FRONTEX

LIBERTAS SECURITAS JUSTITIA

European Agency for the Management of Operational Cooperation at the External Bo
of the Member States of the European Union

Best Practice Guidelines on the Design, Deployment and Operation of Automated Border Crossing Systems

Warsaw, March 2011

Release 1.1
Status: APPROVED

Frontex Agency
Rondo ONZ 1
00-124 Warsaw
Poland
Tel.: + 48 22 544 9500
Fax: + 48 22 544 9501
Web: www.frontex.europa.eu
Enquiries: frontex@frontex.europa.eu

ACKNOWLEDGEMENTS

This report was prepared by the Research and Development Unit of Frontex in close collaboration with the following EU member states who, at the time of writing, are currently operating or testing an ABC system at different border crossing points (BCP) of the Schengen area:

Finland
France
Germany
Netherlands
Portugal
Spain
UK

Frontex is also grateful to the EU member states, industrial corporations and research centres who contributed to the review process.

TABLE OF CONTENTS

1. PURPOSE

This document presents a compendium of best practice guidelines on the design, deployment and operation of automated border crossing (ABC) systems. These have been elaborated in an effort to achieve at the different border crossing points:

- harmonization of practice,
- similar passenger experience
- consistent security levels

The intended audience are the different stakeholders in automated border checks, namely practitioners, technical bodies, and decision makers:

- current and prospective practitioners, i.e. border guards, will benefit from a wealth of practical information on what to do, and what to avoid too, in order to run an ABC system in an effective, efficient and user-friendly way;
- system architects and project managers from border authorities will find detailed technical information in order to specify and implement a fully compliant system that performs up to standards while staying away from previously known risks and dead-end streets;
- finally, decision makers at national and EU level will benefit from a better understanding on ABC systems, what they are, how they work, and more importantly how these help to manage the unavoidable security, facilitation and cost trade offs in border checks, thus allowing better informed decisions when it comes to allocating scarce human and financial resources.

2. COMMITMENT TO ACCURACY AND IMPARTIALITY

The Working Group (WG) responsible for the development of this document is committed to achieving due accuracy and impartiality. This commitment is fundamental to the trust of audiences.

The WG aims to achieve accuracy by:

- the accurate gathering of material using first hand sources wherever possible
- checking and cross checking the facts
- validating the authenticity of documentary evidence and digital material
- corroborating claims and allegations made by industry / border guards / users wherever possible

Impartiality lies at the heart of public service and must apply to all the contents of this document. The WG must be inclusive, considering the broad perspective of alternatives available, and ensuring the existence of a range of views is appropriately reflected.

The WG's commitment to impartiality means:

- we strive to reflect a wide range of opinion and explore a range of solutions
- no preference is given to vendor-specific solutions
- we must ensure we avoid bias or an imbalance of views
- we may provide professional judgments but may not express personal opinions on matters of public policy or political or industrial controversy

3. TERMINOLOGY

Although the recommendations and guidelines presented in this document are non-binding for MSs, the present terminology has been adopted in order to provide an unambiguous description of what should be observed in order to achieve a coherent approach with a common security baseline across Schengen borders.

SHALL	This word, or the terms "REQUIRED" or "MUST", mean that the definition is an absolute requirement.
SHALL NOT	This phrase, or the phrase "MUST NOT", mean that the definition is an absolute prohibition.
SHOULD	This word, or the adjective "RECOMMENDED", mean that there may exist valid reasons in particular circumstances to ignore a particular aspect, but the full implications must be understood and carefully weighed before choosing a different course.
SHOULD NOT	This phrase, or the phrase "NOT RECOMMENDED" mean that there may exist valid reasons in particular circumstances when the particular behaviour is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behaviour described with this label.
MAY	This word, or the adjective "OPTIONAL", mean that an item or feature is truly optional. A vendor may choose to include the option because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item or feature. An implementation which does not include a particular option MUST be prepared to interoperate with another implementation which does include the option, though perhaps with reduced functionality. In the same sense an implementation which does include a particular option MUST be prepared to interoperate with another implementation which does not include the option.

4. ACRONYMS AND ABBREVIATIONS

AA	Active Authentication
ABC	Automated Border Crossing/Control
B900	IR sensitive ink
BAC	Basic Access Control
BCP	Border Crossing Point
BMP	Image format Windows Bitmap v3
BPG	Best Practice Guidelines
CA	Chip Authentication
CCD	Charge Coupled Device (Image sensor based on the principle of)
CRL	Certificate Revocation List
CSCA	Country Signing Certification Authority
DG1	Data Group 1 of the ePassport chip (machine readable zone data)
DG2	Data Group 2 of the ePassport chip (encoded face data)
DG3	Data Group 3 of the ePassport chip (encoded finger(s) data)
DG14	Data Group 14 of the ePassport chip (chip authentication public key data)
DG15	Data Group 15 of the ePassport chip (active authentication public key data)
DS	Document Signer
EAC	Extended Access Control
EF.COM	Common Data Object of the ePassport chip (version information and tag list)
EF.SOD	Document Security Object of the ePassport chip (data integrity and authenticity information)
EMC	Electromagnetic compatibility
eMRTD	Electronic MRTD
EU	European Union
FAR	False accept rate
FoM	Figure of Merit
FRR	False reject rate
HW	Hardware
ICAO	International Civil Aviation Organization
IR	Infrared light
ISO	International Organization for Standardization
JPEG	Joint Photographic Experts Group
JPG	JPEG compression format for images
JPG2000	JPEG 2000 compression format for images
MRTD	Machine Readable Travel Document
MRZ	Machine Readable Zone
MS	Member State of the Schengen Agreement
NVC	Non Verbal Communication
PA	Passive Authentication
PAX	Passenger
PC	Personal Computer
PC/SC	Personal Computer / Smart Card (specification for smart-card integration into computing environments)
PKI	Public Key Infrastructure

PPI	Pixels per Inch
RF	Radio Frequency
SDK	Software Development Kit
SW	Software
TA	Terminal Authentication
TCN	Third Country National(s)
UV-A	Ultraviolet light A (400 nm–315 nm wavelength)
VIZ	Visual Inspection Zone
WG	Working Group

5. INTRODUCTION

5.1. Background

Despite the economic downturn the world is still suffering, air transport business still forecasts a steady growth for the upcoming decade. As passenger numbers continue to rise while the number of international airports remains constant, the pressure to process large volumes of people as quickly and securely as possible grows.

But this increased throughput at international air border crossing points cannot come at the cost of additional hassle for passengers or reduced security. New approaches are thus needed to make air travel an enjoyable experience for the law-abiding majority while keeping borders effectively closed for the unlawful individuals.

ABC systems at border crossing points allow passengers holding electronic passports to pass smoothly through airport electronic gates, leaving border security personnel to concentrate on second-line controls, managing of possible rejections, and manual screening of ineligible travellers. The result is less frustration for passengers, reduced pressure on both airline and airport resources, and increased consistency and security of the identity verification. When used in conjunction with other forms of risk management such as biographical data screening, ABC systems also provide a powerful defence against threats of terrorism, smuggling, illegal immigration, and other criminal activities that make use of forged documents and stolen identities.

Understanding how to strike the right balance between passenger facilitation and security is a crucial aspect. In the Schengen Borders Code it is stated that EU nationals should undergo minimal checks, and the main reason for this is to allow these low risk passengers to have a fast track into the member states of the Schengen agreement. The introduction of automated border checks must honour this principle, thus the first priority of any ABC should be passenger facilitation. Security is to be understood as a boundary condition that must be met (i.e. keeping a harmonized security threshold along Schengen border crossing points) rather than an objective to be maximized at the cost of reduced facilitation.

5.2. History

The traditional solution of border guard officers manually processing travel documents and passengers has been working effectively for as long as international travel has existed, but this approach is not free of problems. In a matter of few seconds, border guards have the responsibility to verify that: a) the traveller standing in front of the officer is carrying a valid travel document, b) he/she is the person that the travel document claims to be, c) this person is eligible to enter the country, and lastly d) this person does not pose a threat to its citizens or institutions. With the improvement of technology applied to forging documents, the uses of aliases and look-alikes, or the time pressure associated to border control processing, among others, it is not surprising that the traditional manual approach is now under revision.

After some trials in different countries, automated border crossing (ABC) systems have proved to be a promising way to meet increasing throughput at border crossing points while maintaining the necessary levels of security. Virtually all these systems rely on some form of biometrics in order to verify the identity of the travellers. Biometric technology uses a person's unique physiological characteristics – for example, the face, iris, retina, fingerprints, hand geometry, voice or handwriting – to verify his or her identity - in short, to confirm that someone is precisely who they claim to be. Computer technology is used to authenticate identity by matching the characteristics of individuals in real time against previously stored records. ICAO (International Civil Aviation Association) recommends facial recognition as the 'globally interoperable biometric technology for machine-assisted identity confirmation', while acknowledging that some authorities may supplement this with fingerprint and iris recognition. Electronic passports (ePassports) contain passenger data (including the biometric markers) inside an embedded chip. This chip has been designed with different data protection mechanisms in place to ensure that only authorized parties can access the information contained inside. First generation e-passports contain the facial image of the holder; second generation (obligatory in the EU since June 2009) contain also 2 fingerprints.

A number of ABC systems have been developed by the industry, according to requirements established by national border authorities, which are intended to provide more efficient and reliable border crossing operations by means of automation of routine tasks. Although no two ABC systems are equal by design, they can be defined as the use of automatic or semi-automatic systems that without the need for human intervention can verify both the authenticity of the travel document used by travellers, the identity of travellers, and their authorization to cross the border at a border crossing point.

5.3. Scope of This Study

The scope of this study is aligned with the EC and ICAO recommendations at the time of writing on the use of biometric passports for automated border checks without enrolment.

Travel documents considered

ABC systems can be divided into two types: (a) systems without enrolment based on the use of an electronic travel document and (b) systems based on pre-enrolment which generally take the shape of Registered Traveller Programmes. The European Union encourages member states to deploy ABC systems without pre-enrolment for EU citizens carrying ICAO compliant electronic passports.

This document focuses on ABC systems based on 1st and 2nd generation ePassports. There are no specific provisions in this document for combined or stand alone use of ABC systems serving Registered Traveller Programmes.

Biometric markers used

Most ABC systems currently in use support facial recognition as the main biometric authentication method, even though there is a large base of 2nd generation ePassports carrying both facial and fingerprint data.

Unfortunately, for fingerprint recognition in conjunction with the use of ePassports there are not -at the time of writing- significant experiences, thus fingerprint recognition is not explicitly covered in the present version of this document. The use of fingerprints for identity verification in ePassport-based automated border checks will be addressed in future versions of this document as more relevant experience is gained.

5.4. About Best Practices and Guidelines

A best practice is a technique, method, process, activity, incentive, or reward which conventional wisdom regards as more effective at delivering a particular outcome than any other technique, method, process, etc. when applied to a particular condition or circumstance. The rationale behind this is that with proper processes, checks, and testing, a desired outcome can be delivered with fewer problems and unforeseen complications. A given best practice may only applicable to particular condition or circumstance and will typically need to be modified or adapted for similar but different circumstances.

A guideline, on the other hand, is any document that aims to streamline particular processes according to a set routine. By definition, following a guideline is never mandatory (protocol would be a better term for a mandatory procedure). Guidelines may be issued by and used by any organization (governmental or private) to make the actions of its employees or divisions more predictable, and presumably of higher quality.

Too often it is not easy to draw the line between Best Practices and Guidelines, and many times they are used together. Thus the term Best Practice Guidelines has been widely adopted in the industry to reflect that knowledge, typically based on experience, which can be shared in order to achieve improved results towards specific objectives. Along the present document, the term Best Practice Guidelines (BPG) will be used.

