Transforming the immigration system through smartphone biometric enrolment

Unlocking policy and technology issues

Powered by sopra steria

Executive Summary

Although smartphone enabled biometric capture technology is still emerging, we predict a near future where fully mobile biometric enrolment will be commonplace. Once sufficiently developed, it has the potential to dramatically improve the way the Home Office provides its services – making them more secure, faster and cheaper - and how customers and users interact with the department. To realise the opportunities, a holistic transformation approach is required, and industry must be provided with a framework within which they can develop the required technology.

Recommendations:

- Update and re-release the Home Office Biometrics (HOB) Programme Biometric Standards - 'Requirements and Information for Partners and their Suppliers' - catering for contactless devices and specifying the number of fingerprints required to be captured.
- Move away from the hardware-based Appendix F certification, towards a software and application-based standard that maintains appropriate levels of security.
- Industry to set-out the technical requirements for matching 3D representations 2D fingerprints databases, and Home Office policy to meet those requirements.
- Establish standards for contactless 'matching', comparable to contact devices and the algorithms in use with them.
- Explore the potential opportunities and risks associated with image processing software, including how digital ethics is considered.
- Adoption of a holistic approach to business transformation that leverages current and emerging smartphone technology

Secure biometrics at the core of the immigration system

The immigration system of the future must be very different to today if it is to respond to the increased security and safeguarding risks, complexity and volumes expected at the UK's borders.

Visa applications will be fully digital, border crossings will be frictionless, in country visa extensions and citizenship applications will be integrated and personalised, enforcement and targeting action will be driven by data, and travellers will be counted in and out of the country. Achieving this vision and realising the benefits of it requires a coherent and holistic approach encompassing operating model design, structured business transformation, a focus on value and integration of emerging technology.

One such technology is biometric capture. New biometric technologies are revolutionising the ease of use and accessibility of traditional biometrics solutions. It is driving more reliable identity verification in healthcare and criminal justice and supporting efficient immigration and cross-border travel. It is adding another layer to police and defence security processes. Also, it is helping to combat increasingly intelligent criminal activity in areas such as financial services.

We have already begun to see the potential benefits of this technology, in the shape of mobile facial recognition and liveness capture, which have been a feature of the UK immigration system for several years. However, while travellers are still required to attend in personto provide their fingerprints, there are limits to the degree to which the future immigration vision can be realised.

The development of smartphone enabled fingerprint enrolment technology presents an opportunity to radically redesign the immigration system and the customer experience, leading to:

- A more seamless border, as full biometric checks can be conducted quickly on any passenger at point of application before they get permission
- Cost reductions, as the UKVI footprint overseas can be radically redesigned to meet the vastly reduced need for in person biometric collection.
- Greater convenience and quality of service for travellers, who will no longer be required to attend inperson or send hard copy documents.

Over and above the direct benefits to UKVI and its customers, capturing all biometrics, on a smartphone, opens the door to creating a secure digital identity to use when applying to come to the UK, crossing the border and subsequently accessing public and private sector services. This digital identity can travel with an individual, on their mobile device, enhancing security, minimising fraud, reducing costs and providing more joined-up, efficient and effective government services.

Smartphone enabled fully biometric enrolment will increasingly become a core component of the immigration system. It will be used in the initial application, reused throughout a customer journey and be available for use beyond the Home Office by other government departments.

Sopra Steria has over 30 years' expertise in the field of biometric capture, storage and reuse – in the UK and overseas – and we know that to be successful our client's need to integrate technology developments into wider strategy and transformation plans. Organisations that want to utilise the technology must recognise the scale and significance of the opportunities and begin the complex business transformation journey now.

To be successful, organisations, with their partners, will need:

1. A coherent **business strategy**, underpinned by transformation plans that integrate the wider systems within which they operate.
2. A methodical approach to **value realisation** - for their organisation, the customer, and other private and public sector bodies – throughout their service offer.
3. To address **policy requirements** and the ethical implications of the approach.
4. To test and build **technology capability**, both in-house and via partnerships with industry leading suppliers.
5. A systematic approach to **systems integration**, managing the inherent complexity involved in the multidimensional transformation programme.

