SECURE IDENTITY ALLIANCE

Authentication...
Are you who you claim to be?

How Optical Machine Authentication (OMA) including Phone Authentication (OPA) can improve document authentication

2021

Mentions

Secure Identity Alliance (SIA)
www.secureidentityalliance.org

Design
Design Motive Ltd

Photo credits
CST, IDEMIA, Keesing, Shutterstock, Thales, WHO

Editorial review
Slingshot Communications

Production of this report

Lead Authors

Frank Smith Advisory Observer, SIA
(Former Deputy Director Home Office UK)

Thomas Poreaux IDEMIA

Contributors

IDEMIA
Aimane Ait El Madani
Patrick Guthmann

IN Groupe
Joachim Caillosse (Chair of the Document Security Working Group)
Amaury Chasseux
Françoise Daniel

Thales
Renaud Laffont-Leenhardt
Alejandro Leon Garcia
Roger Edwards

Veridos
Faten Ben Jemaa

Crime Science Technology
Cosimo Prete
Christophe Halope

OeSD (ÖSTERREICHISCHE STAATSDRUCKEREI)
Claudia Schwendimann

Our thanks also go out to INTERPOL's Counterfeit Currency and Security Documents (CCSD) Branch for their comprehensive review of the guide.

SECURE
IDENTITY
ALLIANCE

Contents


VISA

Executive summary

This paper

This 'white paper' considers the authentication challenge - why it is difficult and how to answer it. It looks at automation, in particular the new and emerging field of how optical analysis of identity documents can be automated, including using mobile smartphones. This and other approaches can answer the question 'Are you who you claim to be?'. Authentication of secure documents has traditionally been crucial in border control but is becoming more important in additional contexts – financial, online and increasingly for members of the public.

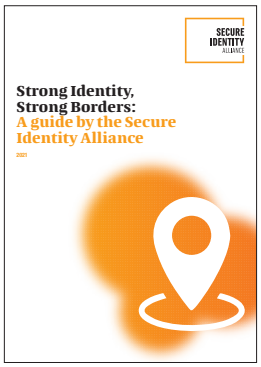
This guide considers:

- **The challenge of authenticating identity** – the majority of people showing a passport or other document to establish their identity may be genuine, but some may be trying to have a false identity accepted. This guide looks at how a document or identity might be attacked and considers how you can try to authenticate a document to prove or disprove an identity that someone is claiming?
  Page 4 »
- **Use cases** – describing how these techniques can be applied in practice.
  Page 22 »
- **Recommendations** – based on the analysis in this paper.
  Page 28 »
- **Glossary**
  Page 30 »
- **References**
  Page 31 »

The information presented in this guide has been collected and validated in collaboration with experts from various organizations across the world. Once again, we have worked with Interpol's Counterfeit Currency and Security Documents (CCSD) Branch.

This guide is part of a wider range of materials on different aspects of identity published by the Secure Identity Alliance (SIA). In particular, it forms a natural bridge between an SIA guide on secure documents (Passport Fraud and Ways to Combat Them) and borders (Secure Identity, Secure Borders). See:

https://secureidentityalliance.org/ressources/publications



1. The challenge of authenticating identity

Many people seeking to establish their identity are genuine and welcome secure documentation or other means of proving who they are. However, there are also people who seek to use false identity for a wide variety of hostile purposes, e.g. for immigration crime, serious organised crime, terrorism or fraud.

It can therefore be critical to tell whether someone's claim to a particular identity is true or false. This could be at a national border, to open a bank account, or in an online transaction. Assessment of an identity document such as a passport, ID card or Driving License (DL) is an important step to authenticate or disprove a claimed identity.

The challenge of authenticating identity is represented in Figure 1: there is a person; an identity document; and an underlying identity that the person is asserting is his or hers.

Is this association true or false? Do the parts of this identity fit together – or is the person trying to pass off a false identity, maybe in a sophisticated deception? How do you tell?

Figure 1
Person, passport, identity… do these fit together?

We do not want to provide a user's guide to identity deception. Nevertheless, in general there are two primary routes for a deception over identification:

- **Deception about the identity document or other credential** – this can take many forms, including making a completely new but false document (counterfeiting) or starting with a genuine document and modifying it to say something untrue, for example by changing the photograph from that of the holder to a different person.
- **Deception by the person claiming the identity** – this can be done without altering the identity document. For example, trying to enter a country by presenting at border control a genuine but stolen passport where there is a close similarity between the true photo and the 'lookalike' person presenting it.

Of course, an attempt to falsify identity may involve both types of deception. For instance, by succeeding in making a fraudulent application for a new passport and presenting it at a border (this is called a Fraudulently Obtained Genuine (FOG)).

Figure 2 overleaf expands the range of possible means of attacks and shows key means of mitigation or defence against them as well as examples of the type of technologies that might be used.

Figure 2
Risks and potential attacks…

FALSE DOCUMENT

Creating a false document, e.g.

- **Forgery** — amending a genuine doc. E.g., by changing the photo of the holder or maybe by personalising a stolen blank document
- **Counterfeiting** — creating a new false doc., maybe using stolen security paper, security features or high-precision printing (a false document factory?)
- **A Fraudulently Obtained Genuine (FOG)** — a real document obtained by deception

Chip attack

Breaking the encryption is considered 'beyond computational feasibility' but may cause:

- **Disabled chip** — "this never works!"
- **Chip implementation or inspection** — may be poor or incomplete
- **Lookalike** user may not be detected

FALSE OR DISHONEST PERSON

Illegal use of an authentic document

A genuine document used by someone who is not the legitimate holder. The user may not match the holder's photo, but may succeed thanks to:

- lost or stolen documents not reported to the authority
- an expired document
- legitimate holder's permission

Biometric attack

A presentation attack attempts to disguise the person's biometrics and therefore identity. E.g. using a mask, a photo in front of the face, morphed images of >1 face, deep fake computer-generated videos, false fingerprints (gummies over the fingertips). In many cases, using a non-live artifact to present in place of the live person.

Dishonesty

Someone declaring their true identity supported by their genuine passport may nevertheless be seeking to deceive someone about their true intentions, e.g. to work after entering a country on 'holiday', to run away after taking out a bank loan; they may also be hiding something they don't want to reveal about their past. Yes, it still happens...

...and Countermeasures

Document Examination

Close examination of a document to check if it is genuine. Does the document 'look and feel right'? Is the quality as it should be? Are the proper security features in place? No evidence of tampering?

- **(1) Human checks** — by general public; trained specialist; expert with access to forgery lab?
- **(2) Optical Machine Authentication (OMA),** e.g. using a desktop scanner (OSA); or
- **(3) Automated Photo Authentication (OPA)** — using the on-board camera + processing on a smartphone or on the cloud.