5.5. How to Read this Document

The present document is structured in 3 main areas, technology of an ABC system, operation of an ABC system, and passenger experience.

The technology area provides detailed insight on the functioning and requirements for the:

- Authentication of travel documents
- Biometric identity verification in ABC system
- Quality control aspects of ABC systems

The operational area proposes best practice guidelines and recommendations on:

- The deployment of an ABC system

- The roles and tasks of border guards
- How to handle most common exceptions

Lastly, the passenger experience area proposes best practice guidelines and recommendations on:

- How to create awareness among passengers about an ABC system and educate them on its proper use
- How to run an excellent user friendly service and help achieve a satisfactory travel experience

The document is also complemented with a series of annexes with additional reference material and a discussion on systems design aspects.

5.6. Methodology

The methodology used by the WG to develop the BPG in this document was based on the following tasks:

- State the problem and goals
- Elaborate the list of relevant topics to be covered
- Structure work into study groups (Technical, Operational, Passenger Experience)
- Carry out research on current practice based on questionnaires, interviews and technical meetings
- Analyse results and extract individual best practices
- Debate and agree on proposed best practices
- Build the present document
- Internal and external review of the document
- Approval

5.7. Review and Updates

This document is intended to be a living one, subject to regular updates in an attempt to gather state of the art technologies and best current practices regarding ABC systems.

Due to lack of experience and time constraints, a number of topics have not been covered in detail in this version of the document. This, however, will be solved in subsequent releases. At the time of writing, the following topics have been identified as the most relevant ones to be included in the next version:

- The usage of ABC systems by third country nationals
- Analysis of the different topologies
- The use of alternative biometric markers (fingerprints) and multi modal biometrics in general
- The usage of ABC systems by handicapped people and minors
- Ensuring data privacy and protection
- Change management within the border management authority

5.8. About Frontex and ABC Systems

Frontex Research and Development Unit actively follows the development and implementation of ABC systems in Europe. Apart from organizing workshops and demonstrations where EU member states can share experiences, it has fostered the creation of common technical and operational best practice guidelines working group, one of whose main results is the present document.

6. OVERVIEW OF AN ABC SYSTEM

6.1. Benefits of automating border checks

Bearing in mind that automated border checks are currently targeted to EU citizens (for which only minimal checks are required as per the Schengen Borders Code), the primary goal of ABC systems MUST be facilitation without disregarding security. Facilitation is thus the main objective to maximize, and security a boundary condition that has to be met. This situation may change in the future if it is decided to open the use of ABC systems to third country nationals (TCN) carrying electronic travel documents and/or electronic Visas. Since TCNs may pose a different risk than EU citizens, the trade-off between security and facilitation is likely to be a different one.

Automating the most time consuming tasks will give border guards more time for processing third country nationals and carry out more thorough checks. At the same time, increased facilitation will allow for an overall better travel experience.

Cost-effectiveness is also an important dimension to be observed. Properly set ABC systems allow for an increased number of passengers checked at first line control while using a lower number of border guards. The technologies involved are likely to improve in the future, thus yielding better performance; additionally, it can be expected that prices will go down when ABC lines will become more widespread.

ABC is a supporting technique in the operation of the border management processes, meaning that the responsibility is still in the hand of the border officers. When properly trained and motivated, border officers operating an ABC system can be more effective than manual checks alone. Improvements in quality can also be expected and should be looked after.

It is important to note however, that for every task in the border checks process that is modified by the introduction of the ABC, a proper risk assessment must be carried out in order to understand how the automation has impacted on existing risks or created new ones, and thus react accordingly.

Of course, nothing prevents from using automated border checks at BCPs other than airports. ABC systems can also be equally effective and beneficial at land and sea BCPs.

6.2. Main Functions of an ABC System

In short, and ABC system performs the following tasks (the same ones as in the classical passport control booth) with a high degree of automation:

1. Check that the traveller trying to cross the border is carrying a genuine and valid travel document. This is more formally referred to as the “Document authentication process”.
2. Verify biometrically that this travel document really belongs to the traveller trying to cross the border. This is more formally referred to as the “Biometric identity verification process”.

3. Check that the traveller is really entitled/authorized to cross the border. This is normally carried out by cross checking against watchlists and other databases.
4. Grant/deny pass according to pre-established logic, sometimes needing the intervention of the supervising officer.
5. Guarantee security in the overall process, meaning that only the cleared traveller is allowed to cross the border (i.e. no tailgating), and that rejected ones are properly handled (i.e. trapped to prevent escaping until attended by an officer). This is typically achieved by the usage of single or double automatic barriers and tailgating detection/prevention mechanisms.

For the purpose of this document, these are the basic functions that any ABC system must provide. Other complementary or more advanced functions are also possible (e.g. automated profiling, Entry/Exit update), but are out of the scope of this document.

From a systems perspective, the basic process of going through and ABC system proceeds as follows:

- The automated border crossing process starts with passport scanning. The traveller inserts the data page of the passport into the passport reader. The reader checks optical security features, reads the optical Machine Readable Zone (MRZ) and communicates with the chip in the passport to read the data and to verify the authenticity of the document.
- A facial image of the traveller obtained at the border is then compared with the one stored on the chip. National (police records) and international registers (e.g. lost & stolen documents, SIS, VIS) are also checked in the same way and under the same criteria as in the classical border control booth.
- If the matching is successful, access is typically granted[1] and the traveller crosses the border. If the matching fails, the traveller is referred to a manual control booth. Human overseeing is typically provided by a border guard officer, who supervises the whole process, including the matching of the facial images.

6.3. 1 step and 2 Step Topologies

A frequent traveller will soon realize that no two ABC systems are equal, despite serving the same purpose and performing the same tasks. This is so because the design requirements, environment and alternatives available at the time decisions were made can be quite different from one BCP to another.

Probably the main difference that a user is likely to perceive from one implementation to another is that in some systems all the tasks are carried out in a single batch (a.k.a. single step process), while in some others the tasks in the process are split into two batches (a.k.a. two steps process). The reasons for deciding between the single step and two steps process are security, cost and efficiency.

[1] The ABC is part of the filter, if a person succesfully passes the ABC system, his/her acces can still be denied by the border officers.

The single step process is conceptually simple, and needs no further clarifications; everything takes place in a single uninterrupted transaction. In the two steps process, the clearance process takes place at a kiosk, and upon successful clearance a token (physical or biometric) is given to the traveller. The traveller then proceeds to the gate where he/she will use the token to cross the border. Note that the kiosk may be co-located with the gate (two steps process in a single service point), or at a different location (two steps process with two service points).

The two steps process builds on the principle that the most time consuming tasks (the document authentication and biometric verification) can be executed at a separate infrastructure (the kiosk) which is generally cheaper to acquire and more compact in size than the physical gates. Thus, it may be the case in some implementations, that for a given fixed budget it is more cost effective (throughput vs life cycle cost of infrastructure) to have a two steps process than a single step one. The decision whether to opt for a single or two steps process is not straightforward, as other relevant aspects like security, floor space availability, environment restrictions and passenger education are often equally relevant.

Each topology option depicted above has its own strengths and weaknesses. This topic is still under debate at the time of writing, as preliminary results on the different topologies are not yet conclusive. Hence, they will not be addressed in the current version of this document. In a future version, a more in depth discussion on each alternative will be provided.

6.4. Other Design Variations on ABC Systems

In addition to the different topology options, there are also a number of design variations among the different implementations. Here we will present just a few of the most relevant ones.

Alternative MRTDs

Although all ABC implementations are required to accept ePassports, some also accept alternative eMRTD. The most frequent case is electronic national ID cards carrying biometric information, which normally is facial and/or fingerprint.

Single gate vs Mantrap solutions

One of the most obvious functions of the gate is to prevent unauthorized persons to cross it. For this purpose physical barriers are used, like automatic doors. All ABC gates use at least one physical barrier (the one that opens once the passenger has been granted access to cross), and some also include an additional one in order to enter the gate. This second barrier forms a mantrap, preventing the user from leaving the gate by going backwards once in it. This is installed normally for security reasons, e.g. to prevent the user from escaping if there is hit against a watch list or the document is recognized as stolen or forged.

Registered Traveller Programs

Some ABC systems operate in coordination with a registered traveller program, where third country nationals may be entitled to use the system if they have been

previously enrolled. Enrolment usually takes place after a background check has been performed and the frequent traveller is identified as low risk (sometimes a biometric document is issued and a fee is paid to cover issuance and service costs).

7. THE DOCUMENT AUTHENTICATION PROCESS

Document authentication is the process by which the electronically machine-readable travel document (eMRTD) -the ePassport for the purposes of this document- presented by the passenger is checked in order to determine whether it is a genuine one in good order or not.

In order to check the authenticity of an eMRTD by an ABC system, a document reader is required as a hardware subcomponent. The associated document authentication process (typically realized in software) is considered to be composed of three separate steps:

1. Optical document checks
2. Accessing and reading ePassport data
3. Verification of ePassport data

Requirements and best practices regarding the document reader and the document authentication process are detailed in this chapter.

7.1. Requirements on the document reader

ABC systems SHALL use a full page document reader that provides at least the key technical specifications and capabilities detailed below.

Technical requirements

The document reader SHOULD be designed in a way that it can be used effectively in self-service environments. This includes easy usage for right as well as left handed people, and easy handling of ePassports with flexible biographical data pages. Note that flexible biographical data pages in ePassports might cause difficulties because in practice the biographical data page may get folded when placed on the document reader, which must be avoided in order to properly read it.

ePassports SHOULD be placed on the document reader in lengthwise orientation, i.e. biographical data page facing down, MRZ-side first towards the document reader.

The document reader SHALL have an integrated RF module according to [ISO14443] Type A and Type B that is accessible via a PC/SC interface. The transfer rate of the RF module SHOULD be as high as possible (at least 424 Kbit/s).

The document reader SHALL have a dedicated wired connection as physical interface to a host system (e.g. PC) with a state-of-the-art transfer rate (e.g. USB 2.0, 480 Mbit/s). It is RECOMMENDED to operate the document reader with a power supply independent from the physical interface to the host system.

The document reader SHALL be able to capture images at IR, UV-A and visible light. The optical resolution SHALL be at least 385 PPI.

The document reader SHOULD have a proper shielding against interfering of external light.

The document reader MUST comply with existing regulations regarding EMC and UV-A light emission.

Capability requirements

ABC systems SHOULD use a document reader that is future-proof. Therefore, the document reader SHOULD support all ICAO compliant eMRTDs, including form factors of ID1, ID2 and ID3[2].

The document reader MUST have a state-of-the-art operating speed. In average, optical images of the biographical data page SHOULD be captured within 2 seconds, and reading of the electronic data (at least EF.COM, EF.SOD, DG1 and DG2) from a typical 1st generation ePassport SHOULD NOT take more than 8 seconds.

7.2. Performing Optical Checks on the ePassport

ABC systems SHALL perform a verification of the optical security features of the eMRTD as explained below.

Mandatory optical checks

The following are mandatory optical checks to be carried out on the eMRTD:

MRZ consistency
ABC systems SHALL verify that the optical extracted MRZ is consistent, using the MRZ checksum digits.

B900 ink
ABC systems SHALL verify that the MRZ is completely visible in the IR image of the biographical data page.

UV-A brightness
ABC systems SHALL verify that no bright paper or remains of glue are visible in the UV-A image of the biographical data page.

Optional optical checks

The following are optional optical checks to be carried out on the eMRTD:

MRZ vs. VIZ
ABC systems MAY compare information taken from the MRZ (e.g. name, nationality or gender) with data that was extracted from the visual inspection zone (VIZ).