Key policy and technology issues for mobile fingerprint enrolment

Three issues at the forefront of the current debate surrounding mobile fingerprint enrolment are policy, standards and technology capability. Policy sets the standards technology will have to meet. As such, the two areas are closely interconnected and early work to resolve currently unanswered questions will smooth the journey to mobile biometric enrolment.

In crucial areas, policy has not yet been established to set out the requirements needed for contactless mobile fingerprint capture, as government wait for industry standards to guide policy, and technology is not yet sufficiently advanced to fulfil the potential requirements.

Policy standards/regulatory issues are unclear or have not yet caught up with the technology ask, leaving industry with no framework to benchmark against.

Camera technology needs to have the depth of field or illumination to sufficiently focus across multiple fingers and highlight/capture minutia accurately, issues of which, NIST (National Institute of Standards and Technology) testing has previously highlighted.

Image processing software and matching algorithms cannot yet make up for the shortfall in mobile camera technology and therefore, a higher degree of errors, compared with enrolment using a contact based technology.

What is Appendix F?
The FBI, EBTS and globally recognised standards

In selecting fingerprint scanners for use in high security applications, organisations globally refer to the FBI's image quality specifications. These are defined in the 'Electronic Biometric Transmission Specification' (EBTS).

An FBI certified scanner is verified to meet stringent interoperability standards, provide high quality images reliable for use in identification, and be fit for use with automated fingerprint identification systems.

EBTS is based upon the ANSI-NIST ITL-2011 requirements and defines two image quality standards:

- PIV-071006 (Personal Identity Verification), suitable for use in one-to-one matching use cases.
- Appendix F, which is the higher technical standard and is intended for use in large scale automated one-to-many and many-to-many operations.
- Appendix F image quality standards are assessed across a number of criteria, including geometric accuracy, spatial frequency response, signal to noise ratio, and grey level uniformity. Output resolution must be within the range of R+/-0.01R, where R is either 500 or 1000 pixels per inch (ppi).

For the capture of identification flats the FBI require that a 'simple capture protocol' be provided and that verifiable finger sequence data be provided. Both requirements essentially reference use of a minimum size of scanner capture area to enrol 4 fingers simultaneously i.e., 3.2" * 3.0".

There are no Appendix F certified smartphone solutions. What is more, the FBI does not have a category defined within EBTS for contactless devices. It's important to note that Appendix F is a hardware based standard and unsuitable for smartphone solutions. Unless EBTS/ Appendix F is updated appropriately, new requirements divorced from Appendix F need to be defined.

Policy standards

The current fingerprint capture requirements - set out in the Home Office 'Biometric Standards: Requirements and Information for Partners and their Suppliers document' - highlight some of the areas that need to be addressed. This document refers heavily to the Federal Bureau of Investigations own policy and specifies that:

- The Supplier must ensure that equipment supplied for recording fingerprints that are transmitted to Home Office Biometric (HOB) systems is certified according to Appendix F of CJIS Image Quality Specifications, as contained in the FBI Electronic Biometric Transmission Specification (EBTS) IAFIS-DOC-01078-9.3. The latest version of this document does not include a categorisation standard specific to contact-less devices.

- At the point of biometric enrolment, all digits present are in scope i.e. 4-4-2 'identification flat' fingerprints are captured. Also, that four fingers be captured on each hand simultaneously for identification 'slaps'. This is particularly challenging for a mobile device, which will be outlined later in this paper.

- Suppliers shall ensure that equipment supplied for recording fingerprints that are transmitted to HOB systems meet the HOB fingerprint standards detailed in Appendix A of the HOB biometric standards and exchange requirements document.

Those developing smartphone fingerprint capture, therefore, have no agreed set of requirements of acceptability. Indeed, as noted above, the FBI has no contactless category against which to assess smartphones, using camera technology solutions. This is a significant gap that leaves technology providers adrift in terms of acceptable standards.

Additionally, if Appendix F continues to be the hardware standard, those organisations wishing to make use of the technology need to ensure it will be supported and new handsets meet the acceptable policy standards. The rapid turnover of smartphone models (with leading handsets replaced annually), coupled with the breadth of handsets available in the market, would present problems in supportability of any service and would require manufacturers to sponsor their handsets through FBI certification as a default business process. This is not a viable approach.