Human document examination

Standard—tilt, look, feel

Expert—different light sources / types, magnification

OMA = OSA and OPA

Automated Inspection:

Scanner or smartphone

Interview

Interviewing someone about a document can give useful insight and strengthen assurance—or concern

Document reference system, e.g.

- **Watchlist** — e.g. of lost / stolen passports in country
- **Global w/list** — INTERPOL Stolen + Lost Travel Docs

Electronic Chip verification

ePassports and certain other documents contain a secure chip protected by cryptographic digital signatures: Public Key Infrastructure (PKI).

Public Key Directory (PKD)

Library of public encryption keys used to authenticate (= give trust in) secure chips and the data they contain (ICAO)

Biometric testing, eg.

- **Biometrics** are used to verify a person against a doc. photo, visa photo / fingerprints
- A **One to Many** search will check for different names the same person may have used
- Advanced matching algorithms should help with **Presentation Attack Detection (PAD)**
- Online, **liveness detection** is very useful.

Automatic Biometric Identification System (ABIS)

Database to link biometrics to identity

Person reference system, eg.

- **Watchlist** — persons of interest, known criminals, organised crime group members, terrorists...

1.1
Document authentication: finding the right balance between human and machine

Traditional examination of identity documents is done by a human operator with appropriate training for the task. Particular attention is paid to border officers who receive training on; identifying forgeries and counterfeits; comparing chip or printed photos with the person presenting a passport; and on operating border systems. Further backup may also be provided by officers with laboratory equipment, specially trained to detect advanced forgeries. Basic training for less-experienced operators will be less effective but can usefully emphasise the need to compare faces and document photos carefully, pay attention to the person's behaviour and conversation and to be aware of more common forgery techniques and detection such as LOOK, TILT, FEEL.

Relative advantages of human versus machine examination could be summed up as:

- **Human authentication** – able to combine examination of the document with a more holistic assessment of all the interaction with the person, knowledge of current forgery trends and significant experience on the job.
- **Machine authentication** – For commercial organisations, machine authentication will help their staff validate documents they do not see often, or it will remove completely the decision from the untrained operator. For remote identity verification whether commercial or government (e.g. US pre-fly mobile phone app or eGates) it will automate authentication where a company agent is not present. For border control personnel, machine authentication provides more active support, especially for less experienced human operators who are more likely to becoming tired after a long session on the control.

According to the use case, the right balance between human and machine authentication should be found to obtain the required level of trust in the authentication. For some use cases (such as border control and secure document issuance), machine authentication will not replace human authentication. It will be more likely be a tool used by the person inspecting the document to assist her/him in authentication by enabling faster controls and to focus on the truly challenging/suspicious cases.

While using an automated solution, the operator should continue to be vigilant for any evidence that an identity is being used fraudulently. Automated systems can be very useful but like any system may give an incorrect result. A human operator can spot evidence that the automated solution does not. The operator should therefore have all factors in mind, even if briefly, and not automatically regard a 'pass' or 'fail' indication as a guaranteed result.

1.2 Optical Machine Authentication (OMA)

Optical machine authentication implies making a visual scan of a document using a camera, which is then analysed in various ways to test its authenticity. In this report the following convention is used:

- **OMA** – covers all forms of optical scanning and authentication. (The ICAO best practice guide on optical machine authentication uses the term Machine Assisted Document Security Verification (MADSV), which is equivalent to OMA, here).

Document scanner (Thales)

- **OPA** – covers Optical Phone Authentication, using smartphones. These are highly mobile and can be moved to view the document from multiple angles. According to the level of assurance needed, OPA will be adapted to:
  - » Assist human controller in the authentication decision for instance for mobile border control (page 15) and for front-line policing (page 17)
  - » Fully performed remote identity proofing: eKYC for the private sector (page 17) and for governments (page 18).

Optical Phone Authentication (IDEMIA)

- **OSA** – covers Optical Scanner Authentication, typically using a desk-mounted scanner. These scanners include more sophisticated light sources (visible, UV and IR light), but are less able to test security features that change when viewed from different angles. OSA is specially adapted to the following use cases:
  - » Full automated machine authentication at automated border control (eGates, kiosks…) (page 15)
  - » Assisting human authentication at arrival desk –border control (page 15) and for private sector for KYC processes (page 17)

1.2 Optical Machine Authentication (OMA) (continued)

1.2.1 What you need to know about OMA:

- Documents that can be tested by OMA include passports, visas, ID cards, Driving Licenses (DLs) and currency (banknotes).
- Authentication of OMA features can be performed online or offline according to the solution and country-specific needs (some solutions can operate in either mode). When performed offline, it means that the machine will embed an algorithm that will perform the authentication by itself. Online, the image will be sent to the cloud where the algorithm will perform the authentication. Special attention should be paid to the choice of cloud solution: public or private to comply with security, data privacy and regulations (for example GDPR).
- The pros and cons between an online and an offline authentication solution can be summarised with the followings:

Online

» Pros: Solution can access the latest version of algorithm and/or document libraries

» Pros: Process can be done on the cloud for faster performances on smartphones

» Cons: Solution is not available if no internet connection

» Cons: Solution may work with only specific devices or smartphones

Offline

» Pros: Solution is available anytime

» Pros: Solution sold with the adequate device

» Cons: Periodic update to be done, solution is more difficult to maintain and manage

» Cons: Limit the functionalities and amount of data you can access using a smartphone or tablet

- OMA can be used in a wide variety of settings, e.g. financial services, car rental, access control, security, e-commerce, gaming, government services, healthcare and hospitality.
- Depending on the use case, the relative needs in terms of level of assurance and convenience for the user will vary. For a governmental use case, achieving a high level of assurance may be more important. Of course, a solution that can provide both high level of assurance and a convenient user experience will be easier to adopt for a wider range of use cases.
- While a secure chip integrating biometrics brings the higher level of assurance in document authentication (eIDAS, ICAO PKI security mechanisms) - integration in some ID documents of some security features enable OMA to act as either a fallback, complement or replacement of the chip. This also brings a high level of assurance for four main reasons:

  1- Not all documents are integrating a chip.

  2- For any technical reason chip may be unusable (the chip is killed or is malfunctioning, or the hardware is defective).

  3- Access to the chip is prohibited/forbidden for legal reasons (i.e. For ID proofing for the private sector).

  4- Not all chip security is checked properly using external certificates. Combining chip authentication and OMA makes life much harder for fraudsters.