[2] There are some ID3-compliant passports which feature a protective cover slightly larger than ID3, which SHOULD also be supported by the document reader.

Pattern checks
It is RECOMMENDED that ABC systems verify optical security patterns (UV, IR, visible) using a database for pattern checks. This verification MAY also be used to identify the type of document. In these cases, it is RECOMMENDED to use a dedicated database for the ABC scenario which consists of reliable patterns for the targeted user group only. The patterns database MUST be updated on a regular basis; otherwise the FRR will increase significantly.

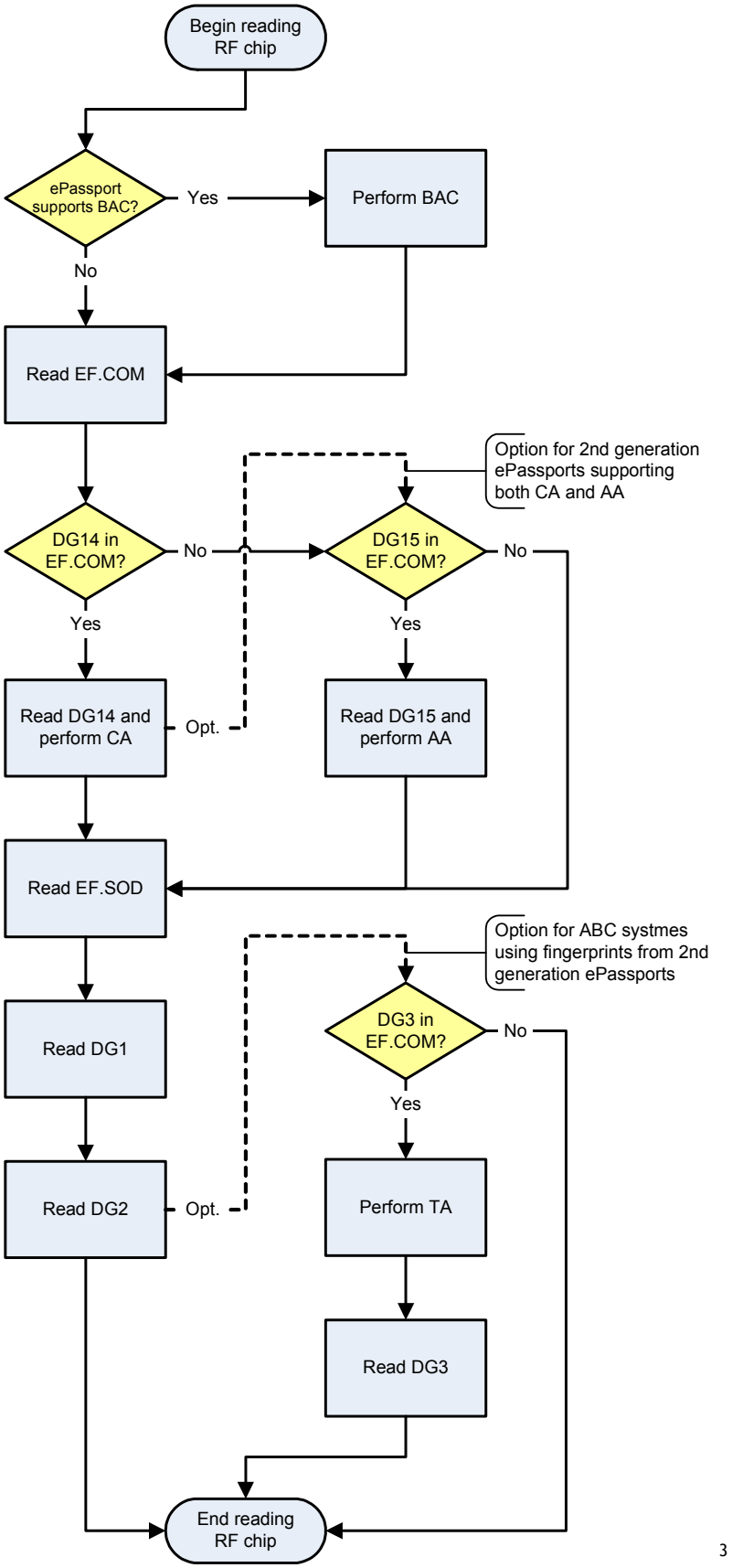
It is further RECOMMENDED to use a pattern database which allows for maintenance and support by the operating agency itself, or under supervision and contract of the operating agency by a trusted third-party provider. The usage of a pattern database that does not allow for modifications of the database content by the operating agency (black-box database) is NOT RECOMMENDED.

7.3. Accessing and reading ePassport data

ABC systems MUST at least support reading and decoding of the following files/datagroups from ePassports: EF.COM, EF.SOD, DG1, DG2, DG14 and DG15.

ABC systems MUST at least support the security protocols BAC, AA and CA. During the reading process, AA or CA MUST be performed if supported by the particular ePassport. For ePassports that support both CA and AA, only CA is REQUIRED. In such a case AA MAY be performed additionally after CA.

ABC systems MUST implement the general high-level sequence for the RF chip reading process as shown in Figure 1.



[3]

Figure 1: High-level sequence for RF chip reading

[3] Note that although all EU/Schengen passports are currently required to include BAC, there is at least one valid EU passport without BAC support, hence the branch in the diagram

7.4. Verification of ePassport data

After the chip reading process, ABC systems MUST verify the data that was read from the ePassport chip. This ePassport data verification process is mainly covered by the Passive Authentication (PA) security method defined by [ICAO9303].

The reliability of the PA security method is only assured, if trustworthy certificates (DS certificates and CSCA certificates) are applied to the verification process. If it cannot be verified that the DS certificate originates from a trusted source or has been issued by an official and trusted CSCA, the result of the entire ePassport data verification process can not be trusted and rendered useless. Therefore, the ABC system MUST be provided with certificates from a trusted certificate store.

It is RECOMMENDED to implement this trusted certificate store as a centralized system. In this case, the integrity and authenticity of the certificate store (which is absolutely crucial for the reliability of the entire ePassport data verification process) MUST be assured "only once" on the central side and efforts for assuring the integrity and authenticity locally on each client ABC system can be saved. As an add-on when implementing a centralized trusted certificate store, the sub-steps 2, 3 and 4 of the PA procedure (see below) MAY be implemented as a centralized service as well. Note that details about the technical implementation of the trusted certificate store (e.g. central LDAP directory, local signed file, etc.) as well as the mechanisms used to safeguard the trust relationship between the certificate store and the ABC system (e.g. by a secure communication channel) are outside the scope of this document.

The PA procedure consists of the following sub-steps, which MUST be supported by the ABC system:

1. EF.SOD verification
2. DS certificate signature verification
3. Certificate validity period check
4. DS Certificate revocation status
5. Comparison between EF.SOD and EF.COM
6. Datagroup integrity check

In addition to the PA procedure, the following sub-steps MUST be performed by the ABC system in order to complete the ePassport data verification process:

7. Comparison of optical and electronic biographical data (DG1 vs. MRZ)
8. Issuing country comparison (DG1 vs. DS certificate)

The overall result of the ePassport data verification process MUST NOT be considered as "Passed" or "Successful" by the ABC system if one or more of the particular sub-steps 1. – 8. (see details below) end up with the result "Failed".

1. EF.SOD verification

The structure of EF.SOD is defined by [ICAO9303] as a SignedData structure conforming to [RFC3369] and ABC systems MUST verify its signature. To perform this signature verification procedure a DS certificate corresponding to the particular EF.SOD is required. [ICAO9303] defines that the DS certificate MAY be included in EF.SOD. In practice, most countries are issuing ePassports which contain the corresponding DS certificate. Thus, ABC systems MUST be able to process EF.SOD files with zero or more DS certificates. Additionally, ABC systems SHOULD be able to obtain a DS certificate from an external source if the particular EF.SOD does not contain the proper DS certificate.

If the verification of the EF.SOD signature is successful, the result of this sub-step MUST be considered as "Passed" by the ABC system. If the verification of the EF.SOD signature is not successful or could not be completely performed (e.g. due to a missing DS certificate), the result of this sub-step MUST be considered as "Failed".

2. DS certificate signature verification

Verification of the certificate chain up to a known trusted certificate is an essential step in the overall process. In many demonstrations that claim to have faked an official ePassport, a new EF.SOD has been created and signed with a new key after a datagroup was modified or exchanged. If it is not verified that the DS certificate originates from a trusted source or has been issued by an official and trusted CSCA, the results of all other security checks become worthless.

Therefore, the following requirements SHALL apply to ABC systems:

- If the signature of EF.SOD has been verified with a DS certificate that has been taken from EF.SOD or from an untrusted external source (like an unauthenticated database), ABC systems MUST verify the signature of the DS certificate as well. This requires an appropriate CSCA certificate that originates from a trusted source.
- If the DS certificate originates from a trusted source (explicitly not from EF.SOD), ABC systems MAY skip the verification of the DS certificate signature.
- Beside from very few exceptions it is common that the DS certificate used to verify the signature of EF.SOD is contained in EF.SOD itself. Therefore, it is common practice to use this certificate for verification and to verify it's authenticity with the corresponding CSCA certificate. In order to do so, ABC systems have to search the proper CSCA certificate out of a larger set of certificates provided by the trusted certificate store. It is RECOMMENDED that ABC systems extract the AuthorityKeyIdentifier extension from the DS certificate and search for a CSCA certificate with the corresponding value in its SubjectKeyIdentifier extension. Although the usage of these extensions is specified as mandatory by [ICAO9303], there are some countries which have issued ePassports without them. Thus, it is RECOMMENDED that in the case that no matching CSCA certificate can be found by comparing key identifiers, ABC systems SHOULD perform only a subject based search for CSCA certificates using the issuer information from the DS certificate.

- If one or more suitable CSCA certificates have been found using the search criteria described above, the DS certificate signature verification result MUST be considered as “Successful”, if the signature of the DS certificate can be verified with one of these CSCA certificates and the particular CSCA certificate subject is equal to the DS certificate issuer. If none of the found CSCA certificates achieves these two requirements, the DS certificate signature verification sub-step MUST be considered as “Failed”.
- It is RECOMMENDED that the signature of the CSCA certificate is not verified, because some countries issue CSCA certificates that are not self-signed or it might be unavoidable to use CSCA link certificates for the DS certificate signature verification. Since all CSCA certificates that are used by the ABC system MUST originate from a trusted source this is not seen as a security flaw.

3. Certificate validity period check

ABC systems SHALL verify that the current time is within the validity period of the DS certificate. Additionally, ABC systems SHOULD also check if the current time is between the start and end of validity period of the CSCA certificate. It is RECOMMENDED to set up appropriate mechanisms to ensure that the current time is valid.

If the performed validity period checks are successful, the result of this sub-step MUST be considered as “Passed” by the ABC system. If the performed validity period checks fail, the result of this sub-step MUST be considered as “Failed”.

4. DS certificate revocation status

Generally, checking the DS certificate revocation status is a mandatory sub-step of the PA procedure. Given the present practice regarding the official distribution of certificate revocation information, it is very difficult to check the DS certificate revocation status for a broad range of ePassport issuing countries. Therefore, ABC systems SHOULD check the DS certificate revocation status if the corresponding revocation information (e.g. CRL) is available.

If the DS certificate revocation status could be checked as “Not revoked” based on trusted according certificate revocation information, the result of this sub-step MUST be considered as “Passed” by the ABC system. If the DS certificate revocation check results in “Revoked” based on trusted according certificate revocation information, the result of this sub-step MUST be considered as “Failed”.

