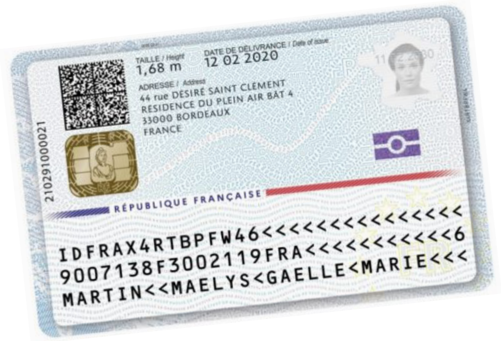
Elyctis White Paper

Reading ID documents needs to combine security, interoperability and efficiency

Reading ID documents is a need that is increasingly frequent in a wide variety of situations. If, a few years ago, reading ID documents was only a prerogative of border officers and law enforcement personnel, it is now a task that happens in a wide variety of situations: voting, financial institutions enrolment, healthcare services, onboarding for many services, hotel reception, age verification, rental car, etc. In addition, ID control is increasingly performed by non-professionals, including hotel receptionist, car rental clerks, healthcare professionals, bartenders, bank employees, etc. who cannot receive an extended training on the topic. Consequently, ID verification needs to be made secure, easy and reliable at the same time.

At the same time, ID documents have greatly evolved. Nowadays, almost all ID documents are based on smart card technologies, *i.e.* they include a contactless or contact chip that can be read by a reader. These data are protected thanks to a variety of cryptographic means, one of them being a code that is printed on the document itself in the Machine Readable Zone (MRZ).



TAILLE / Height 1,68 m
DATE DE DÉLIVRANCE / Date of issue 12 02 2020
ADRESSE / Address
44 rue DESIRÉ SAINT CLÉMENT
RESIDENCE DU PLEIN AIR BÂT 4
33000 BORDEAUX
FRANCE
210291000021
RÉPUBLIQUE FRANÇAISE

```
IDFRAX4RTBPFW46<<<<<<<<<<<<<<<
9007138F3002119FRA<<<<<<<<<<<6
MARTIN<<MAELYS<GAELLE<MARIE<<<
```

The presence of the chip in almost all ID documents allows to verify their authenticity, ensure they have not been cloned or altered and contain the document holder's biographic and biometric data in a secure manner. Already more than 100 countries are issuing ePassports and over 490 million ePassports are in circulation, according to *ICAO (International Civil Aviation Organization)*.

Electronics are secure and reliable

Smart card technologies have proved their reliability thanks to decades of massive use in various fields, such as banking cards, SIM cards, etc. Consequently, any information that comes from an ID document chip is secure. There is no known way by which this information could have been altered.

Typically, the chip contains all the needed information for an identity reading: type of documents, full name, gender, date of birth, characteristics of the document (type, expiry date), … The chip also contains a digitized photo of the holder, biometric information such as a signature of his/her fingerprint or iris scan.

By reading a chip, one ensures that the chip has been issued by a genuine issuer, and that it has not been cloned or tampered with in any way.

In other terms, the information that comes from the chip is a lot more reliable than the information printed on the card (or passport data page). Access to this information is dependent on a set of authentication methods; many of these authentication methods include the reading of the Machine Readable Zone (MRZ) to unlock the chip.

As the information in the chip is a lot more trustworthy than the information printed on the e-ID document (or ePassport datapage), reading the MRZ is always a requirement while reading the full surface of the document is useless. For this reason, reader developers favor so called half-page readers, that read only the MRZ rather than full page readers that try to read a full e-ID document page. A half-page reader can be built with the best user friendliness and is able to read the MRZ in a second, thus making the whole operation smooth and efficient for ID verification operators.

