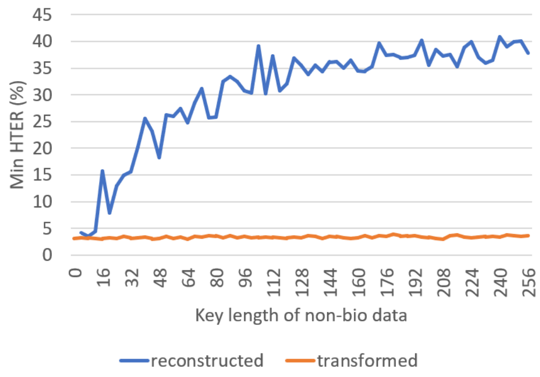


Fig 1. A study of the effect of the length of nonbiodata (X-axis) on the reconstruction property of IT^2 token in terms of Half Total Error Rate (HTER). As the length of nonbiodata key increases, the reconstructed samples match poorly to the original native biometric reference, as indicated by the blue HTER curve (Y-axis) whereas the probe IT^2 samples remain similar to the enrolled EgHash references, as indicated by the orange HTER curve.

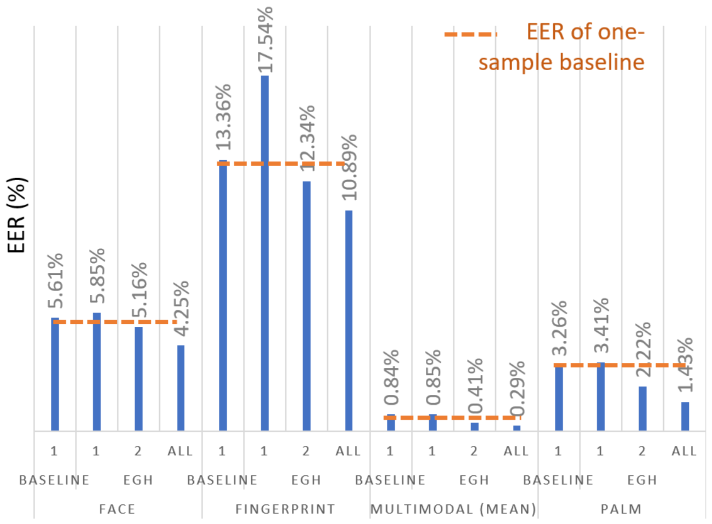


Fig 2. Comparison of the baseline one-sample native template solution and the systems from one to three IT^2 tokens (transformed biometric references) in terms of Equal Error Rate (EER), across face, fingerprint and palmprint modalities as well as their score-level fusion multimodal biometric system.

References

Kindt, E. (2013). Best practices for privacy and data protection for the processing of biometric data. In *Security and Privacy in Biometrics* (pp. 339–367). Springer.

Organisation:	*Trust Stamp*
Name:	*Norman Poh and Emma Lindley*
Telephone:	*+44 77321 84832*
Email:	*nnaik@truststamp.ai*

18. Unisys: Working from home in the age of COVID-19: Why VPNs are no longer sufficient

The work from home (WFH) movement being enforced on and with companies around the globe is helping to stop the spread of COVID-19. It also opens up critical new risks to our economy that go above the current pandemic. We have to evolve from simply implementing WFH and instead ensure that employees are secure from home (SFH). Many organizations use VPNs to establish a secure connection. However, VPNs have proven to have insufficient capacity to handle the large numbers of people WFH. And that inadvertently leads to a weakening of the security of the home workplaces, which cyber criminals are eager to take advantage of. The number of attacks on VPNs has recently increased by no less than 400 percent. The Zero Trust model and biometric solutions can offer a helping hand in preventing and limiting further cyberattacks.

Using flawed VPNs leads to enormous risks

VPNs were the right solution when all secure systems were hosted in a company's own data centers, rather than being scattered in clouds and containers. Many VPNs cannot handle the suddenly increased demand. Certainly for organizations that often work in the cloud and are part of a vital infrastructure, this entails serious consequences. Companies are forced to purchase additional hardware or software licenses. In addition, the use of free or cheap VPNs, with the chance that data will be sold, is now common. Because people think they are protected, cyber criminals are given the opportunity to do damage under the radar. In the worst case, VPN problems even result in managers deciding to grant employees unsecured access. Let us not think of the risks this would bring about.