5. Comparison between EF.SOD and EF.COM

Because EF.SOD does not contain a digest (hash-value) of EF.COM, a modification of EF.COM can not be detected by just verifying the signature of the EF.SOD. Thus, ABC systems SHALL compare the content of EF.COM with EF.SOD to make sure that each DG listed in EF.SOD is also contained in EF.COM and vice versa. If a mismatch between EF.COM and EF.SOD is detected, the result of this sub-step MUST be considered as “Failed” by the ABC system. If EF.COM and EF.SOD correspond to each other, the result of this sub-step MUST be considered as “Successful”.

6. Datagroup integrity check

For each datagroup that was read from the ePassport chip, ABC systems MUST calculate the datagroup's digest (hash-value) and compare it with the corresponding digest contained in EF.SOD. ABC systems SHALL rely on the content of a datagroup for further processing (e.g. biometric verification) only if the digests are equal. In case the ePassport chip supports AA and/or CA, the ABC system MUST also verify the digest of the corresponding datagroup (DG14 in case of CA and DG15 in case of AA).

If all of the performed datagroup integrity checks are successful, the result of this sub-step MUST be considered as "Passed" by the ABC system. If one or more integrity checks fail, the result of this sub-step MUST be considered as "Failed".

7. Comparison of optical and electronic biographical data (DG1 vs. MRZ)

If the overall border control process includes background checks, the information to perform these queries is typically taken from the optically scanned MRZ, which is usually the first information available.
If an ePassport enforces to perform the BAC protocol, some parts of the MRZ are implicitly verified against OCR errors if the protocol execution was successful. Nevertheless, it is possible for an attacker to falsify other parts of the MRZ that are not used for BAC (e.g. surname and/or given names). To prevent this attack, ABC systems MUST verify the whole content of the optical MRZ against DG1.

If the verification of the optical MRZ against DG1 is successful, the result of this sub-step MUST be considered as "Passed" by the ABC system. If the verification of the optical MRZ against DG1 fails, the result of this sub-step MUST be considered as "Failed".

8. Issuing country comparison (DG1 vs. DS certificate)

Another possible way for an attacker to falsify an ePassport is that he has managed to sign his manipulated data by a DS of a foreign country. By doing so, he could for example try to bypass visa regulations by appearing under a false nationality.

Thus, ABC systems SHOULD extract the country attribute from the issuer name in the DS certificate and compare it to the issuing country information stored in DG1. This check can only be performed if the following preconditions are fulfilled:

- A mapping table with a distinct mapping between ICAO 3-letter country codes and ISO 2-letter country codes MUST be defined. Note: This is not necessarily a distinct mapping for each particular country (e.g. an ISO 2-letter country code may map to multiple ICAO 3-letter country codes).
- The issuer name of the particular DS certificate contains a country attribute with a properly encoded ISO 2-letter country code.

It is RECOMMENDED to implement this sub-step as follows:

1. Extract the ICAO 3-letter country code from DG1 (called CountryICAO)
2. Extract the ISO 2-letter country code from the DS certificate (called CountryISO)
3. Compare CountryICAO against CountryISO based on the defined mapping table.

If CountryICAO and CountryISO correspond to each other according to the mapping table, the result of this sub-step MUST be considered as "Successful" by the ABC system. If CountryICAO and CountryISO do not correspond to each other according to the mapping table, the result of this sub-step MUST be considered as "Failed".

7.5. Design of the Document Authentication Process

There are several interdependencies amongst the separate steps of the document authentication process (optical checks, reading RF data and ePassport data verification). Generally, each step or sub-step of the document authentication process SHOULD be started as soon as the required input data (e.g. optical MRZ, particular datagroup, etc.) is available. Performing the process steps concurrently (running several tasks in parallel) as much as possible, allows for a minimization of the time period required for the entire document authentication process.

A high-level illustration of the RECOMMENDED document authentication process for ABC system is shown in Figure 2.

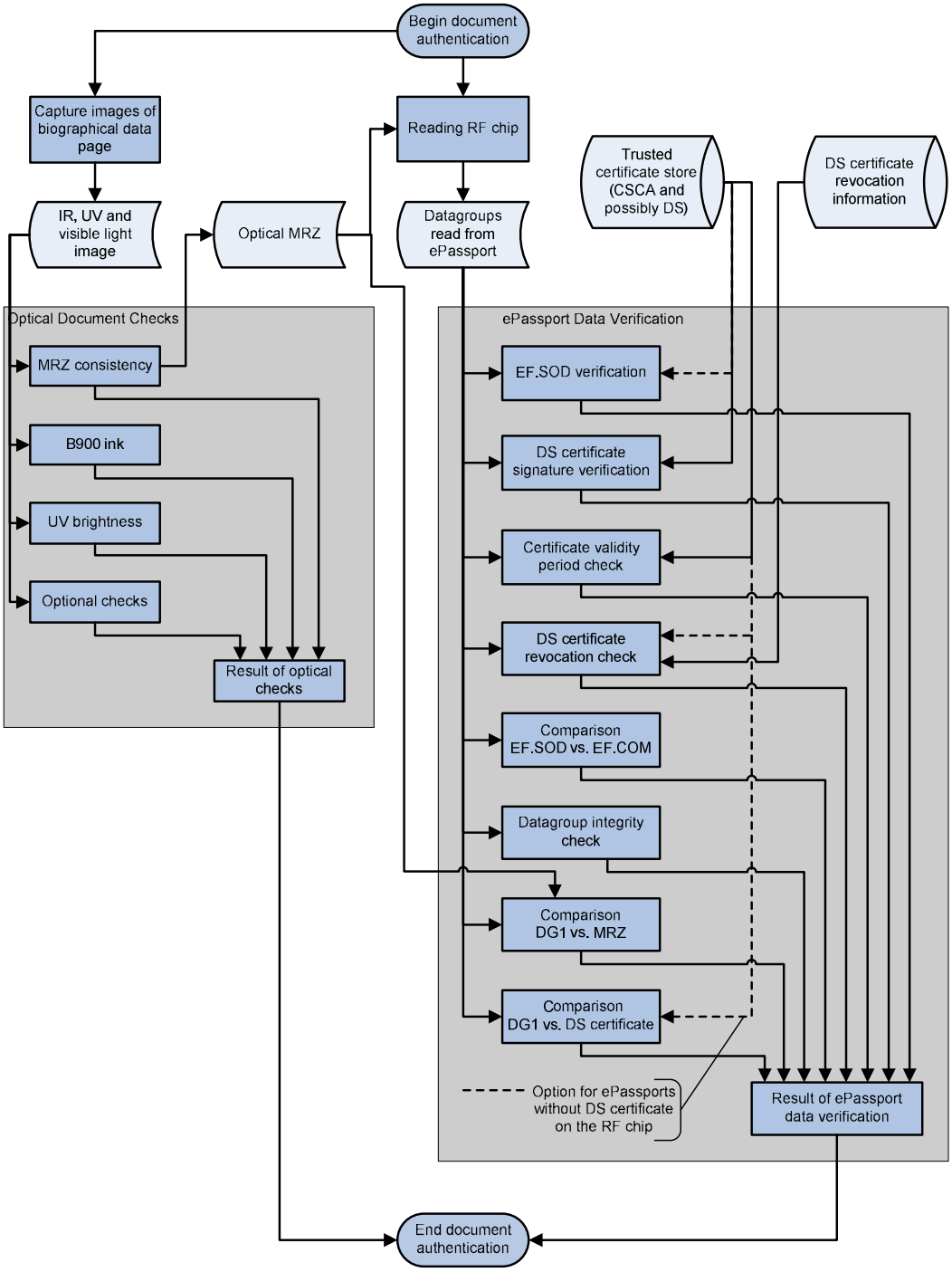


Figure 2: Document authentication process

8. THE BIOMETRIC VERIFICATION PROCESS

Biometric verification is the process by which it is verified using biometric technology that the person holding the eMRTD is actually the owner of the eMRTD.

Self-service ABC systems based on ICAO compliant eMRTDs SHALL follow the recommendations of [ICAO9303] and SHALL use face recognition technology as the main biometric marker for identity verification of passengers. They MAY support fingerprint or other biometric markers in compliance with [ICAO9303] at present or in the future.

The biometric verification process is considered to be composed of two separate steps:

1. Face capture sub-process, carried out by face capture unit
2. Face verification sub-process, carried out by face verification unit

Requirements and best practices regarding the units and sub-processes are detailed in this chapter.

8.1. Face Capture Unit

Architecture and setup

The face capture unit SHOULD be in the flow of the passenger (a straight-line for the passenger to walk and look in the camera). It is NOT RECOMMENDED that camera and the flow of the passenger form an angle greater than 45°, as this is likely to slow down flow.

The cameras within the face capture unit (one or more cameras per capture unit) SHALL have a resolution of at least 2 Megapixel. It is RECOMMENDED to use CCD cameras (or technologies that provide a comparable image characteristic). The depth of field depends on the setup (mantrap, single gate or kiosk); it MUST be adjusted to the area where the passengers face is located in the regular use case. A frame rate of at least 10 frames per second is RECOMMENDED.

The unit SHOULD contain lighting modules to ensure a proper illumination of the face region. The lighting SHALL NOT cause reflexions on glasses or the skin of the face. The lighting SHALL be switched on during the complete capture process and brightness MAY be varied to get best contrast and illumination. It MAY be a permanent light source or it MAY be switched off in times where no face images are captured. Sunlight will vary both on a daily and on a seasonal basis. It is RECOMMENDED to test that the system will perform adequately under different sunlight conditions. It is RECOMMENDED that direct sunlight is avoided, and environmental illumination be controlled for best capture results.

The unit SHALL be able to capture frontal images of persons in a height of at least between 140 and 200 cm. For instance, most of the deployed solutions make use of a moving camera, a single wide angle camera, or several cameras at different heights.

The unit MAY automatically adjust in order to capture proper images for the biometric comparison. The time period required for this adjustment (e.g. height adjustment by movement of the camera) SHOULD be minimized in order to avoid needless delays within the face capture process.

The face capture unit SHOULD give feedback to the passenger by an integrated display. It is RECOMMENDED to show the live stream that is currently captured (digital mirror) and to give an indication if the image is good to be used by the face verification unit. If the feedback is realised as a digital mirror on a display, the display MUST move with the camera (if a movable camera unit is used). The feedback SHOULD NOT interfere with the face capture process.

The capture unit MAY be connected directly to the PC that controls the complete ABC process or indirectly via a pre-processing unit. To connect the capture unit to the control PC standard state of the art interfaces (e.g. USB2.0, Ethernet, FireWire) SHALL be used.

It is RECOMMENDED to use standard interfaces according to BioAPI [ISO19784-1] for the capturing of the biometric data. The agency operating the ABC gates MAY decide to allow proprietary vendor-specific SDK interfaces for the integration of the capture unit.

Functionality

The face capture unit MUST provide facial images to the face verification unit.

The term “pre-processing”, which is used in the following, means the provision of a face image from a frame, whereas “quality assessment” means the provision of an appropriate face image from a set of face images.

It is RECOMMENDED to provide pre-processed and quality-assessed images to the verification unit. The pre-processing SHOULD cover at least

- detecting the face in a frame,
- cropping the face from the frame,
- de-rotating the face to ensure that the centres of the eyes are nearly on a horizontal line.

It is RECOMMENDED to perform a quality assessment on the images. The quality assessment SHOULD cover at least face and eye finding; it MAY contain a quality estimation based on criteria according to [ISO19794-5]. If a quality assessment is performed within the capture unit the best image according to the applied criteria SHOULD be provided to the verification unit. This speeds up the complete process because template generation and verification on obviously inadequate images is avoided.