Available readers to access e-ID documents

Dedicated ID documents readers have in common a series of characteristics. They have been built with user-friendliness in mind and are adapted to professional usage. In an adequate e-ID document reader, the necessary optical reading and the chip reading take place in a single step. A dedicated high-performance scanner is used to ensure an accurate reading of the MRZ, that gives access to the chip data. As data in the chip are more secure than the ones printed on the card, a half page reader, dedicated to reading the MRZ, is the best option. A professional NFC reader, with a high throughput is used to ensure that not only all ISO-standard e-ID documents will be read seamlessly but also that data will instantly be sent to the application. A dedicated ID document reader ensures it is able to read the chip regardless of its location in an ePassport: front cover, back cover, datapage or even elsewhere.

An alternative solution may be to use an ID reading application on a regular smartphone. This solution may be adapted to infrequent ID readings. It does not require a dedicated piece of hardware but it can hardly be deemed professional. Known issues in this context include poor lighting of the ID documents, difficulties in reading the MRZ, different locations of the NFC antenna making operation uncertain for the user, and unqualified NFC chips in the handset that may not be able to read all ID documents.

Different types of e-ID document readers are available on the market:

- Full page e-ID document readers read optically the full printed information from the e-ID Document (or the datapage in the case of an e-Passport), including the MRZ to obtain data that are used to access the e-ID Document chip, among which two categories: Static scanners and Swipe-through scanners,
- Half-page e-ID document readers read optically only the MRZ and use the read data to access the e-ID document chip,
- An alternative solution is a dedicated app on a smartphone, that uses the smartphone camera to read either the MRZ or the full printed information and then the NFC reader to access the chip information of the e-ID document.

ELYCTIS Half-page reader

	Full page Reader	Half page Reader Static	Half page Reader Swipe	Smartphone app
MRZ data reading	✓	✓	✓	✓
Full page read incl. physical security features (Ink, UV, IR)	✓	Useless	Useless	Depend
Integrated Contactless chip reading	✓	✓	X	✓
Integrated Contact chip reading option	✓	✓	✓	X
Authentication methods	All	All	All	All
Simultaneous read MRZ & chip	✓	✓	X	X
Reading without movement	✓	✓	X	X
Desktop and Mobile use	Desktop only	Desktop & Mobile	Desktop & Mobile	Mobile only
User-friendliness	+++	+++	- -	- - -
Reading speed (MRZ and Chip)	+++	+++	-	- - -
Size, weight, ease of integration	- - -	+++	+	NA
Cost	€€€€€	€€	€€€	€

Security is to be adapted to each context

Not all ID applications require the same security level: checking if a person is over 18 before delivering alcohol or tobacco is obviously less critical than the enrolment of a citizen biometric features for the delivery of a passport.

Typically, a secure e-ID Document (ePassport, National e-ID card, e-Driving License, etc.) identity check is performed in several steps:

At first, the e-ID Document reader needs to read the MRZ, in order to get data that will allow it to access the e-ID Document chip. Then, the interaction between the e-ID Document and the reader will allow to answer the following questions:

Is this e-ID document authentic and genuine?

Does the e-ID document belong to the person standing in front of me?

The answers to these two questions are covering a large majority of what is required on most of the use cases related to e-ID applications.

Use cases

There is no such thing as a universal e-ID document reader. The requirements for e-ID readers vary from application to application. Depending on the application context, ID documents reading may take place on a desk, in a kiosk or on the move, driving the need for fixed, integrable and portable readers. Also, the way ID document reading interacts with an application will play a role in the reader choice. Finally the number of documents to be read in a day will also drive the choice of the reader.

Citizen registration

Governments are in need of enrolling their population to generate e-ID documents including ePassports, ID cards, voting cards, driving licenses, healthcare cards, etc. Citizen registration is also needed for governments setting up a population register.

In order to do this, it is often necessary to read existing ID documents.

Citizen registration typically takes place in a government office or agency. A half-page ID document reader sitting on a desk or embedded in a kiosk is the best solution to allow professional and secure operations.