A safe remote workplace with the Zero Trust model

The number of remote workers at Unisys has also exploded. Within the first week that the COVID-related mandates were in effect, the percentage of remote workers rose from 15 to more than 90 percent. We made this change completely transparent and safe to our global workforce with the help of the Zero Trust model. This model supports the efficiency enabled by containers, clouds and Kubernetes; understands the external and internal threats we all face today; and enables the secure scalability that today's operations demand.
The Zero Trust model works according to the "never trust, always verify" principle. This means that nothing is trusted inside or outside the perimeter, so that the degree of security stays the same. The fact that something is inside the perimeter does not mean that something is safe. Just think of phishing attacks. Only when complete authentication - on both the user and the device - has taken place is something considered reliable. The most fundamental difference with VPNs is that the Zero Trust Model does not authenticate based on a user's network segment, but based on the user's location, devices, behaviour and context. The technology thus effectively becomes the control plane, which enforces encrypted data traffic between endpoints.

Biometrics to grant remote access

Next to the Zero Trust model, you can add an extra layer of security by integrating biometrics. Instead of submitting a password or code, employees are asked to verify with e.g. their fingerprint. In that way, you can be 100 percent sure that the person who says is logging in to your company's system, is truly the person they seem to be. Also, the need for extra hardware tokens to facilitate WFH can become more flexible by adding biometrics, as employees carry these tokens themselves.

A good time to switch

VPNs, like the firewalls that preceded them, have had their best time. Due to the explosive increase in digital home workplaces, companies have to reconsider their security. The use of modern security that meets today's requirements is of the utmost importance. It is therefore high time to double, or perhaps even triple, the number of employees who can WFH safely and productively. Switching to the Zero Trust Model and adding a layer of biometrical checks is currently the most sensible choice. This allows you to quickly guarantee a safe home workplace for all your employees. There is too much at stake to follow through.

Organisation:	*Unisys*
Name:	*Frank Voogel*
Telephone:	*+31610001060*
Email:	*frank.voogel@unisys.com*

19. Vision-Box: Biometric touchless technology can help prevent the transmission of pathogens at airports

The global growth of aviation travel is steadily increasing the risk and facilitation of a faster worldwide spread of pathogens through person-to-person and surface-to-person contact at airports. The hard and smooth surfaces of clearance touchpoints used by travelers is an efficient source of pathogen transmission since these surfaces transmit microbes much more effectively than soft surfaces. Reducing this method of communicable disease transmission represents an important challenge for airports and airlines. Current global travel patterns and increasing passenger capacity demand that the aviation industry play an important role in reducing the transmission of communicable diseases.

SEAMLESS IDENTITY MANAGEMENT: A NEW PATH FOR HYGIENIC TRANSACTIONS

The presence and transmission of communicable pathogens represent a very real risk to passengers, airport personnel and operations because of interaction with infected touchpoints, travel documents or other travelers. Identity Management Platforms offers airports hygienic advantages that mitigate the risk of pathogen transmission by leveraging touchless biometrics and contactless passage through security, border control and boarding. This is accomplished by enrolling travel documents and facial images at airport check-in or remotely using digital mobile ID apps. Subsequent airport touchpoints then automatically recognize and authenticate the traveler’s face and identity in a few seconds, thereby eliminating the need to physically interact with potentially infected surfaces or exchange documents with an agent or officer.

This is especially important at hotspots throughout the passenger journey that present a higher risk of transmission including check-in, security checkpoint, border control and boarding. Hotspots are instances where passengers are required to physically interact with touchpoints or exchange documents with airport personnel where pathogens may be present. These points are usually characterized by bottlenecks and long waiting lines, with crowd density and duration being a key factor in transmission risk. Seamless digital identity mitigates these risks by speeding up the clearance process and reducing both factors, especially important during peak hours. Touchless technology minimizes contact between passenger and airport personnel, potential exposure to pathogens and the possibility of further contamination inside and outside the airport complex.