The parameters of the camera, the pre-processing and the quality estimation steps MUST ensure the provision of face images within a broad range of contrasts.

The face images provided by the capture unit SHOULD have at least 90 pixels between the centres of the eyes (see [ISO19794-5]). Depending on the verification unit additional characteristics MAY be required.

It is RECOMMENDED to provide uncompressed (e.g. BMP) or lossless compressed live images. Alternatively non-lossless compression MAY be used, e.g. JPG. In this case it MUST be ensured that the loss of information has no significant impact on the recognition performance of the face verification unit.

The complete process of capturing (including pre-processing, quality assessment and provision of the resulting face image to the face verification unit) SHOULD NOT take more than one second per frame.

8.2. Face Verification Unit

Architecture and setup

The face verification unit SHOULD run on standard, industrial grade PC hardware. It's on the decision of the agency operating the ABC gates to allow more complex requirements.

The verification process MAY run locally within each ABC system or as a centralised service.

It is RECOMMENDED to use standard interfaces according to BioAPI [ISO19784-1] for the biometric verification process. The agency operating the ABC gates MAY decide to allow proprietary vendor-specific SDK interfaces for the integration of the verification unit.

Functionality

The face verification unit MUST compare the DG2 reference image and the captured live image.

Additionally it is RECOMMENDED to compare the DG2 reference image and the crop image scanned from the biographical data page. The benefit of this optional check is the detection of forged data pages (substitution of printed face image). Because of optical security features within the data page the comparison of DG2 and crop image may result in an error rate of about 10% FRR, this additional check may raise an alert for the official to have a more detailed look at the cropped image.

The verification unit MUST process DG2 reference images which may be stored in data formats JPG and JPG2000. It SHOULD process live images and crop images in uncompressed or lossless compressed data formats.

One face verification attempt (consisting of template generation and comparison) SHOULD NOT take more than one second.

The configuration of the face verification algorithm SHALL ensure a security level in terms of the False Accept Rate (FAR) of 0.001 (0.1%). At this configuration (comparison threshold) the False Reject Rate (FRR) SHOULD NOT exceed 0.07 (7%). It is RECOMMENDED that the achievable performance of the face verification algorithm is measured by an independent test laboratory or an official agency. The operating agency SHOULD NOT rely on performance figures given by the algorithm provider only.

The operating agency SHOULD NOT rely on the standard configuration of the algorithm provider only. For live operation of the system, it is RECOMMENDED to determine a proper algorithm configuration based on image data and verification results (cross-comparisons between different passengers) from the actual operational environment and a representative catalog of test users. It is RECOMMENDED to monitor the error rates (especially the FAR) continuously or at least periodically (e.g. once a year) and to adjust the configuration if needed.

Note: For systems based on the facil image biometric[4], it is RECOMMENDED to perform the FAR calculation of the ABC system as an independent but parallel process as follows:

- The reference face images (DG2 images) of the last ten passport verifications are temporarily and anonymously stored in a dynamic list.
- The live face image from the actual face verification process is compared against all other faces in the dynamic list and the comparison scores are saved (impostor comparisons). It has to be ensured that during the process a comparison of face images of the same person is avoided, which might happen due to multiple verification attempts of the same person.
- The actual live face image is compared against the corresponding reference face image and the comparison score is saved (genuine comparison).
- The reference face image is added to the dynamic list.
- The oldest face image in the dynamic list and the actual live face image are discarded and deleted safely. Storage and deletion of the face image data has to be implemented in accordance to the applicable data protection regulations.
- Calculate the FAR based on the impostor comparison scores. Genuine comparison scores MAY be used to calculate the corresponding FRR. Care has to be taken about the statistical base for the FAR calculation. In order to measure the performance of the face verification algorithm up to a security level (FAR) of 0.001 (0.1%), it is RECOMMENDED to perform the FAR calculation on the basis of at least 30.000 impostor comparisons.

8.3. Design of the Biometric Capture and Verification Process

If the face image acquisition and/or the biometric verification are not successful the process SHALL stop after a time-out. This time-out SHOULD be configurable.

[4] Other biometric modalities, such as fingerprints, will lead to different recommended settings and shall be discussed in future versions, as already alluded to in 5.3(Scope of This Study)

The process design SHALL guide the passenger for looking straight into the camera. While the live face images are captured other actions by the passenger SHOULD NOT be necessary and NO eye-catchers apart from the camera or feedback modules SHOULD draw off the passenger's attention. The feedback modules (display, LEDs etc.) SHOULD be installed very close to the camera.

The result of the biometric verification process SHALL be provided to a monitoring station. At least the overall verification result SHALL be displayed in the summary view on the monitoring screen. Additionally, the image data (DG2 image and live image used for the verification) SHOULD be shown in the summary view on the monitoring screen. It is RECOMMENDED that further details regarding the detailed checks of the biometric verification process be shown upon request by the operator of the ABC system.

The process SHOULD provide a fake detection (or liveness detection respectively) to detect fake attacks or improper use. Therefore, the biometric components MAY provide technical features for fake detection like dedicated sensors or software-based mechanisms. For this purpose an additional video surveillance MAY also provide video streams to a supervising operator.

A high-level illustration of the RECOMMENDED face capture and verification process for ABC system is shown in Figure 3.

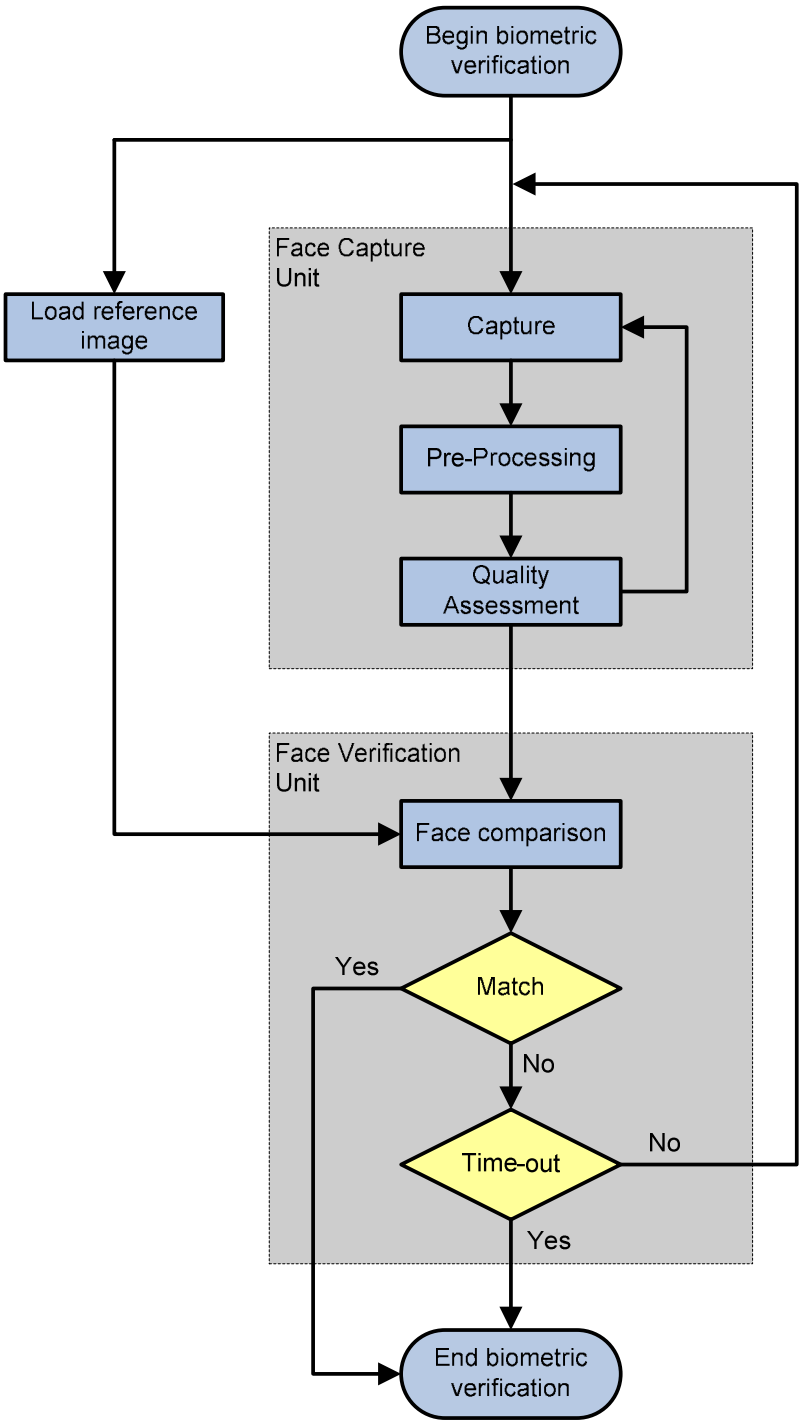


Figure 3: Face capture and verification process

9. QUALITY CONTROL

Quality control is a process by which the quality of all factors involved in the operation and exploitation of the ABC system are measured. Quality of an ABC service as such, in more practical terms, is the perception of the degree to which the ABC service meets the expectations of passengers and border authorities.

Quality control is of importance when assessing the performance of a given ABC system, aiding in the task of identifying potential problems in the operation of the said system. Also, operational data can be collected with the aim of obtaining key performance indicators of a system, thus enabling comparative analysis for the designer and the Border Guard.

The present recommendations focus on the minimum recommended anonymous operational data to be collected for quality control and the extraction of business statistics in ABC systems.

It is important to observe that quality control and statistical analysis are not part of the core functionality of this system and thus cannot be enforced, but is nevertheless highly RECOMMENDED to implement it. This section should be read as a set of REQUIREMENTS and RECOMMENDATIONS should the system designer decide to include data storage for quality control and statistical analysis.

Note that the following aspects are explicitly OUT OF THE SCOPE of this document:

- specific details on how to encode each data item to be stored
- specific tools for statistical analysis and performance indicator definition

9.1. General Recommendations

The following requirements and recommendations are broadly applicable when designing the dataset to be stored for quality control and statistics extraction.

Any set of operational data to be stored on a permanent basis in an ABC system MUST comply with the limitations imposed by national and European Data Protection regulations. Therefore personal data SHALL NOT be stored for the purposes of quality control and statistics extraction unless properly anonymized.

Any information MUST be stored within a structured data schema (e.g. a relational database, XML entries).

It is RECOMMENDED that anonymous operational data is stored in a centralised way at least at the ABC installation level (i.e. at the group of gates and monitoring stations at a given airport/port hall). Detailed maintenance and SW debug traces MAY be stored at the local level (e.g. at a given gate computer), since such data is unlikely to be of use when analysing operational performance.

It is RECOMMENDED that a clear interface for data extraction is offered, since it is out of the scope of the basic functionality of an ABC system to provide built-in statistical analysis.

An entry in the operational register should be created for any transaction taking place in an ABC system, regardless of its degree of success. Thus, apart from data from successful border crossings, anonymous data for at least the following types of transactions SHOULD be logged:

- Access attempts with documents not accepted by the system (i.e. non-electronic passports, not a passport).
- Access attempts with non-eligible documents (i.e. underage Schengen citizens holding an ePassport, third country nationals holding an ePassport).
- Access attempts by an eligible traveller, with a valid ePassport but whose verification was not successful (for example due to a biometric verification error).

It is RECOMMENDED that each entry within the operational register is as complete as possible, depending on how far the verification process could be completed. When a field within the transaction entry cannot be filled (e.g. unknown nationality or check not applicable for a document), a distinctive value MUST be used as placeholder, so that these gaps can be easily identified when processing the data.

The following sections add detail to the sorts of data which are of interest when logging for quality control and performance analysis.