ID delivery

In most countries, e-ID documents, such as ePassports, e-ID cards, voting cards, driving licenses, healthcare cards, etc. are manufactured in a central location and then delivered to the citizen. Of course, the delivering entity, often a civil servant or dedicated agency employee, has to verify that each document is delivered to its rightful owner. This means that the employee needs a reader to read the MRZ and access biographic and biometric data. The citizen will be biometrically authenticated thanks to these data, before receiving his/her new document.

Elections

Depending on government choices, citizens have to present their national ID card or a dedicated voting card to be able to vote. In all cases, their identity needs to be read and verified against an electoral roll.

Consequently a typical voter identification requires to read the MRZ thanks to a half-page scanner and then the e-ID document chip. This ensures the document has not been tampered with, and a fingerprint scanner, or simply a visual control of the photo ensures the voter is actually the owner of the document. Data are also controlled against the electoral roll before allowing the citizen to vote.

Border control

In many cases, border control takes place in a fixed border post. It is part of the role of an immigration officer to read thousands of e-ID documents a day. An efficient operation of a border post can easily be measured when persons who are entering the country legally are whisked through the border leaving time for the immigration officers to take care of specific cases. To achieve this, a professional half-page reader that reads the MRZ and the chip simultaneously is the best solution, however due to rare exceptions where the travel document still does not have a chip, full page scanner is still the preferred solution.

Law enforcement ID verification

ID verification is a typical part of the role of law enforcement officers. Typically, during an ID verification, the officer needs to visually control that the person presenting an ID document is its actual owner. To resist counterfeiting and ID theft, the only secure information in an ID document is the one in the chip. In an ID check situation, the law enforcement officer needs a dedicated professional reader able to read the MRZ from the e-ID document and to use these data to access the chip content. This way, the officer is able to compare the photo in the chip with the face of the controlled person.

Healthcare rights

Many governments and private entities have set up health insurance systems. In order to keep the system operating, one needs to authenticate that the person receiving healthcare services is actually entitled to them and the care provider will be paid for the services. Depending on contexts, some public and private insurances have issued healthcare cards while others rely on their country national ID card infrastructure.

Car rental and hotel registration

In the case of a car rental or hotel registration, the need is to record the identity of the person coming to the counter. To achieve this, the receptionist needs to insert the customer e-ID card, driving license or ePassport in a reader. Then the reader reads the MRZ of the e-ID document, and is able to access the biographic data of the card/ePassport holder and the photo

Remote onboarding

There are situations where a consumer is required to prove his/her identity remotely, and the whole process is conducted automatically. To do this, consumers will use their mobile phone to communicate with the onboarding platform, They will scan their ID document with the camera and in some cases use the NFC functions of their handset to access data in the chip of the document. They will also use the camera to show their face and prove they are alive. All verifications are performed on a host server.

Many obstacles may prevent an efficient operation of home onboarding: it may be difficult to analyze a document read under poor lighting conditions, reading the MRZ may not always be successful due to lack of light and quality of the camera, and reading the NFC may not be successful as NFC chips in handsets are essentially designed to behave in card emulation mode rather than reader emulation mode, and it may be difficult for an untrained consumer to properly align the NFC antenna with the e-ID document antenna.

KYC

Know Your Customer is a set of regulations that have been developed to fight financial crime and money laundering. These regulations include provisions requiring to efficiently identify customers. Financial institutions are the best example of entities that have had to implement strict KYC procedures. Nowadays KYC in banks is typically performed in two different ways: person to person in a bank branch, or remotely with the customer connected through his/her smartphone.

In the case of KYC happening in a bank branch, the bank clerk performs an authentication of the consumer. To do this the person’s ID document is inserted in a half-page reader, that reads the MRZ and then uses the data to read the chip from the ID document. Different authentication methods may be used, according to regulations, to read the photo or to perform a stronger authentication using the customer fingerprint or iris image.

Consumer remote enrolment

> For applications that require very few ID document reads, smart phone apps that read the MRZ and the use the handset NFC to read the chip may be a solution. However, a professional reader will always bring more user-friendliness.
>
> Typically, a self-enrolling consumer for access to a service needs only to read once his/her own ID document. In this case, a mobile phone with a camera may be an appropriate tool to read the MRZ, and the NFC reader included in the phone could, under some circumstances, read the ePassport chip. However, a smart phone does not constitute a secure environment and substantial or high level of assurance can hardly be envisioned.