TOUCHLESS IDENTIFICATION: THE NEW NORMAL

By design and function, touchless identification systems prevent the introduction, transmission and spread of communicable diseases. They eliminate the need to touch potentially infected clearance points or to exchange travel documents. Seamless Identity Management use advanced contactless biometrics to optimize and speed-up passenger clearance that can increase personal space between passengers. It establishes identical contactless clearance procedures throughout the passenger journey that eliminate time-consuming identification tasks and establishes faster clearance for both inbound and outbound passengers. This means travelers can leave the airport quicker, reduce the number of passengers inside the premises and decrease potential pathogen exposure.

PROACTIVE RISK MANAGEMENT

Pathogen risk management includes assessing current disinfecting protocol, procedures and ease of equipment cleaning. By installing Seamless Digital Identity Systems designed with smooth modular lines, both routine cleaning and targeted decontamination procedures vastly improve the elimination of pathogens present on passenger touchpoints. Moreover, systems designed with fluid lines speed up and improve the decontamination procedure involving the use of hazardous decontaminants for high-consequence pathogens. Additionally, the lack of hidden nooks and crannies minimize the pooling of cleaning liquids that can affect the performance of critical components and structural integrity.

The consideration of pathogen risk management goes hand-in-hand with other operational and commercial benefits seamless technology and legacy process remodeling can bring together as currently aggregated in the IATA-driven One ID initiative. How to effectively address the human-factor challenge and its unpredictability aspect as critical variables must be considered at the inception of every project design and solution delivery. This is a critical concern when designing both hardware and software platforms whose goal is to deliver sustainable automation of complex processes independently of human singular characteristics. Using biometrics as a foundational element enables the realization of all the value friction-less processes bring by unleashing the power of human-centered technology.

THE INDUSTRY SEAMLESS CONTRIBUTION

During this occasion when modern society is challenged by an unprecedented global pandemic, we are proud of being part of industry-leading companies that deliver tangible benefits back to all global citizens, and in the process, make the world a better and safer place. Biometric touchless technology is clearly one of the main pillars of a strong proactive and preventative approach to limiting the spread of pathogens. By limiting physical contact between humans and interactions with machines in times of an outbreak, Seamless Identification technology delivers a solution that can contain the spread of viruses. As touchless processes become more widely available to travelers, it will provide a steady model of business continuity for airports during times of prosperity and in challenging conditions that require physical distancing. As with all digital identity solutions, privacy and personal data protections are fundamental rights that must remain unchanged during circumstances where individual rights may be curtailed because of public emergencies. It actually becomes a complementary solution value-add when contactless identity allows the delivery of information security and facilitation at the same time, in a responsible and sustainable manner.

While every airport has planned for incidents such as mass casualties, natural disasters and manmade events, very few have put in place systems to mitigate the risk of communicable disease transmission. Airports can gauge and manage this risk present throughout the passenger journey by deploying Seamless Flow and Identity Management clearance systems. The installation of these systems can be done without adding to or conducting any substantial remodeling of the existing terminals. Since pathogens can have a sustained impact on airport operations, it directly and indirectly affects the benefits they deliver to local communities, nations at large and the world in general. Large airports support thousands of aviation jobs, passenger spending at hotels, restaurants, rental car companies, entertainment venues, tourist attractions, and numerous other local businesses. This underscores the fact that continuity of operations at airports is an essential component of daily life as we currently experience it.

Organisation:	*Vision-Box*
Name:	*Jeff Lennon*
Telephone:	*+351 21 154 3900*
Email:	*Jean-Francois.Lennon@vision-box.com*

20. WorldReach: Border management after the pandemic: The urgent need for remote and touchless identity services

The COVID-19 pandemic has impacted almost every aspect of contemporary life. Immigration and border management are no exception. Border agencies are looking urgently to the biometrics industry for remote and touchless services.

At the time of writing, in April 2020, international flights are empty or cancelled, airports are deserted and queues in the immigration hall are just a memory. Those working outside immigration and border management might assume that national border agencies are not much affected by the pandemic; surely, they have nothing to do?

The reality is very different. Border agencies are aware of their role in the shop window of national economies: an efficient and secure process before, at and after the border is essential for both trade and tourism. Soon, health restrictions will begin to lift and international travel will show the first green shoots of recovery. That recovery will depend in part on the ability of border agencies to respond to the legitimate concerns of travellers.