OMA solutions can be broken down to the different categories described below. It is important to note that some technologies and security features are only available from a few certified document manufacturers or component suppliers. While this is good for document security, it also means that some proprietary technologies can be exclusive to a single supplier, carrying a risk of customer lock-in that needs to be assessed and managed. Just because a feature is exclusive to one vendor does not mean that an issuing authority should automatically avoid its use. When modernising a document, the right balance has to be struck between holistic security and a possible desire to avoid using proprietary technology.

- Two key points to remember when integrating OMA security features into a document design: Firstly to enable a high level of assurance that the document is authentic (for example not a photocopy) and secondly to prove that it is the right owner that presents the document:

  » **To fight against deception about the identity document or other credential:** The solution should check the integrity of the document to ensure it is genuine, that it has been issued by a trusted authority and that it has not been altered. The best way is integrating security features into the design that protect the holder's information, especially the portrait, which is both the most attacked (for example against morphing attack) and most scrutinised area of a document.

  » **To fight against deception by the person claiming the identity:** For remote authentication, the solution should enable proof that the right ID document is presented by its rightful holder to allow identification. This can be achieved in various ways, such as with an OMA security feature protecting the portrait, which can be authenticated and enables a trustful comparison between the ID document portrait and the holder's face with facial matching.

1.2
Optical Machine Authentication (OMA) (continued)

The following examples show different ways in which OMA technologies can be implemented…

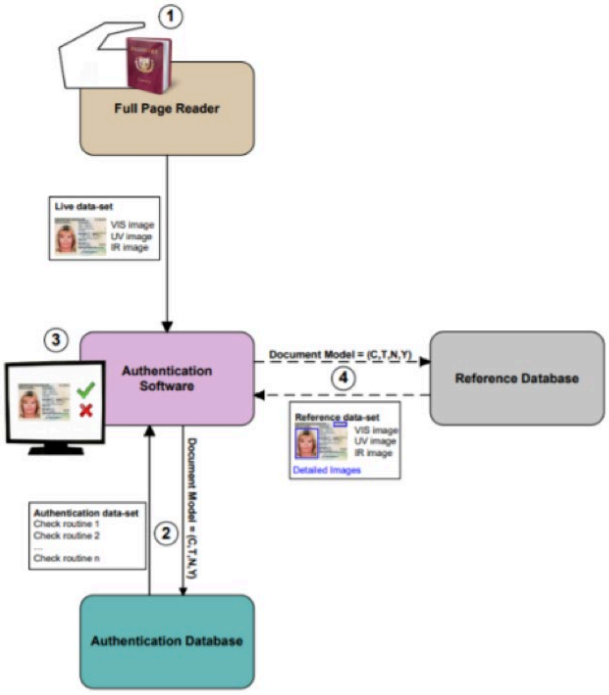
(1) Template verification – scanning the key part of an identity document (in a passport: the biodata page) and checking the image of the document against templates of related documents stored in a reference database, which can include use of visible, UV and IR light.

Today, this is the most widely deployed type of OMA solution, as it has been common practice for border control use cases. The optical authentication can be performed online or offline. An algorithm will perform multiple tests: check the consistency of the Machine Readable Zone (MRZ); compare it with the Visual Inspection Zone (VIZ) of the MRTD; perform the B900 test (MRZ IR ink test); and many more recommended in ICAO's Best Practice Guidelines for Optical Machine Authentication, Part 1 (see references). This assists the operator authenticating the document and helps them to fight against deception regarding the identity document to a certain level.

Some limitations exist with this solution. A lower level of assurance is achievable with most smartphones (OPA) compared to scanners (OSA), because a smartphone will typically provide only visible (VI) light, but not UV or IR. In addition, this solution is not able to detect automatically good quality portrait substitution, tampering of security features (like holograms), fine lines or superior quality paper copies. Consequently, it is not always possible conclusively to make the link between the holder and the ID document and therefore to counter deception by the person claiming the identity.

22nd picture: ICAO Best Practice Guidelines for Optical Machine Authentication

Source: Keesing



MRTD Best Practice Guidelines for Optical Machine Authentication

Process of document identification and verification; the numbers denote the order of the involved process steps

Source: ICAO Best Practice Guidelines for Optical Machine Authentication (Part 1), Version 1.2, February 2018

(2) Decoding and verifying embedded data – that is encoded in a Visible Digital Seal (VDS), barcode or other features.

Such features are now well deployed in document design, for example the 2D barcode embedded in the new Schengen visa, which can easily be read and verified using a scanner/smartphone. Depending on the issuance implementation, an algorithm will extract the data (either online or offline), which can be personal information and/or biometrics. The operator will then be able to compare the decoded data with the data on the document to authenticate it.

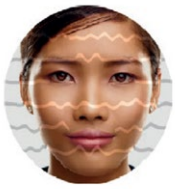
This solution, by authenticating the holder's data, will allow counter deception regarding the identity document with a good level of assurance when cross-checked with the printed and chip data, although limited by the fact that most of the time, this solution will not protect against portrait substitution. Consequently, it will not enable creation of a link between the ID document and the holder in order to counter against deception by the person claiming the identity.

European Visa with a Visible Digital Seal (VDS)

(3) Verification of physical document integrity – using **software functionality** to verify the integrity of the document or other specific security features.

Here a scanner and/or smartphone will capture an image or video of the document. This capture will then be analysed by a specific algorithm, either online or offline, which will authenticate a specific security feature. This type of feature is a rising trend in document design and provides operators with a clear yes or no authentication answer to guide them in their decision.

Those OMA features can enable the authentication of a document with a high level of assurance. In addition, they are often designed to protect the data of the holder by using the portrait to verify its integrity. It will then protect against photo substitution and enable remote identification with a comparison between the authentic portrait and live facial matching of the holder. This solution is strong against both deception related to the identity document authenticity and deception by the person claiming the identity.



Encoded Guilloche from Thales

Photometrix from Surys

Lasink Authentication from IDEMIA.

1.2
Optical Machine Authentication (OMA) (continued)

(4) Augmented verification of the integrity of a physical document, which may include using the OMA device as a tool to augment more basic security features (publicly advertised 'Level 1' security features, such as optically variable devices or inks).

Some security features have been specifically designed to be verified manually using the smartphone as a tool to assist human decision-making. For example, asking the user to use the light torch to reveal some specific optical effect is very hard to counterfeit. Linking those effects with a portrait reproduction will help protect against portrait substitution.

As well as automating document examination, OMA solutions can provide an interface that is able to provide guidance to operators with tips and advice (connecting to an online reference library). For example, 'this document should contain visible features that will change appearance / colour when viewed at different angles – look and tilt to see reaction': in other words, they may be able to assist the operator in the authentication of the identity document. Also, combining this technology together with a (2) Decoding and verifying embedded data solution will create an enhanced concept, with a strengthened level of assurance. Benefits are available with both solutions: the integrity of the physical document can be checked manually and the data can be decoded using a smartphone or a scanner to either perform an automated authentication or assist authentication by the controller.