9.2. Access Data

In all cases, the data entry MUST be time-stamped to allow for detailed performance and trend analysis.

In all cases, a data entry MUST include a specific field summarising the final outcome of the verification process, that is, whether the traveller was granted the crossing of the border without further, manual, action required by the officers monitoring the Border Crossing Pint (BCP). In its simplest form this can be a Boolean value, or it MAY include other information regarding the type(s) of failure of the verification process, although, as depicted in the following sections, such details SHOULD be stored separately, so that changes in access logic (the decision tree in charge of granting or denying the crossing to a traveller) affecting the outcome of the ABC verification process do not hide the result of each sub-process.

It is RECOMMENDED that the following traveller information to be part of a data entry:

- Nationality of the document issuer
- Age (or alternatively age bands, e.g. 21-25, 26-35…)
- Gender

It is RECOMMENDED that the following timing information is included in a data entry:

- Total verification time: defined as the time needed to fully verify an eligible traveller, regardless of the outcome of each of the particular checks (document authentication, biometric verification, background checks, etc.).
- Total access time: in single gate and mantrap solutions, defined as the total time spent by an eligible traveller since its first interaction with the system (presentation of the travel document in a 2-step mantrap, entry in the mantrap space in a 1-step mantrap, first interaction with the verification modules in a single gate or kiosk solution). The exact definition and estimate of this time will ultimately depend on the architecture of the system (e.g. when the full verification process takes place within a mantrap, this time measurement will always be greater than the verification time).

9.3. ABC Installation Data

It is RECOMMENDED that each ABC installation is uniquely identified within a national ABC deployment. It is RECOMMENDED that the identifier shows:

- A clear identification of the BCP (e.g. airport moniker).
- Detail information regarding the location within the BCP (e.g. terminal number, floor, arrival/departure hall number).
- Information regarding the type of BCP: entries or exits.

It is RECOMMENDED that every component of an ABC installation to be uniquely identified. This identification SHOULD be done at least at the verification and access module level, although a finer granularity MAY be used for maintenance logging purposes. It is RECOMMENDED the identifier shows:

- Module type (e.g. verification, access, monitoring, level 2).
- Module number. When numbering modules within a given ABC installation, designers SHOULD find the adequate criteria for numbering consistency in a given installation and across all ABC system locations (e.g. the lower numbers are given to modules closest to the actual exit of the installation).

9.4. Document Authentication Data

It is RECOMMENDED to include a subsystem for the logging of statistical and technical data regarding the document authentication process, for the purpose of having a continuous quality control, extraction of business statistics and improvements of the ABC.

It is RECOMMENDED that the following details on the document inserted are included in each data entry:

- Issuing country and date of expiry of the particular ePassport (if allowed by the applicable national data protection regulations)
- Date of issue (if extracted from the VIZ)
- Passport type (e.g. 1st or 2nd generation ePassport)

It is RECOMMENDED that the following details of a document electronic and optical authentication process are part of a data entry:

- time period for the entire document authentication process (from the beginning of optical image capturing until the provision of the final document authentication result)
- time period for the optical document checks
- time period for the RF chip reading process
- time period for the verification of the ePassport data
- Outcome of each of the authentication checks actually performed in the document, depending on the type of document and the authentication algorithm used. At least a Boolean value for each of the checks SHOULD be included, although the designer MAY choose to include more details on each field (e.g. indicating a given check is/is not supported by the document being read).
    - result of the optical document check and results of each optical sub-step (B900 ink, UV-Brightness, MRZ consistency, etc.).
    - result of the ePassport data authentication process and results of each authentication sub-step (EF.SOD verification, DS certificate signature verification, Certificate validity period, etc.).
- dump of the DS certificate used for the EF.SOD verification
- error messages from the particular process steps and document reader unit

9.5. Biometric Verification Data

It is RECOMMENDED to include a subsystem for the logging of statistical and technical data regarding the biometric verification process, for the purpose of having a continuous quality control, extraction of business statistics and improvements of the ABC.

It is RECOMMENDED that the following details of the facial verification process are part of a data entry:

- Overall result of the face capture and verification process
- Error messages from the face capture unit and the verification unit
- Time effort for the biometric verification process (from the beginning of image capturing until the provision of the final verification result)
- Delays resulting from the passengers behaviour (time effort from starting the capture process until the first successfully captured image is provided to the verification unit)
- Amount of single verification events within the verification process.
- At least the best comparison score of all single verification events within the face capture and verification process
- Best quality score of all successfully captured facial templates.
- The threshold against which the verification scores were compared.

For any other biometric verification which might be part of the system, it is RECOMMENDED that at least the following data is part of an entry:

- Time effort for the biometric verification process (from the beginning of live sample capturing until the provision of the final verification result)

- Delays resulting from the passengers behaviour (time effort from starting the capture process until the first successfully live sample is provided to the verification unit)
- Overall result of the verification process or, alternatively, the verification score and comparison threshold.
- Quality indicator of the best live sample (e.g. number of minutiae in a fingerprint).
- Quality indicator of the template, if available (e.g. number of minutiae in the fingerprint stored in DG3).

9.6. Other Data Sets

Depending on the exact features of the border control process, an ABC system MAY run other background checks in parallel with the document authentication and biometric verification checks. It is assumed that this background checks are obtained by accessing systems external to the ABC (such as a query to a Lost & Stolen Document Database). For this background checks, it is RECOMMENDED that at least the following data is included within an entry:

- Total connection (round-trip) time.
- Overall result of the check.

For kiosk systems in which access tokens are used, the following data SHOULD be part of an entry:

- If a physical token is issued, its serial number or any other identifier the token may carry.
- If a biometric token is used, the quality of the "enrolment sample" captured at the verification module (e.g. number of minutiae captured for a fingerprint).
- Total time invested in token generation or capture at the verification module.
- For successful verifications and token generation/capture: delays between the completion of the verification process and the crossing of one of the access modules. If the delay is too great or the crossing process is discarded by the Border Guard, this SHOULD be clearly indicated as process abandoned or aborted by the Guard.
- If a biometric token is used, the quality of the live sample captured at the access module (e.g. number of minutiae captured for a fingerprint).
- Total time invested in token reading/capture and authentication/verification at the access module.
- Overall result of token reading/capture and authentication/verification at the access module

10. OPERATION OF AUTOMATED BORDER CHECKS

10.1. Overview of the Border Checks Process

Schengen Borders Code, Visa Code and national legislation set the framework of the different measures used at the many border crossing points of the Schengen area. The detailed operations model followed at each border crossing point is carefully designed according to the specific demands, border checks code of practice, cooperation scheme with neighbouring state and risk analysis, thus differences are often found from one implementation to another.

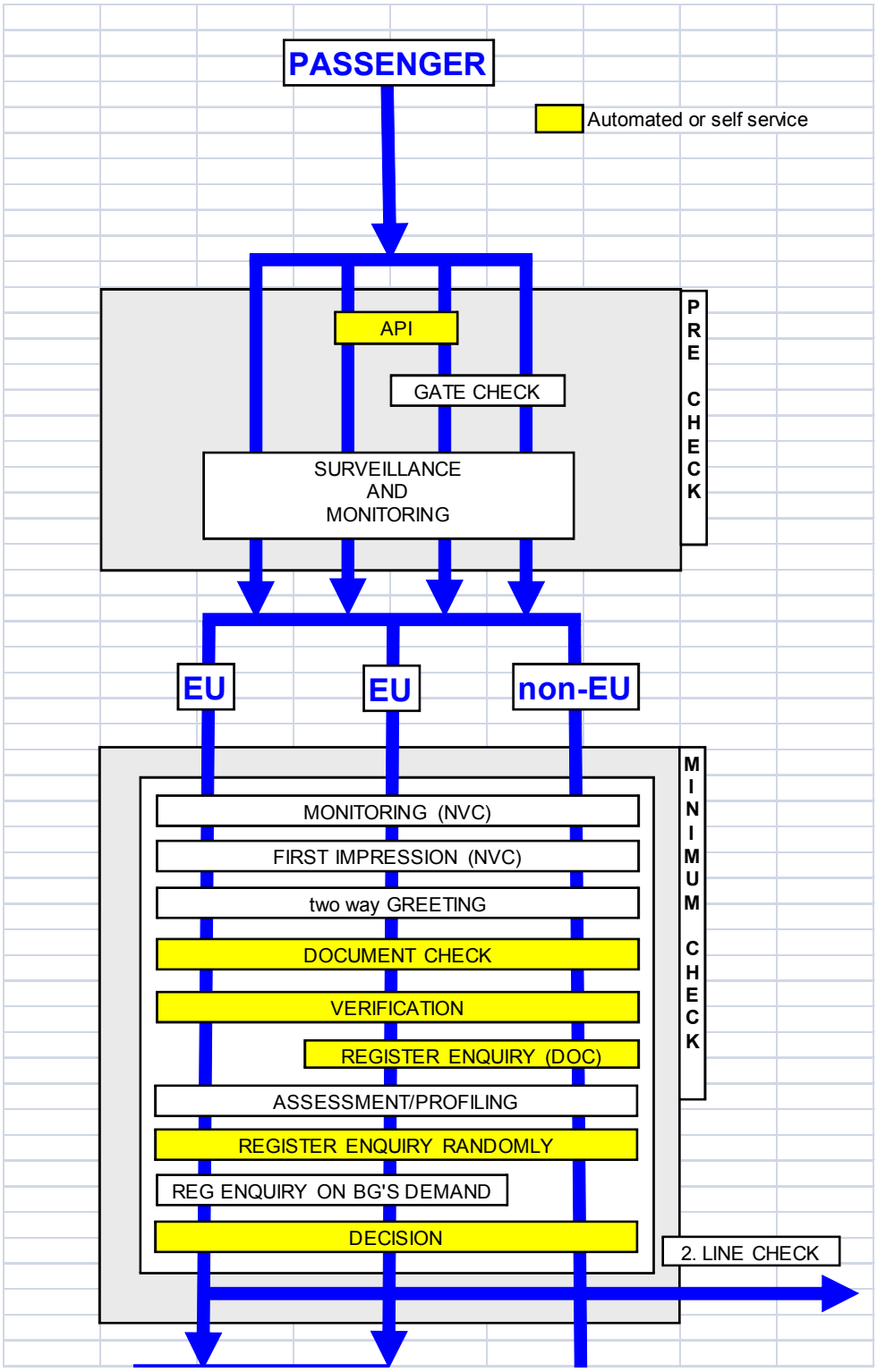
Narrow interpretation of border checks means only actions at the 1st line of control starting when a passenger hands his passport to a border guard and ends when he gets his passport back. In a wider interpretation, border checks starts when the passenger books his/her trip and ends when a passenger gets past the border crossing point.

Border checks are part of the four-tier control model forming an important part of a wider process. In automated border checks some tasks are automated and other parts are carried out by passengers as self-service. As a general principle, there should be no difference in the outcome (i.e. acceptance / rejection) if border checks are automated or carried out in the "traditional" way. It is very important however to note that automating many of the routine tasks allows a better use of officers' skills, i.e. devoting more time and effort on risk passengers and less time on bona-fide ones.

A border check process can be split into several sub-processes or tasks. Each sub-process is an individual part of the general process. The content of sub-processes is likely to vary from one BCP to another.

General process flow

The following flow diagram illustrates a tentative border checks process. This is presented here for illustration purposes only, in an attempt to provide the right context for the requirements and guidelines hereby proposed. It should not be considered as explicit recommended practice since the specific needs of each border crossing point may require a different approach.