High on the list of traveller concerns will be: am I required to wait in close proximity with other travellers, and am I required to use touch devices (such as kiosks, eGates and fingerprint readers) immediately after other travellers? This is where the biometrics industry must step up with new and innovative solutions.

At WorldReach, we have been working for several years on an IDV service (identity and document verification) designed for the specific needs of border agencies and other travel service providers. Our platform – Know Your Traveller™ – combines the power of smartphones to read a passport chip (via NFC) with the latest in facial recognition technology. This includes an instant facial match between selfie and passport, and a genuine presence test to prevent spoofing.

Any agency using this service can have confidence that a genuine document has been presented and that it has not been lost or stolen. They can also be sure that the traveller is a real, live person who is the rightful holder of the document. And all this can be achieved remotely, without the traveller needing to be seen in person or submit documents in the mail.

This IDV service is already in production at volume in the real world: it has been used since early 2019 by the UK Home Office as the first step in the innovative EU Settlement Scheme. An estimated 3.5 million EU nationals living in the UK are required to register with the Home Office for a new 'settled status', in order to continue living and working in the UK following Brexit.

The Home Office recently announced that, after only a year since launching the scheme, more than 3 million applicants had already applied successfully. And an overwhelming majority of those applying did so remotely, through the digital route that allows them to verify their identity with no in-person visit and no mailing of hard copy documents.

The large majority of those choosing the digital route completed it successfully, without assistance, in just a few minutes. This compares favourably with similar remote digital on-boarding processes in other sectors, including financial services, where there is often a high drop-out rate.

In Canada, the same approach is being explored by Canada Border Services Agency as part of an innovative concept called Chain of Trust, in which biographic and biometric data captured early in the travel continuum is combined with dynamic risk assessment to determine the appropriate channel for each passenger at the border. The ultimate aim is to achieve zero wait time at the border for eligible, low-risk travellers, via the use of biometric corridors.

Thanks to this experience, WorldReach has been presented with some urgent challenges in recent weeks, as border agencies begin to set strategies for pandemic recovery. These challenges include:

- How can a border process heavily dependent on touch-screen kiosks or eGates adapt to the post-pandemic world in which many travellers demand a touchless alternative?
- How can a visa application system based on in-person fingerprint capture in visa application centres respond to travellers' expectations for a fully digital, remote process?

A significant part of the answer to these questions lies in innovations based on the fully remote, digital IDV process described above. Instead of requiring newly arrived travellers to stand in a queue with others and use a touch-screen kiosk or eGate, why not allow them to enrol in advance of arrival, on their own smartphone, and grant access based on a touchless facial match at the border?

Instead of expecting visa applicants to travel to an application centre and wait with others to enrol their biometrics, why not allow them to submit the information remotely, at home, using a mobile device?

The technologies required to do this are already available. But it is not enough for biometric vendors to sell components to government agencies and then go on our way. That is a recipe for failure, when government can least afford it.