OVM from CST

1.2.2 Use of multiple OMA and other verification techniques

Multiple OMA solutions can be combined to provide a high level of assurance authentication concepts. For instance, combining **(1) Template verification** with **(3) Verification of physical document integrity** will strengthen the level of confidence to remove the drawbacks of template verification (portrait substitution, photocopies…) and cumulate the benefits of each solution.

According to the use case and the level of assurance that is looked for, a solution including OMA can be coupled with additional authentication solutions. Such as:

- verification of electronic data of a secure chip; (e.g. Border control use case, Business / Customer relations…)
- interview of the document holder; (e.g. Border control, Front line policing, KYC,…)
- biometric capture and search /comparison with biometric records; (e.g. Border control, visa application…)
- test for liveness when someone uses a system on a self-service basis; (e.g. eKYC, eGates, Kiosks…)
- and perform checks and/or update reference systems such as watchlists, casework and travel history records; (e.g. eKYC, visa application…)

1.2.3 Co-operation between document design and authentication

Design features can be introduced when a document is manufactured or when an individual document is personalised. For human examination, examples include security features that change appearance or colour, such as Diffractive Optically Variable Image Device (DOVID) and inks that change colour when viewed from different angles. Likewise, for OMA the designer may include security features from the different categories listed above (for template verification, decoding and verifying embedded data technologies, verification of physical document integrity – using software functionality, augmented verification of the integrity of a physical document). They may even relate to an individual holder, to allow an OMA process to authenticate the document more securely. Linking design and authentication in this way maximises the effectiveness of OMA.

1.3
Optical Scanner Authentication (OSA)

This type of OMA is usually a desktop document scanner. Such a solution may well be more robust for frequent, high-volume use and may be able to include a wider range of document sensors such as Ultra-Violet (UV), visible light (direct and oblique), Infra-red (IR), and others. Each of these can potentially reveal particular security features in a given document design. They will however be heavier than a smartphone solution and may not provide the mobility, operator familiarity and ease of deployment and network access advantages of a smartphone.

1.4
Optical Phone Authentication (OPA)

The last decades have seen a steady increase in the power and capabilities of smartphones and similar mobile computing devices (laptops, tablets, wearable devices), as well as an explosion in the performance of mobile broadband communications infrastructure (4G and 5G). It is now typical for law enforcement mobile solutions to carry a wide range of functions and access to information on the 'front line' that would otherwise only be accessible in a fixed office or via radio. This can include checking identity, verifying ePassports and cards, capturing biometrics, searching reference data, entering transactions – and conducting mobile border control.

OMA (i.e. OPA) capability adds to the functions that law enforcement can achieve on the move, with a broad range of other functions. In addition, OPA can give access to automated authentication of documents to non-professionals that are willing to perform in-person verification as well as remote authentication during Know Your Customer (KYC) processes.

Comparing OPA with other checks:

- **Advantages** – quick and easy check that can be used with less skill than having to depend on specialist knowledge and training. Can be used by a wide range of users including those who are not necessarily expert. With OPA particularly, all types of smartphones (even without NFC) can be used to check for optically variable features, a range of functionalities to authenticate other types of security features. It is small, light and easily carried.
  - » OPA is a strong comprehensive solution against risks and threats for all types of operators, who do not have access to confidential watchlist information (e.g. for forgery, counterfeiting, and false biometrics and other attacks).
  - » In eKYC use cases, OPA solutions can be particularly cost-effective. It will enable an easy and reliable authentication; limiting the number of times, the process will require an operator to perform an additional manual adjudication.
  - » OPA solutions are durable and can act as a backup if, for example, the chip of a document does not work or is not accessible by the controller.
  - » OPA solutions will enable secure Digital ID derived from physical documents without electronic chips.
- **Disadvantages** – Not all security features can be tested automatically (most smartphone cameras cannot check UV and IR features). It may be impractical to test multiple pages of a book document (passport), missing multi-page security features. Risk that users do not look carefully for false documents, just whether the indicator light is red or green. Risk of false positives and negatives.

1.5
Interview

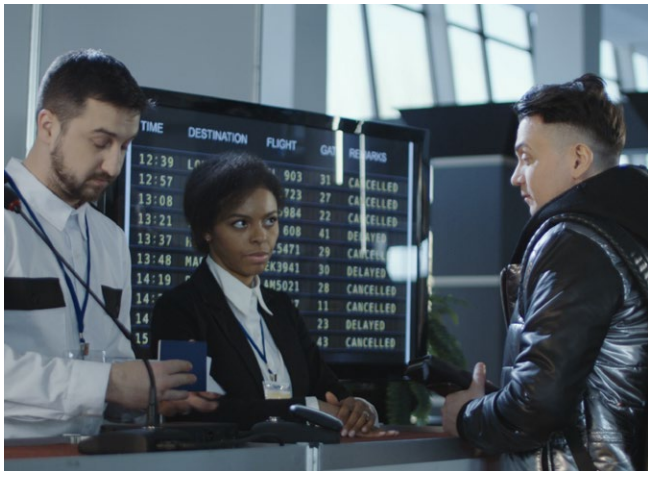
Questions, particularly by someone with training and experience, can be important in testing and establishing facts and credibility of what the subject is saying. Humans can read 'body language' and sense if a person is telling the truth or trying to steer the interviewer away from something he/she is trying to avoid being asked about. An interview can also test complex questions going beyond just identity or the authenticity of a document such as 'what is this traveller's real intention if he enters the country / is loaned the money he is asking for'.

Different training may be appropriate for different types of users. For example, a skilled border officer will need significant training on forgery detection and comparison with passengers; a forgery expert even more time, plus use of specialist forgery lab equipment. On the other hand, someone working in a retail shop may need more straightforward training, such as how to recognise a false document, how to operate the equipment and practical advice on how to respond when the evidence or authentication tests indicate a problem.

Forgery detection and facial matching / comparison skills are important for officers on the border and can be enhanced by training. Automated tests are normally confined to the key part of a passport (biodata page), but a trained forgery officer may spot signs of forgery or counterfeiting across many other features of a document.

Support resources and action that can support front-line interviewing can include good initial and continuing training; secondary (extended) interviewing away from the primary border control; specialist forgery detection officers and laboratory equipment; and confidential intelligence e.g. on current forgery technique and examples recently detected.

- **Advantages** – subjects the person to considered evaluation by another human being in ways that a computer could not. Can form a sense that 'something is not right' about what someone is saying and that a longer interview or more rigorous forgery examination of a document is needed.
- **Disadvantages** – Computers can process far more data than humans, who also get tired and make mistakes.