Camera technology

Fingerprint scanners within smartphones are a common technology, used to secure the device. There are three technology types currently in use:

- **Optical sensors (In screen)** - Embedded under the display, the fingertip is presented and a photograph effectively taken by the sensor. An algorithm converts the image into a record of the print for authentication comparison.
- **Ultrasonic scanners (In screen)** - When the fingerprint is presented an ultrasonic pulse is transmitted against it and the ridges reflect it back to create a basic 3D image of the fingerprint. The technology is challenged in accuracy by having to pass through the phone backplane and the screen, but it is growing in popularity.
- **Capacitive sensors (Direct contact)** - Works by passing an electric pulse through the fingerprint to map its contours.

These sensors only capture and encode a small area of the fingerprint, much like a low FAP* level mobile scanner device. The resolutions are to a lower standard than required for enrolment and 'one to many' use cases.

Smartphone-based solutions that are being proposed for use in government and criminal justice applications are predicated on use of the device camera to photograph the required fingers using the built in LED for illumination of the fingers. This enables the capture of the necessary area (although some solutions require the users to tap the screen manually to trigger the capture, which can be a problem in Appendix F compliant capture, which needs both thumbs to be captured simultaneously).

Fingerprint capture image resolution must, according to the Home Office 'Biometric Standards – Requirements and Information for Partners and their Suppliers document', be a minimum of 500ppi, with potential for 1000ppi also being supported going forward. Smartphone camera technology will need the depth of field to focus on multiple finger points at once to sufficient detail.

*Fingerprint Acquisition Profile - EBTS defines six different FAP levels, with each being qualified by; the number of fingers to be captured; The associated capture area: The image quality specification.

Image processing software

Smartphone solutions suitable for visa applications all have photographic capture at their core but the small depth of field offered by smartphone cameras makes it difficult to maintain focus over four fingers simultaneously to capture an image of sufficient quality of all digits. The challenge for developing these algorithms means assumptions are required as to how to interpret image features as either ridges or furrows. The software has been unable to reliably recover the fingerprint ridge structure of the out of focus areas and such processing is still a major source of error.

Additionally, contactless technology has challenges relating to the different way the prints are captured and currently there are no accepted industry standards for 3D representations that are compatible with databases of 2D fingerprints. This impacts on the success of correctly matching contactless fingerprint captures against existing database entries.

Contactless also has challenges relating to spoofing (presenting fake fingerprints perhaps as a high-resolution image), with 'Presentation Attack Detection' capabilities less effective than for contact-based solutions, for example liveness checks.

How effective is the current technology?

The National Institute of Standards and Technology (NIST) has previously published an assessment of the relative performance of contact and contactless fingerprint capture devices. The results confirmed that contact devices remain superior to contactless. Within the contactless category they assessed both fixed specialist fingerprint scanners and smartphone-based solutions. Here, they found the former to be superior.

- Match accuracy for contact devices generally produce a match rate of 99.5%. For smartphone-based solutions the match rate was up to 70%, if matching a single digit. If matching against multiple digit combinations the performance was superior, reaching up to 95% for the leading device.

- Contactless devices did display a low rate of false positive rates, in line with contact devices.

- While true optical resolution on smartphone cameras may be capable of reaching 500ppi, if the capture resolution sample rate is greater than 500ppi, then it must be down sampled using filtering. This control of scale rate was found to be difficult for smartphone based contactless solutions, which demonstrated a broad distribution of results with ~50% of the distribution falling outside the lesser PIV range (+-10ppi).

NIST assessment of smartphone technology shows that such solutions do not meet the stringent standards specified for Appendix F and that the error rate is significantly higher than contact-based devices. However, performance improvements are being made with each passing year and each smartphone generation. With the right guidance, industry can make even faster progress.