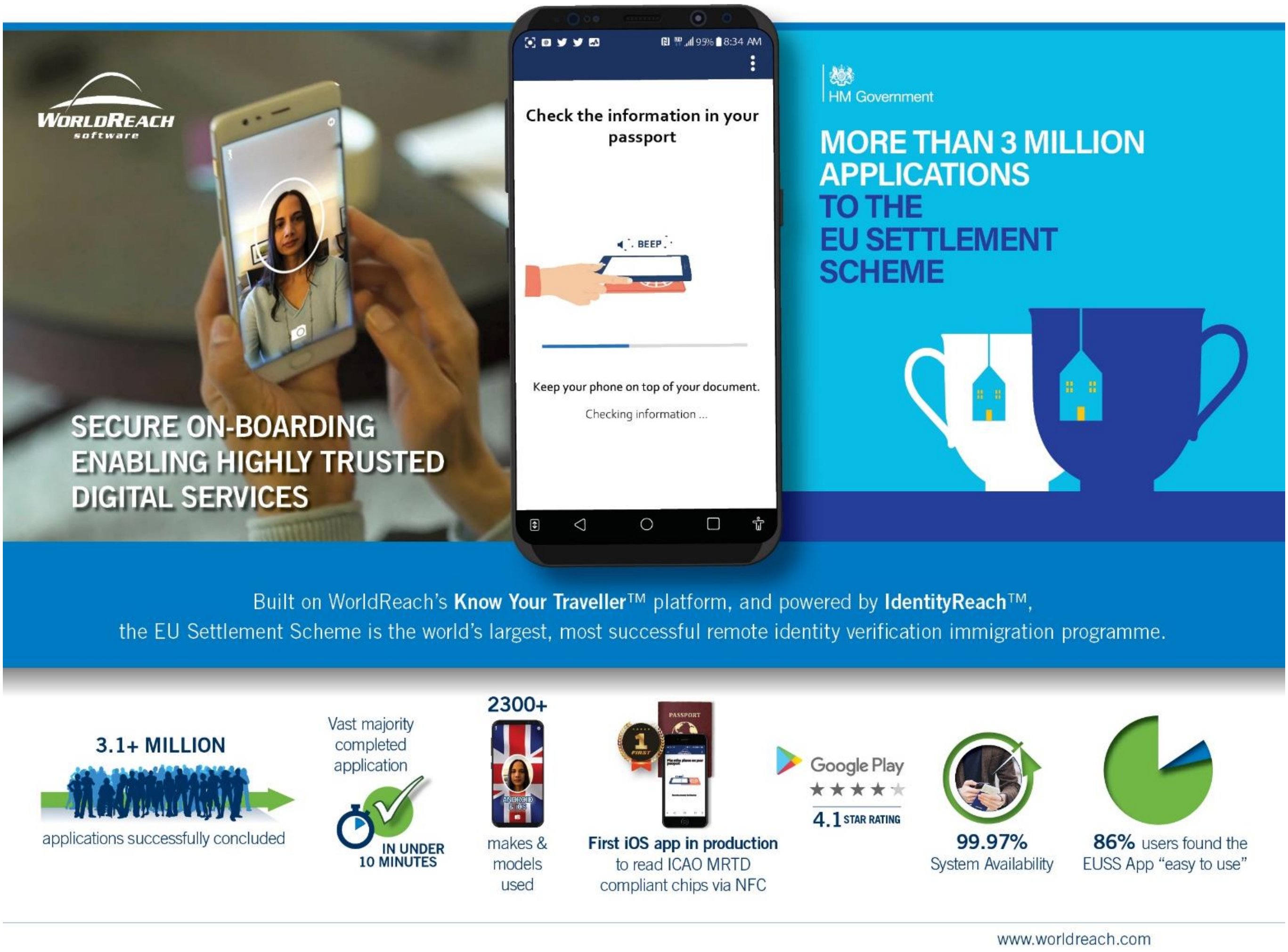
Our experience deploying these services successfully in real-world, mission-critical environments tells us that two other elements, besides good technology, are vital:

- We must understand the end business results that client agencies are seeking, not just in terms of compliance with security standards, etc., but also operational success, including the expected take-up rate of digital routes versus other options;
- In order to deliver that success, we must be prepared to work with client agencies not just on the technology required but also on the whole user process, to ensure that innovations can be understood and successfully navigated by the travelling public.

For many, this is a difficult time. It is also a time in which innovations that might have been explored in the medium term are required right now.

At WorldReach, we believe border management systems can contribute to pandemic recovery globally by adopting new processes that support the remote and touchless use of biometrics. We in the industry have an obligation to work collaboratively with agencies and partners to make that happen.

Organisation:	*WorldReach Software (US office)*
Name:	*Jon Payne*
Telephone:	*+1 703 883-7022*
Email:	*Jon.payne@worldreach.com*


WorldReach software
SECURE ON-BOARDING ENABLING HIGHLY TRUSTED DIGITAL SERVICES
Check the information in your passport
BEEP
Keep your phone on top of your document.
Checking information ...
HM Government
MORE THAN 3 MILLION APPLICATIONS TO THE EU SETTLEMENT SCHEME
3.1+ MILLION
applications successfully concluded
Vast majority completed application
IN UNDER 10 MINUTES
2300+
makes & models used
First iOS app in production to read ICAO MRTD compliant chips via NFC
Google Play
4.1 STAR RATING
99.97%
System Availability
86% users found the EUSS App "easy to use"
www.worldreach.com

Built on WorldReach's **Know Your Traveller**™ platform, and powered by **IdentityReach**™, the EU Settlement Scheme is the world's largest, most successful remote identity verification immigration programme.