1.6 Electronic Authentication

Secure documents such as ePassports and electronic bank / payment cards may contain a special chip with information about the subject, together with advanced cryptographic codes (called 'digital signatures'), which can be used to test conclusively that the data on the chip is authentic – it comes from the source it is claiming to have been issued by – and that it has integrity – that no one has modified the data that was put there by the issuer… therefore, that the data can be trusted.

ePassports (known as electronic machine-readable travel documents (eMRTDs)) are defined in standard ICAO 9303. This uses a Public Key Infrastructure (PKI) solution, using private and public encryption keys to sign and authenticate data.

An ePassport contains a secure chip holding a copy of certain information printed on the passport. Several security features protect the data on the chip more strongly than on a traditional passport:

- **Access** – The chip is accessed by a localised radio connection, but only after reading some key data from the title page of the document to generate a secure access code. This is designed to prevent access to the chip when the passport holder is unaware.
- **Data integrity** – Strong cryptographic codes known as digital signatures are used to 'lock' each block of data on the chip, linking it securely to the correct originator - any amendment such as substituting a different face image will be evident because a forger cannot create the correct digital signature for the new data.
- **Chip integrity** – A further test can verify that the chip is the original one issued by the passport authority, not a 'clone' copy of a valid chip.
- **Fingerprints** – in the European Union, additional security is used to protect two fingerprint images of the holder. This can be used as additional confirmation that the passport holder is the right person, whilst protecting privacy.
- **Advantages** – correctly applied and implemented PKI technology gives extremely strong authentication of data and origin. It is the highest level of authentication today.
- **Disadvantages** – specialist and complex; requires special purpose systems, including access to ICAO's global Public Key Directory (PKD) of public encryption certificates. Consequently, electronic authentication is not accessible for all use cases. Additional techniques such as OMA must be put in place as a fallback.

1.7 Biometrics

Long-lasting or permanent features of a person such as face image, fingerprints, iris and DNA can be captured and encoded into a computer system for future reference. For example, to identify the person by searching for a match in a database or to verify that someone is who they claim to be by matching against their existing record.

Biometric systems have advanced substantially in terms of capability, sophistication and performance over the years and are used for identification, and to link together systems between different systems. Two such multi-biometric examples are the HART system being built by US Department of Homeland Security (DHS) and the shared Biometric Matching System (sBMS) being built by eu-LISA for use by Member States of the European Union.

Many of the techniques mentioned earlier can be attempted in relation to biometric identification. Responses come under the heading of Presentation Attack Detection (PAD), which can involve advanced, effective detection and matching techniques, reinforced by robust testing to try an assortment of attacks to see whether the protective measure spots the deception.

- **Advantages** – can give strong assurance on the link between a passport that has been reliably authenticated and the person presenting it for inspection. Biometrics can also establish a reliable link between a biometric sample obtained from a person and records held in an automatic biometric identity system (ABIS). It enables a link between the person and pre-existing records about him or her, even when the person has used a different name on different occasions. It can therefore give a strong defence against someone seeking to use an illegitimate identity.
- **Disadvantages** – possibility that an attempt is made to 'spoof' the biometric test by using a false feature, known as a Presentation Attack, which requires an action to defeat, such as testing for 'liveness' of the subject. A comprehensive biometric system can be large, complex and expensive to adopt and integrate with other systems. Liveness detection and Presentation Attack Detection (PAD) help defend against fraudulent attacks.

Source: Keesing

1.8
Reference systems

Reference systems are also important and can cover issues that will not be noticed by other means. Watchlist systems can include INTERPOL's Stolen and Lost Travel Documents (SLTD) database, travel history, case histories, intelligence, criminal or other alerts for people wanted for arrest for a range of possible offences, or whose biometrics show they regularly travel under false names and documents.

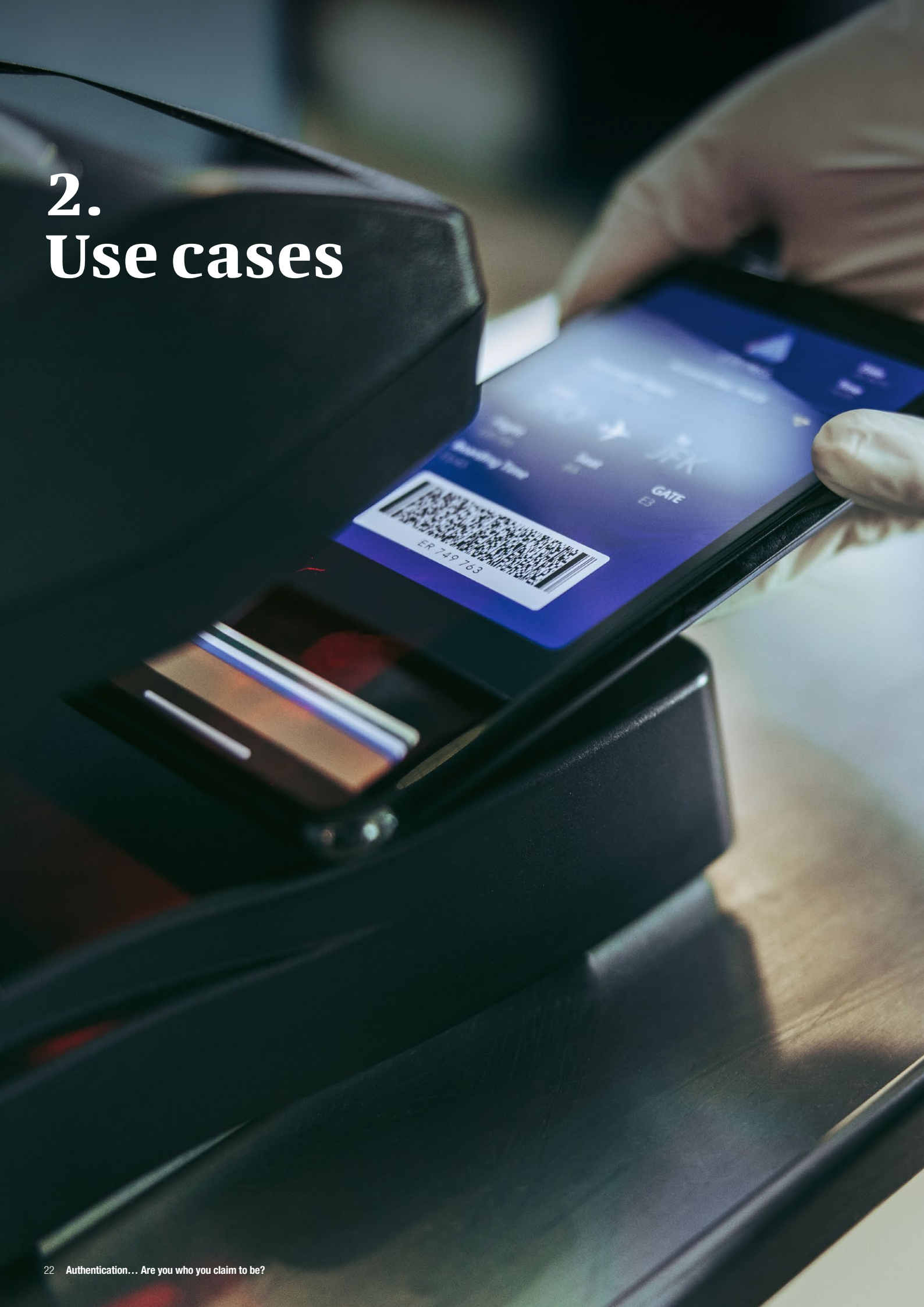
- **Advantages** – a watchlist or other reference system can highlight issues that would otherwise be missed (e.g. the document may be genuine… but it may also have been reported as stolen).
- **Disadvantages** – further cost and complexity of accessing and maintaining these systems; need for careful protection of confidential information.