Conclusion

In many use cases, the best way to control an e-ID document and to ensure of its authenticity and to ensure the person presenting the document is its actual owner includes reading the MRZ with a half-page scanner and reading the document chip. There are very few contexts where reading the full page of an ID document makes practical sense. Half-page readers that include MRZ reading and contactless chip readers ensure application needs can be satisfied while providing a reliable, secure, small, versatile (can be desktop, portable or integrated in a kiosk), user-friendly and cost-efficient solution for a wide variety of use cases.

For all professional applications, dedicated readers bring the best adequation between application requirements and constraints such as dimensions in a constrained environment, portability, low electrical consumption, cost, ease of integration in kiosks, operation by unskilled personnel, maintenance, etc. In addition, half-page readers are able to read the MRZ and the chip in a single operator movement, bringing unparalleled user-friendliness.

Authentication methods

Smart card based ID documents can support different levels of authentication. These are specified by ICAO, ISO and EU standards, which have defined a series of security mechanisms that apply to ePassports as well as to other ID documents. It is essential to notice that all authentication methods are fully covered by half-page readers.

Passive Authentication (PA): the reader authenticates the ID document, ensuring the chip is authentic (i.e. issued by an authorized authority) and its contents have not been altered. ICAO mandatory

Active Authentication (AA): Prevents copying and cloning of documents. The reader and the document establish a challenge - response mechanism allowing the reader to verify that the chip has not been cloned. The ID document must contain a private key.

Basic Authentication Control (BAC): the passport is opened, the MRZ is read, and some of its data are used to access the ePassport chip thanks to the establishment of a secure communication channel. ICAO mandatory - EU mandatory

Supplemental Access Control (SAC) or **Password Authenticated Connection Establishment (PACE):** this protocol is an improved version of BAC, that uses stronger cryptography, which can be based on the MRZ or a PIN. Standards specify that BAC or SAC are mandatory to access the passport holder photo stored in the chip. ICAO optional - EU mandatory

Extended Access Control (EAC): uses both chip authentication and terminal authentication to ensure a terminal is allowed to read sensitive data from the document. EAC is mandatory to access biometric data of the passport holder, fingerprint and retinal scan. EU mandatory

Glossary

AA	Active Authentication	*Authentication using a challenge - response mechanism*
ABC	Automated Border Control	*Use of eGates to verify travelers' credentials and biometric data at a border post, often in an airport.*
BAC	Basic Access Control	*Authentication based on accessing certificates and signatures in the chip*
CSCA	Country Signing Certification Authority	*Government entity in each State issuing CSCA certificates that constitute the anchor in the trust chain.*
DSC	Document Signer Certificate	*Government-issued certificate that contains the information required to verify the digital signature on an ePassport.*
EAC	Extended Access Control	*Access control using cross authentication between the chip and the reader*
ICAO	International Civil Aviation Organization	*Main standardization force in the ID environment*
ISO	International Standards Organization	*World level standardization body*
KYC	Know Your Customer	*Set of regulations to fight financial crime and money laundering based on an authentication of each service customer*
MRZ	Machine Readable Zone	*Data printed on an ID document that can be read by a reader and that is necessary to unlock access to the chip*
NFC	Near-Field Communication	*Communication standard allowing to read a card or ePassport from a mobile device*
PA	Passive Authentication	*Authentication based on reading certificates and signatures from the document chip*
PACE	Password Authenticated Connection Establishment	*Authentication based on reading certificates and signatures from the document chip – Mandatory to access document holder's photo.*
SAC	Supplemental Access Control	*Authentication based on accessing certificates and signatures in the chip, with enhanced cryptography*
SIM	Subscriber Identity Module	*Smart card chip used for authentication in a mobile phone*