PASSENGER
Automated or self service
API
GATE CHECK
SURVEILLANCE
AND
MONITORING
PRE CHECK
EU
EU
non-EU
MONITORING (NVC)
FIRST IMPRESSION (NVC)
two way GREETING
DOCUMENT CHECK
VERIFICATION
REGISTER ENQUIRY (DOC)
ASSESSMENT/PROFILING
REGISTER ENQUIRY RANDOMLY
REG ENQUIRY ON BG'S DEMAND
DECISION
MINIMUM CHECK
2. LINE CHECK

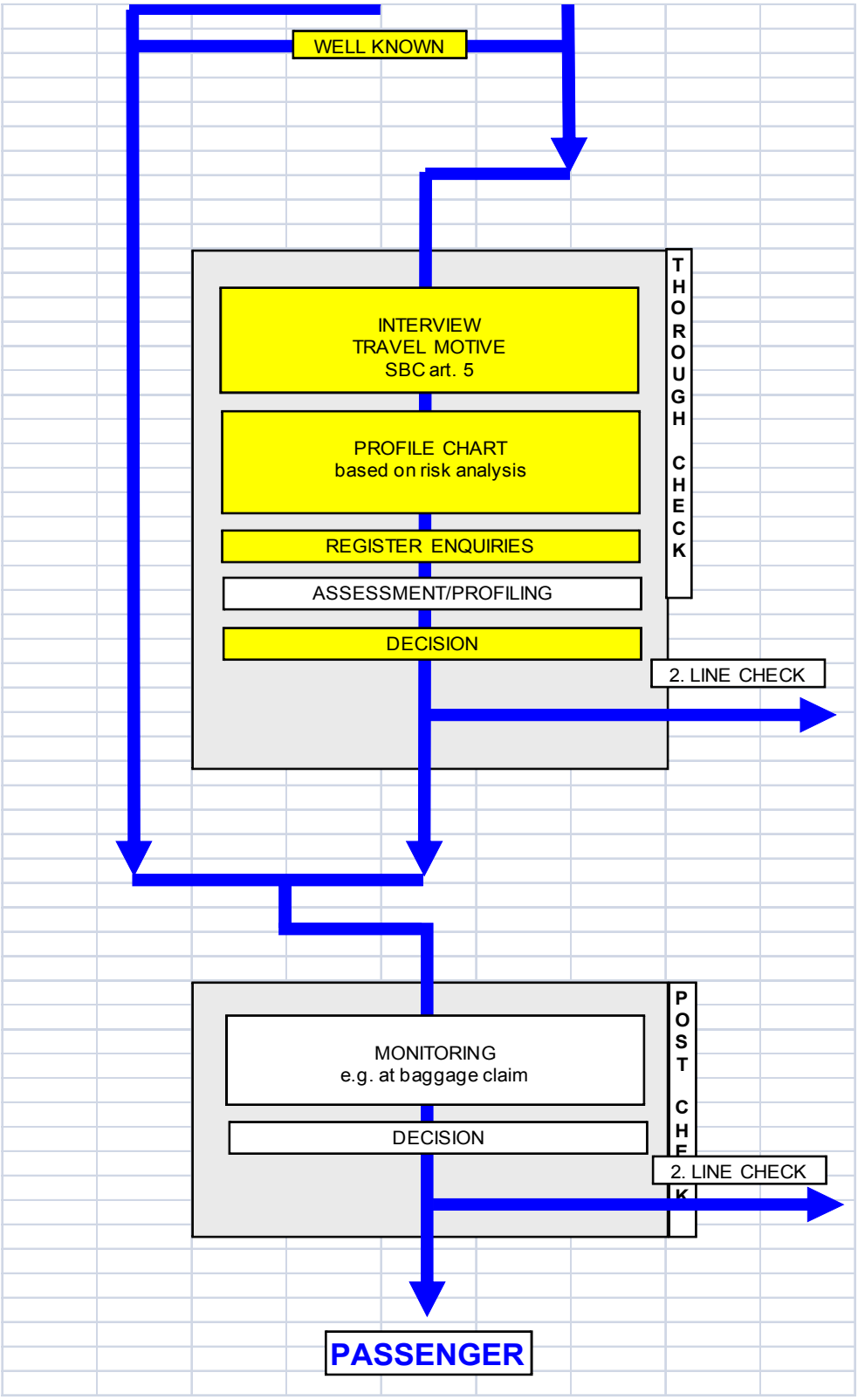


Figure 4 - Border Checks Process Flow

The yellow colour indicates tasks within the process that can be automated by means of an ABC system, hence these will be the focus of subsequent discussion.

Note that the diagram describes a border check process including third country nationals, which might not be the general case for many MSs. This possibility has been included here in order to provide some insight on the impact that future legislation about registered travellers program may bring, as ABC systems might need to be revisited in order to allow RTP passengers in the future to use ABC lines.

Operational requirements for an ABC system

The following general operational requirements MUST be observed by any ABC system in order to achieve basic operational harmonization across EU implementations:

1. "Cold lines" (i.e. stand-alone unattended ABC gates) MUST NOT occur. There SHALL always be an operator present monitoring the functioning of the gates. The operator MUST be trained to use the system and also to be capable of reacting to malfunctions or passenger's non-acceptable behaviour. The operator MUST NOT leave his/her post if ABC gates are active.

2. The operations of an ABC system MUST be compatible with the Handbook for Border Guards and comply with Community legislation (e.g. regular database enquiries shall not be done to EU citizens, except document enquiries.).

3. Number of gates attended by each officer (operators and/or assistants, see below) SHOULD vary depending of the number of passengers during a time period, whether it is entry or exit control, the nature of the passenger flow (e.g. risky routes), and the specifics of the environment (e.g. visibility on the gates and queues).

4. An ABC system MUST be easy to use by passengers, requiring as little guidance as possible. There SHOULD be adequate instructions for the use of an ABC system. If ABC systems are complicated or unintuitive to use, passengers will likely try to seek manual lines instead of automated ones.

5. Tailgating MUST NOT be possible. Regardless whether lines have mantrap or not, there SHALL be an automated detection of tailgating which gives an alarm and locks the ABC gate line. Tailgating is one of the biggest risks that come with ABC gates.

6. There MUST be a possibility to close an ABC partly or in full. A closed filter MUST prevent trespassing. There will be situations when some ABC gates are out of service or the passenger flow does not demand the whole line of gates to be opened. Therefore flexible configuration is vital to ensure a smooth operation of the gate line.

7. Overall time at an ABC gate SHOULD NOT take significantly longer than that at a manual line. It is natural behaviour that people want to minimise their queuing time. If it will take more time to pass at automated gates than manual lines, then the manual ones will be favoured. Present technical solutions at the market are regularly a bit slower at processing

than a well trained and experienced border guard at manual line. This can be compensated by opening several gates, thus reducing overall time by reducing queuing time. The psychological effect of seeing upon arrival a longer queue at the manual checks than at the gates is also as important as the actual time actually needed at each of the options.

8. The system MUST alert the operator in order to pay attention when a minor is using an ABC gate. There Schengen Borders Code annex VII paragraph 6 commands that major attention SHALL be put controlling border crossing minors and accompanying adults. In some states there are no legal obstacles in denying minors to use ABC gates, but some member states have no legal basis to reject passengers under 18 years old. If minors are allowed to use ABC gates, they and accompanying adults SHALL be interviewed if it is not obvious that they are members of the same family.

10.2. Deployment of an ABC System

Physical arrangement of gates and monitoring Station

Queuing lines for the ABC gates SHOULD be placed next or close to the queuing lines for manual checks. Very often it is difficult for inexperienced passengers to orient themselves towards the correct queuing lines, be they manual or ABC. If a wrong line is chosen by accident it must not be too complicated to reach the intended line. Some synergy on operations can also be achieved when manual and automated lines are situated next to each other.

The monitoring station (i.e. operator's control post) SHOULD be built in a way that it also allows manual first line checks. It is also RECOMMENDED that the monitoring station have the same equipment as manual lines. A RECOMMENDED approach is to build the monitoring station like a control booth for two manual lines. One post is for the operator and the other for his/her assistant (see below). If a case occurs that needs further inspection/interview, an operator points out the person to the assistant who will release the passenger from the gate for closer inspection. This kind of monitoring station may also be used as two manual lines in the case of an ABC system being out of service (e.g. system crash, repair, maintenance).

Dimensioning the number of gates

The number of gates available for users will vary on the flow rate to be processed and the service quality to be delivered. For any given amount of passenger flow, more gates will reduce queuing time but at the same time will use more resources (financial and human) and will complicate the monitoring, support and risk profiling tasks. There is an inherent trade off between service excellence and cost effectiveness that needs to be carefully balanced.

One way to tackle the right dimensioning of the number of gates is by means of operational research. A queuing analysis, either analytical or by simulation, will reveal the relationship between the three variables: flow rate, service quality and

lifecycle cost; and will allow for the identification of bottlenecks, resource consuming elements and optimal trade offs.

One possible way is as follows:

1. A service quality figure of merit is defined (e.g. queuing time)
2. A desired value is chosen for this figure of merit (e.g. less than 5 minutes for 95% of passengers)
3. Passenger flow is stochastically characterized (e.g. arrival rate as a log-normal distribution)
4. Operational model is developed observing different arrangements and number of gates
5. Lifecycle cost model is developed for the different arrangements and number of gates
6. Figure of merit and lifecycle cost are calculated for all possible combinations of arrangements and number of gates (e.g. using discrete event simulation and Monte Carlo[5] simulation). Combinations failing to meet the security threshold (or other equivalent criteria) are automatically discarded at this point (i.e. only points in the Pareto frontier are considered).
7. Dominant configurations providing the best figure of merit for any given lifecycle cost are drawn in a curve FoM vs Lifecycle Cost. This is the cost-effectiveness Pareto efficiency frontier of the system
8. A point in the curve (and thus a specific arrangement and number of gates) is chosen on the basis of available budget and comparison with manual checks

The above method can also be used (with minor modifications) to forecast the point when an already operational implementation might need to be upgraded, or even simulate the effect on service quality of possible modifications.

10.3. Roles and Tasks of Personnel

There are two main roles in the operation of an ABC system: the Operator and the Assistant. Other roles are also possible, although these two are the ones common to every ABC in place at the time of writing.

Operator

An operator is responsible for the remote monitoring and control of the ABC system. The most important task of an operator is to bring the needed human factor into the automated tasks. With unattended stand-alone lines it is impossible to reach acceptable level of facilitation and border security.

[5] - Monte Carlo simulation is a computerized mathematical technique that allows to account for risk in quantitative analysis and decision making. Monte Carlo simulation performs risk analysis by building models of possible results by substituting a range of values—a probability distribution—for any factor that has inherent uncertainty. It then calculates results over and over, each time using a different set of random values from the probability functions. Monte Carlo simulation produces distributions of possible outcome values.

An operator:

- Monitors and profiles passengers queuing in the ABC line and using the ABC gates looking for suspicious behaviour in passengers
- Monitors the user interface of the application
- Reacts upon any notification given by the application
- Manages exceptions and makes decisions about them
- Communicates with the assistant for handling of exceptions at the gates
- Communicates with second line checks whenever their service is needed

Operators do their job from the user interface of the control application located at the control desk or booth. This should be stationed on a lifted position allowing the operator to monitor passengers at the ABC lines. When monitoring queuing passengers an operator must evaluate passenger flow in order to select suspicious targets to be more closely checked. The evaluation or assessment method is typically based on passenger's actions and body language, i.e. non-verbal communication. When a passenger is pointed out, the operator shall request the assistant to redirect the passenger to a manual first line check or directly to the second line check. Passengers pointed out are then escorted to the appropriate next step. It is also possible that the assistant shortly interviews the passenger before the above decision is made.