1.9
Multiple approaches

The techniques already described all have very useful features in proving that identity and travel documents are genuine (or not!) and in proving that a person claiming to have a certain identity is genuinely that person. However, no matter how good any of these techniques are, none of them in isolation can do the whole job in every situation. A wide range of possible attacks may be attempted. A range of tests is therefore desirable to look for evidence of deception and maximise the chances of detecting a false document.

- **Advantages** – using multiple rather than single techniques to test documents and identity is critical, to obtain a higher level of confidence into the authentication.
- **Disadvantages** – extra cost / complexity… no guaranteed success!

2.
Use cases



2.1
Border control

- **Arrival desk** – the traditional border control arrangement with an experienced border officer who can: examine the passport visually and checking for signs of forgery; scan the passport on a specialist reader that checks details against a 'watchlist' of passports that have been recorded as lost or stolen and authenticates the data in the chip using the relevant encryption keys held in the ICAO Public Key Directory (PKD); and who speaks to the traveller. If the person must demonstrate that they meet certain criteria (for example, that someone claiming to have come for a holiday can support himself and has not come to work illegally), then officer assesses the overall validity of all the evidence – is this traveller and the evidence of her/his identity credible and consistent, or are there discrepancies that need further discussion?

  How to ease authentication with OMA? OMA will enable to perform authentication as a fall back when electronic authentication cannot be done (no chip in the document, chip is not functioning). In addition, OMA enables border guards to perform pre-checks in the waiting line when facing crowded borders.

- **Mobile border control** – can include several examples…

  » NFC reader and passport chips – many smartphones are equipped with a Near-Field Communication (NFC) antenna to read cards and passports when they are in close proximity. With the on-board camera being used to read the MRZ on a passport or card, this provides the ability to read and authenticate eMRTDs (ePassports / cards).

  » On-board camera and biometric acquisition – small, portable biometric readers can be connected to a smartphone. In addition, software is available to configure the on-board camera on a smartphone to read fingerprints, which can be used to search an automatic fingerprint identification system (AFIS). Biometric capture and verification may be needed for types of border control including the EU Entry Exit System (EES).

  » Mobile border control – some situations require full border control to be carried out on the move, e.g. on a train or ship. With increasing adoption of rigorous technical controls and biometrics, this requires mobile systems to be provided with capabilities equivalent to those at fixed locations, such as a border control desk at a major airport. It is however becoming realistic to build a mobile system with a tablet or smartphone with that capability: the NFC and camera use described above shows how major components can be provided technically on the move. Nevertheless, care is needed to ensure the full business process can be carried out realistically.

IDEMIA

2.1
Border control (continued)

- **eGate or Automated Border Control (ABC)** is an automated equipment, which can substitute for a border officer at a control desk, as described above. Typically, the passenger enters the gate and opens then presents his/her passport to the reader device (similar to the one used by a border officer), which performs the same checks. The passenger is then directed to look at a camera, which captures a face image and verifies there is a clear match with the authenticated photo in passport chip, using facial recognition (FR) technology. If all these stages are completed satisfactorily, the passenger passes through the gate and is admitted to the country. If not, he/she must be examined by an officer supervising the gates who may have some further questions. Because a successful passage through the gate does not involve an interview with a border officer, eGates are typically limited to travellers who have an authorisation to enter the country – a national of the country, or someone enrolled in a Trusted Traveller Scheme who has been cleared to enter without interview. In effect, eGates filter out 'easier' passengers arriving at the border, allowing skilled and experienced officers more time to examine passengers who need more consideration.

How to ease authentication with OMA?
OMA solutions (especially those who fight against a false copy of a document) will strengthen the document authentication when coupled with other authentication means.

- **Kiosks** – a kiosk is an alternative solution with some of the elements of an e-Gate. A typical configuration is that the traveller arrives first at the kiosk (a self-standing desk with a screen, keyboard and passport reader, but no gate). The traveller scans his/her passport, which the system will recognise from Advance Passenger Information, and answers questions such as the purpose of his/her visit; arrival flight; customs; health and food declaration, etc. When these are completed, a coded ticket is printed out. The traveller then presents this to the officer at the arrival desk; but in the meantime, the system has been able to make checks on the information displayed to the officer once the traveller presents the ticket from the kiosk and his/her passport.

How to ease authentication with OMA?
OMA solutions (especially those who fight against a false copy of a document) will strengthen the document authentication when coupled with other authentication means.

2.2
Front-line policing

- Powerful and capable mobile smartphones have become a regular part of everyday life for most people and the police and other law enforcement is no exception for where they can have useful application. Well-designed mobile systems enable officers to undertake a wide range of functions when dealing with the public on the street and front-line. They can receive the results in real-time from core systems they would otherwise only be able to access back in the police station, or by speaking over voice radio to their control room. This can include checks on a person; various types of document; vehicles; issue penalty tickets; complete the hand-over to the central system for enforcement checks; and integrate their mobile system with the central command and control system.
  Two fundamental questions when an officer is dealing with someone who appears suspicious are “Who is this?”, and “What do we already know about him / her?”. A good mobile solution can resolve many doubts, increasing detection of people that are wanted and avoiding unnecessary arrests.

An Garda Síochána (the Irish Police)

2.3
Business / Customer relations

including Business to Customer (B2C) and Customer to Customer (C2C) authentication.