Moving forward

Technology is developing fast and, based on expert opinion and market analysis, we estimate that capturing fingerprints for enrolment using a smartphone for visas may be available in 2-5 years. But the fact remains that there are currently no smartphones that are FBI Appendix F certified for use as a fingerprint scanner

To fix that problem and give technology providers the best chance of speedy rollout, interconnected policy and technology issues need to be addressed so that industry knows the benchmark it must meet. We recommend:

- The Home Office 'Biometrics Standards and Exchange Requirements' should be re-released catering for contactless devices and specifying the number of fingerprints required to be captured.
- Moving away from the hardware-based Appendix F certification, towards a software and application-based standard that maintains appropriate levels of security.
- Policy requirements for matching 3D representations 2D fingerprints databases are agreed.
- Minimum standards for contactless 'matching' are communicated to industry.
- Exploring the potential opportunities and risks associated with image processing software, including how digital ethics is considered.
- A holistic approach to business transformation that leverages current and emerging smartphone technology

Only through enablement of privately held smartphone solutions to biometric fingerprint enrolment can the visa application process be digitally transformed, removing, for the vast majority of prospective travellers, the need to attend fixed physical locations. With this technology in place, government can take a step forward in starting to unlock the value of an authenticated, fully secure and mobile digital identity that creates opportunities for benefits throughout other areas of the public and private sector.

To discuss these issues, contact Sopra Steria's experts

"Sopra Steria's biometric applications and expertise supported the department by drastically increasing efficiency through the automation of communication between end users with several AFIS solutions. This enables us to focus our expertise where it is needed."
Vidar Hovland, Police Superintendent Fingerprint section, NCIS – Norway

Did you know...

- Sopra Steria's global community of biometrics specialists has delivered solutions in 27 countries, including the UK, Switzerland, Netherlands, Germany, Norway, Belgium and France.
- A dedicated Biometrics Centre of Excellence in Oslo, Norway, has developed and delivered biometrics booking and identification solutions across Europe.
- Our new-generation biometrics capture and enrolment system processes ten-prints, quick checks, latents, palm prints and mugshots, as well as iris and signature scans.
- Sopra Steria has worked closely with police forces and immigration services for two decades to design the most efficient biometrics solutions.
- SteiaFit (Unify) offers police, border control and other homeland security teams high-speed searches for greater efficiency.
- We are the prime contractor for the Eurodac system which contains biometric data of asylum seekers as well as providing a gateway solution to member states (EURODAC NAP).
- We also manage Schengen Information System (SIS II) which alerts on people or objects in order to find them.
- In partnership with IDEMIA, Sopra Steria was selected by eu-LISA to develop the new Shared Biometric Match system (BMS shared or sBMS) that will, among other things, secure border controls in the Schengen area.
- We are experienced in implementing large AFIS for managing asylum seekers in Europe, as well as for the policing bodies Europol, Prum and national police forces in Norway, Denmark, Sweden, Switzerland and Belgium.
- Sopra Steria has also been chosen with our partners IDEMIA by the French Ministry of the Interior for the design, implementation, deployment, maintenance and evolution of the new central border control system (CCAF) which is part of the entry-exit system (EES). The aim is to improve the management of the external borders of the Schengen area - Biometric technologies at the heart of CCAF contribute to the reliability and speed of this new service.
- Our revolutionary software, integrated biometric algorithms and hardware is already deployed in service that that makes identity verification possible in military operations, and in operational theatres to safeguard military personnel and facilities, and to identify injured personnel.
- We partner with specialist technology product vendors, including Crossmatch for livescan technology and Cognitec, whose facial recognition technology is integrated with our proprietary solutions.

Innovation is nothing without impact

A great idea isn't an answer in itself. You need to deliver on that vision and turn it into a value-added reality for your department. For that, you need a consulting and IT services partner that has the passion, insight and pace to continually take you from ideation to impact. Ongoing innovation is only the beginning of what we can achieve together.

Sopra Steria does more to help you adapt in a changing world. We design, develop and deliver technology solutions that achieve your strategic outcomes and meet your specific challenges. By combining collaborative consultancy and strategic expertise with sector specialisms, digital best practice and accelerated delivery, we make a real difference to every client's challenges.

Contact us

Ben Brown
ben.brown@soprasteria.com

Gary Craven
gary.craven@soprasteria.com

Chris Gordon
chris.gordon@soprasteria.com

Brendan Swarbrick
brendan.swarbrick@soprasteria.com

Learn more about our capabilities at **soprasteria.co.uk**