- **Assisted document authentication – Know Your Customer (KYC) –** regulations on financial services often require companies and professionals to use due diligence to verify the identity and risks involved in having a business relationship with a new customer, as part of an overall framework of Anti-Money Laundering (AML).

  How to ease authentication with OMA?
  OMA will enable the authentication of all types of documents using only a smartphone (easy to deploy). It can be coupled to a liveness check for better security.

- **Remote Identity Proofing and onboarding** – this is the online form of KYC and is similar to an online visa application. Information supplied by the applicant can be checked against the financial institution's own information and databases held by agencies that provide credit rating services. This process is required for banks and financial institutions to verify the identity and integrity of someone wanting to do business with them, e.g. opening a bank account. This is often done with a potential customer applying online where there may need to be a reference to credit rating agencies, who compile information about someone's financial history and creditworthiness. The challenge here is to authenticate the document with a good level of assurance, but also to link it to its holder to avoid deception by the person claiming the identity.

  » **Self-service enrolment** – are accepted by many immigration authorities for visas or visa waivers and by banks for opening a bank account. Additional questions may be asked; ID documents or passport may be scanned and the chip read; biometrics may be captured using 'selfies'; liveness detection may be performed; biometrics captured initially may be verified when the person attends an interview or (for visas) arrives at the border to enter the country.

  » **Visa application** – for many countries a traveller can apply for a visa online, providing access to his/her passport (and chip) via the NFC antenna of his/her mobile phone; providing a 'selfie' photograph, which can be checked (FR) against the passport image and/or against a previous application if one exists; and various technical checks can be made to test that the 'applicant' is genuine and alive, not a fake (Presentation Attack Detection). Information supplied by the applicant can be corroborated against reference databases owned or used by the agency. Remaining doubts about the person can be validated in-person at a later stage, e.g. when an in-depth interview is conducted (often required to obtain a visa) or when a visa-holder arrives at the border.

  » **Boarding pass** – allowing the citizen to download a barcode, which is accepted at the airport to board an aircraft – it is important to consider the security of this solution. Came into use in 2007.

  » **Digital Identity derived from a physical document** – Digital identities (credentials that are available in a mobile solution: DTC, Digital Driver License, Digital NID) will soon be available and adopted by citizens. One way (perhaps the most inclusive) to create those digital identities (DI) will be to derive the DI from the physical document. To ensure the security of this derivation, documents will need to integrate features (electronic or physical) that enable a secure communication and authentication by the mobile device.

How to ease authentication with OMA?
OMA will enable authentication of every type of documents using only a scanner with a PC or a smartphone. To fight against deception of the credential and/or of the person claiming the identity, a good solution would be to integrate into the document design an OMA feature that can be authenticated by a smartphone using dedicated software. In addition, this feature should protect the personal information, especially the portrait, as it is the most attacked feature and best way to link the document to its holder using, for example, a comparison between the portrait and face with biometric matching. With this solution, fraudsters will not be able to present a fake document, a photocopy or video (with the right security feature) and the company performing the authentication will be able to identify the person behind the screen.

Keesing

- **Health Pass –** designed to give assurance of the health of passengers. As we emerge from the COVID-19 pandemic, this may also become a necessity (see earlier description under electronic authentication).Various forms of Health Pass using electronic authentication are under consideration to enable a traveller to prove that he/she has had a recent COVID-19 vaccination and possibly a negative COVID test or has recovered from COVID-19 and is considered to have some immunity. Consensus on what solution(s) will be agreed is yet to emerge – possibly a combination of solutions for different components of the overall solution. It may be that a hard copy (printed) version including a digitally signed barcode may be accepted alongside a smartphone-based solution. In both cases, the need to read and authenticate health-related data may arise in addition to other forms of encoded / signed data already described in this paper.

WHO example of a possible hard copy and mobile-based health certificate

3. Recommendations

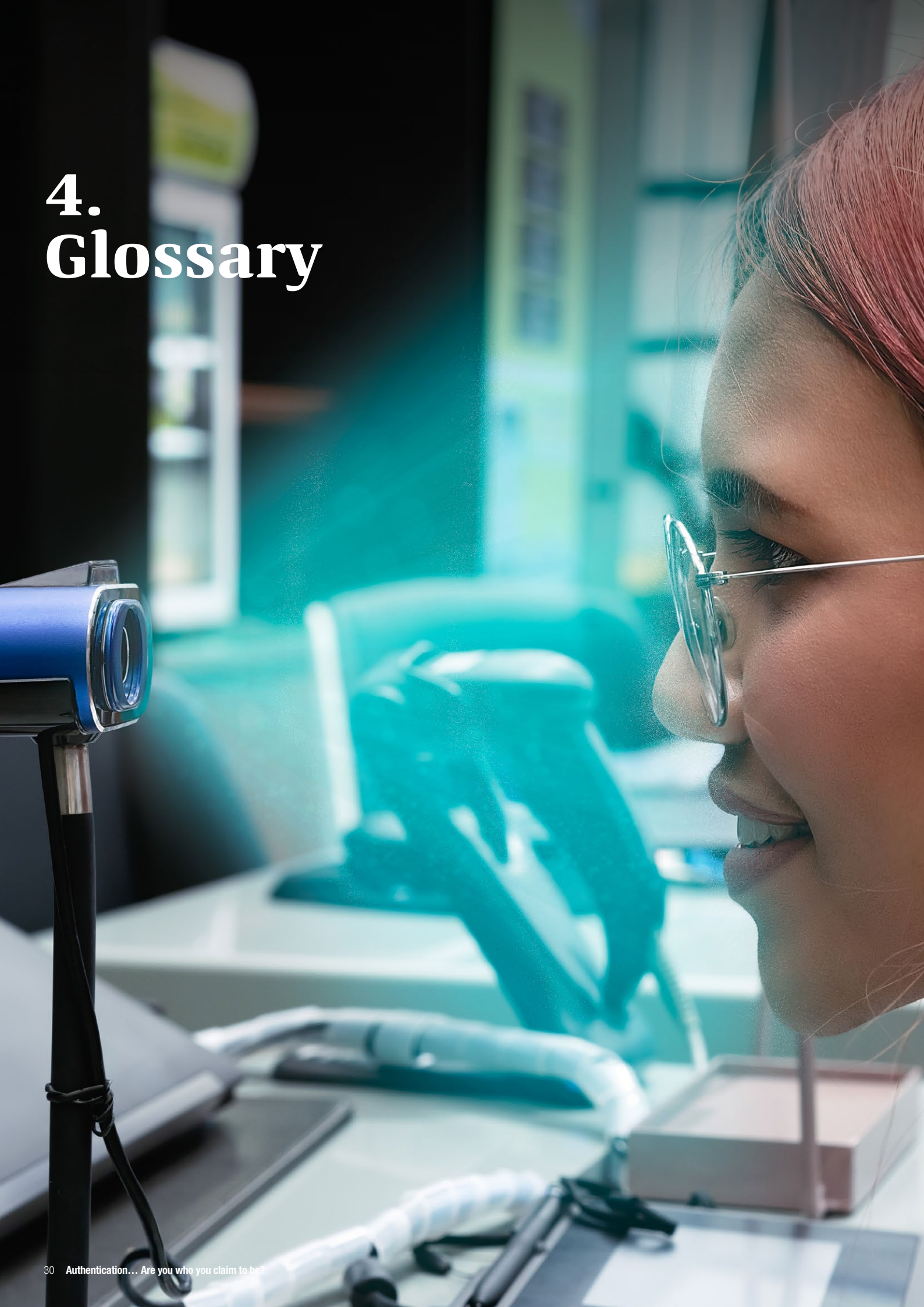
We hope the discussion in this paper is helpful. In conclusion, we offer some recommendations about effective authentication of documents and identity, particularly using automated means:

- **Take this subject seriously!** – There is an increasing movement to digital and online evidence and transactions--the scope for identity fraud is therefore increasing, as is the need to protect against it. A US Association of Certified Fraud Examiners survey in November 2020 found 79% of respondents had observed greater fraud in the previous 12 months; and 90% expected greater fraud in the next 12 months - cyber fraud, payment fraud and, particularly, identity theft (www.acfe.com/covidreport.aspx). There are many ways of attempting identity fraud, as summarised in the section on risk.
- **Machine Authentication offers an increasing means of protection and should be considered.** This paper has given several examples of Optical Machine Authentication (OMA), using a traditional desktop scanner (OSA) and increasingly important, using a smartphone (OPA). These solutions offer real benefit and should be given serious consideration-- to be explored and studied, to be evaluated and tested in pilots and where appropriate, to be deployed operationally.
- **When choosing a solution, take into consideration that OMA is the more inclusive solution in authentication:** it can be used easily by everyone (private or public sector as well as citizens themselves); it can be deployed for every use case, even when other verification techniques are not available. It is especially adapted for use cases that do not need access to confidential information (for example certain forms of electronic authentication and international watchlists).
- **More detailed considerations** are also recommended:
  - » **Document design** – can include security features that make automated authentication easier and more effective (document specialists can help).

    Including security features that enable Optical Phone Authentication would be a must, considering the rising authentication needs of both the private and public sectors.

    To fight against deception about the identity document and deception about the person claiming identity, an additional benefit would be to have an OPA security feature included into the document design that protects the personal data of the holder and authenticates its integrity. Especially the primary portrait as it is the main attacked feature by fraudster and best link to make the connection between the document and the holder.
  - » **Infrastructure** – can also help--technical solutions and organisational. For example, in providing up to date templates of new document types and connecting to the Public Key Directory (PKD) to authenticate eMRTDs.
  - » **Training** – should be included and adapted to the circumstances and users in any context (for example, border guards and retail shop assistants need to know how to check documents, use their authentication equipment and respond to alerts, even though the time and detail needed will differ). Also, a special attention should be given to privacy issues.
- **Multiple ways of authentication are better than one** there is no one solution that does everything in any situation, as we have tried to explain in this paper. Optical authentication, electronic (PKD) checks, face-to-face interviews, reference systems and biometrics can play a part: the right solution must be selected for each case.

4. Glossary



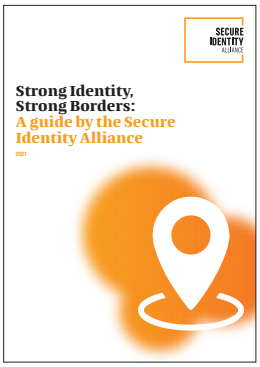
ABC	Automatic Border Control (eGate)
AFIS	Automated Fingerprint Identification System
CAN	Card Access Number
DHS	Department of Homeland Security (US)
DOVID	Diffractive Optically Variable Image Device
DTC	Digital Travel Credential
EMV	Europay, Mastercard, Visa – financial card standard, including Chip + PIN
eMRTD	Electronic Machine Readable Travel Document (standard: ICAO 9303)
EU	European Union
eu-LISA	European Large Information Systems Agency (EU)
FR	Facial Recognition
ICAO	International Civil Aviation Organisation
IR	Infra-Red
KYC	Know Your Client / Customer
MRZ	Machine Readable Zone
NFC	Near Field Communication
NID	National Identity Document
OMA	Optical Machine Authentication
OPA	Optical Phone Authentication
OSA	Optical Scanner Authentication
PAD	Presentation Attack Detection
SIA	Secure Identity Alliance
UV	Ultra-Violet
VIZ	Visual Inspection Zone of an MRTD biodata page

Other reports by the Secure Identity Alliance:

https://secureidentityalliance.org/ressources/publications

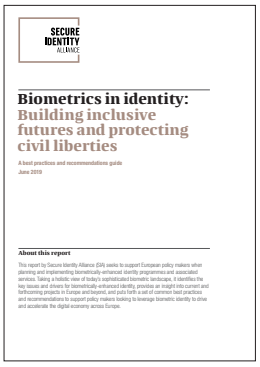
Passport Fraud Trends and Ways to Combat Them

The purpose of this report is to draw a clear link between the problems of document and identity fraud faced by issuing and control authorities, and selected private organizations such as financial services institutions. It also explores some of the technical solutions to those challenges as proposed by the global identity management industry.



Strong Identity, Strong Borders

Looks at the need for border authorities to balance security and protection with efficient and frictionless passenger experiences. In addition to the major drivers shaping the future of the border control space, the report looks at the vital - and complex - role played by identity management, highlighting some of the evolutionary technologies incl. automation, biometrics, mobile, and bringing those solutions to life in the form of case studies from around the world.



Biometrics in identity: Building inclusive futures and protecting civil liberties

This report seeks to support policy makers when planning and implementing biometrically-enhanced identity programmes and associated services. Taking a holistic view of today's sophisticated biometric landscape, it identifies the key issues and drivers for biometrically-enhanced identity, provides an insight into current and forthcoming projects in Europe and beyond, and puts forth a set of common best practices and recommendations to support policy makers looking to leverage biometric identity to drive and accelerate the digital economy across the world.

Giving Voice to Digital Identities Worldwide

Providing unprecedented 'on the ground' insights and perspectives, the study produced in partnership with onepoint gives a unique voice to stakeholders from 25 innovative sovereign digital ID schemes. Their shared learnings highlight the guiding principles and good practices that are critical for driving usage, adoption, and success – regardless of the digital ID model adopted.

SECURE IDENTITY ALLIANCE