An operator MUST not leave his post when ABC gate(s) are active. If a situation occurs that an operator should leave his post (e.g. to help a passenger in a mantrap), he MUST lock ABC gates first.

In normal circumstances when a passenger flow is continuous without pauses, a maximum surveillance time for an operator SHALL not be longer than 30 minutes. An operator and an assistant MAY change their tasks at intervals of 20 – 30 minutes. If there are natural pauses in passenger flow (e.g. because of flight schedules) or the frequency of passenger flow is moderate an operator MAY work for periods longer than 30 minutes.

Assistant and operator MUST be linked with a communication system.

Assistant

An assistant is an immigration officer whose task is to handle the exceptions that take place at the gates, redirect passengers as needed, and support passengers on specific situations. An assistant works in close co-operation with an operator.

An assistant:

- Retrieves passengers from mantraps pointed out by the operator
- Makes short interviews in order to find out if there is need to redirect passenger to a second line check
- Makes passenger assessments and informs the operator
- Retrieves passengers to second line checks when needed
- Makes manual first line border checks, if the infrastructure of ABC lines fails
- Handles other exceptions and assists the operator
- Informs and provides on the spot support to passengers (e.g. families, minors etc.)

Every assistant SHOULD have at least one operator assigned. Task of an assistant may be organised so that every operator has an assistant of his own or there is(are) assistant(s) that co-operate with several operator.

The location of the assistant highly conditions the time he/she will spend in each of the above tasks. Placing the assistant after the eGates will make him/her focus more on handling exceptions and assisting the operator, whereas placing before the eGates will make him/her spend more time in assisting passengers and profiling.

Assistant and operator MUST be linked with a communication system.

Number of ABC gates supervised by operators

During field tests it was observed that a single border guard officer can typically supervise from three gates to ten gates. Those tests were carried out on inbound flow (passengers entering the state operating the ABC system).

There are limitations as to how many gates an operator can supervise in practice. Those limitations are due to limited ability of human being to concentrate on several things at same time. In some studies it has been found out that an average person can notice and understand three things simultaneously without major problems. It is therefore important to assess how much attention it will cost for the operator to stay in the loop. If it costs a lot of attention (and therefore energy) to have a good and thorough situational awareness (at the three levels) of the number of e-gates you use, the less e-gates is possible to monitor.

There are some known aspects that condition the maximum number of gates controlled by an operator. These are (among others):

- Quality of face recognition, how much human action is needed
- Frequency of the passenger flow, how crowded the system is
- Whether it is entry or exit checks
- Profile of the passenger flow at the BCP, what is the combination of own nationals and other EU citizens, how often operators have to react and channel passengers to manual first line or second line checks
- User interface of operation desk
- Reliability of the system
- Proficiency and training of border guards

The above mentioned factors MUST be considered and analysed when deciding the number of ABC gates to be simultaneously supervised by an operator.

In practise it has been found out that there are no reasonable benefits in having less than three gates per operator. Practise has also shown that on entry side more than seven gates is inadequate, and on exit side there should not be more than ten gates per operator.

The operator's interface should be designed in a way that it can easily be split into two or more supervision stations in order to quickly accommodate new operators into the task.

10.4. Handling of Exceptions

Border guards need detailed instructions on how to proceed when specific exception situations occur.

There MUST be a modus operandi handbook (e.g. ABC Handbook for Border Guards) providing detailed instructions on how to proceed with the different unwanted situations that may happen at ABC gates. Those measures SHALL be decided in advance and SHALL be practiced by operating personnel. Provisions SHALL be made to insure that all forms of unwanted situations can be avoided or effectively neutralized Chosen measures may vary at different BCPs depending infrastructure, number of gates, frequency and profile of the passenger flow etc.

The following is a compilation of RECOMMENDED way forward for a set of commonly encountered situations. Specific instructions MUST be tailored according to the specifics of each implementation.

System malfunctioning

If a system fails to perform normally (e.g. power shutdown, communications outage, component failure, random errors), there are typically two possible ways forward: first one is to open one or two ABC gates and perform manual checks at supervision station, this is the default recommended option. If that is not possible, ABC gates SHALL be closed and first line checks be carried out at manual first line.

When establishing the contractual agreements with solution providers or developing own service system, it is RECOMMENDED to define service quality agreements.

Gates out of service

If one or more ABC gates have to be out of service while the rest operate normally, there MUST be an option to physically close those gates and avoid passengers from inadvertently try to use them.

Tailgating

If two persons try to pass an ABC gate at the same time, it MUST be stopped. The assistant MUST find out the reason for such action. Both persons MUST be interviewed if a justified cause for the tailgating attempt is not obvious. If there is clearly no illegal behaviour intended, the second person MAY be returned front of the gate for a new personal attempt and the first person is to continue if system accepts his pass.

Minors and children

If minors (under 18 years) are allowed to use ABC gates, their families MUST be advised about minimum height and gates must be passed one person at a time under all circumstances. Manual checks SHOULD be recommended for families with small or several children.

If a passenger enters an ABC gate with a child in his arms, he MUST be stopped and redirected for manual checks observing SBC annex VII paragraph 6.

Passenger foregoing

It is important that operators and assistants are able to monitor passengers at ABC gates. If a passenger approaches an ABC gate with an obvious intention to pass it, but foregoes it for some reason, it is in some circumstances necessary to find out their reason. Operators and assistants SHOULD make an assessment based on passenger's non-verbal communication, if there is a reason for further questions.

Trespassing

The infrastructure at ABC lines SHALL be such to prevent trespassing. If trespassing happens despite the measures in place, there MUST be practised modus operandi to quickly react and catch the trespasser. Methods may vary at different BCPs. E.g. there may be a patrol(s) behind first lines or remote controlled doors.

Non-EU citizen

If a non-EU citizen tries to use ABC gates that are for EU citizens, the system SHALL reject his attempt. The passenger SHOULD be redirected to manual first line checks for non-EU citizens.

Passport is not biometric

If an EU citizen tries to pass an ABC gate with non-biometric passport, the system MUST reject his attempt. The passenger SHOULD be redirected to manual first line check for EU citizens.

Passport is placed wrong way into a reader

If a passenger places his passport into a reader in the wrong way, he SHOULD be informed about the correct way to do it. Informing can be made by system screen, voice command by the operator or hand-to-hand guidance by an assistant or airport personnel. A new opportunity SHALL be given before rejecting the passenger.

Non-cooperative behaviour in a mantrap

Non-cooperative behaviour at the gate may occur when e.g. a passenger moves too much when face recognition is taking place, looks in the wrong direction, stands in the wrong place etc. An advice SHALL be given. If this has no influence, the person SHALL be taken into manual first line checks.

Chip is broken

If a chip is broken or it cannot be read for some other reason, a passenger SHOULD be redirected to a second line for more through checks on the travel document. Since ePassport chips are quite sturdy and reliable, a broken chip SHOULD be considered as a red flag indicating a risk situation.

Anomalies in chip data

There have been cases that ABC gates do not accept some EU passports (not fully ICAO 9303 compliant genuine travel documents, known as “defects”). Reason may be missing public key, expired certificates or some other technical reason. In these cases those passengers MAY be redirected to manual first line checks for EU citizens as the travel document is still a valid one.

Database hit

If a database hit occurs, the passenger SHALL be redirected to the second line check. A practical way is to let the passenger enter the mantrap, and after that an assistant escorts him to the second line. In single gate configurations, the gate SHALL stay closed until an assistant arrives.

A rejected passenger at an ABC gate because of a database hit SHALL NOT be given a second chance at either the manual line or the ABC gates.

Failed biometric verification mismatch

In the case of a failed biometric verification the monitoring operator should compare the displayed images and decide how to proceed. As a general rule the passenger SHOULD be redirected to a second line check.

Wrong or no security features on the biographical data page

The biographical data page SHALL be checked with visual light, UV light and IR light. The system is configured to check and detect for irregularities in the security features. If there a security feature is missing or some other hints suggest a false or forged document, a passenger SHALL be redirected to a second line check.

11. PASSENGER EXPERIENCE

As noted in other parts of this document, the main goal of an ABC system should be facilitation in order to make border checks a simple and hassle free process. Education and information will be essential to ensuring that the passenger experience when using ABC systems is a good one. First by creating the right expectations on the benefits of using the system, and second by unambiguously explaining what to do in order to materialize these benefits.

ABC systems, as they currently stand, provide similar service to travellers although there are a number of differences between implementations. This lack of universality makes the task of harmonizing passenger experience a significant and difficult one. The novelty of such systems (while decreasing all the time) is also another major challenge – many eligible passengers will be unfamiliar with many concepts and parts of the process, particularly since implementations tend to differ not only in the looks, but also in functionality and usage.

In order to provide a successful passenger experience, care must be taken in:

1. Creating awareness and education before arriving to the gate, and
2. Making the ABC a user-friendly service

The following sections offer a number of findings and recommendations on the above areas. The reader should be aware that what is presented here is not the result of an exhaustive research, thus more successful approaches might be found than the ones proposed in this document.

11.1. Awareness and Education Before the Gate

Delivering information before the passenger arrives to the gate is a challenging task, for the following reasons:

- Since it is given in advance, only a limited amount of information will be retained. It is not realistic to expect that travellers will remember detailed usage instructions for a long time.
- The information given in advance does not have the visual support of the real system or other users using the system, thus interpretation may vary significantly from one individual to another

Thus, it is RECOMMENDED that any information given in advance be oriented towards creating awareness on the system and developing willingness to use it. The earlier this information is given, the simpler it has to be in order to be effectively retained.

Key messages to be transmitted

Making the passenger aware that an ABC system is present and can be used for his/her own benefit is critical to getting more passengers to leave the queue for the conventional manual control. Advance information SHOULD convey the message that it is better to use automated border checks than manual border checks. Only if a considerable number of passengers use the system, the investment will be justified.

The process of providing education before the gate can usefully be divided into the following categories:

1. Understanding the BENEFITS that the system brings to users
2. Communicating that the system is EASY to use
3. Communicating that it is POSSIBLE to use an ABC gate at the port
4. Explaining who is ELIGIBLE to use the ABC gate
5. Describing HOW to use the ABC gate

The latter aim overlaps considerably with the aim of information provided at the gate, but can also differ, being aimed, for example at different aspects of the process at the gate (e.g. instructing passengers what signage to look for in order to find the gate, the queuing process, what to have ready (biometric passport) etc.)

Delivery methods

The following methods have been used at the different ABC implementations to deliver these messages to the passengers:

- Signs ("airport" format)/logos
- Videos
- Human assistance (either ahead of the gates or at enrolment)
- Leaflets
- Posters/banners
- Literature (a page in in-flight magazines)
- Audio announcements

The locations in which this is done include:

- On aircraft flying to the airport possessing the gates
- In waiting/transit areas (this could include lounges, walkways, baggage handling areas)

No formal assessment has been carried out yet on the effectiveness of the different methods used. It is also clear that there is no uniform signage at ABC systems currently in operation in the EU, which will be detrimental to the public understanding of such systems.

It is RECOMMENDED that:

1. A study be conducted by the owner of the system to establish the most effective ABC awareness-raising methods.

2. The target audience be carefully analyzed, and the best methods be chosen according to the specifics of this audience. It is also important to remark that the composition of this audience will vary in time and thus the methods of choice at any point in time will also have to be modified accordingly.

It is equally clear that other public information methods exist which have not yet been tried by some or all MS, and are worth considering. Examples include:

- An EU-wide awareness-raising campaign (this becomes more cost-effective as ABC systems are extended to road BCPs, where opportunity for pre-border education is limited or non-existent)
- Videos on flights (and other vehicles)
- "live" demonstrations by staff in appropriate areas
- Literature provided at issuance of biometric passports

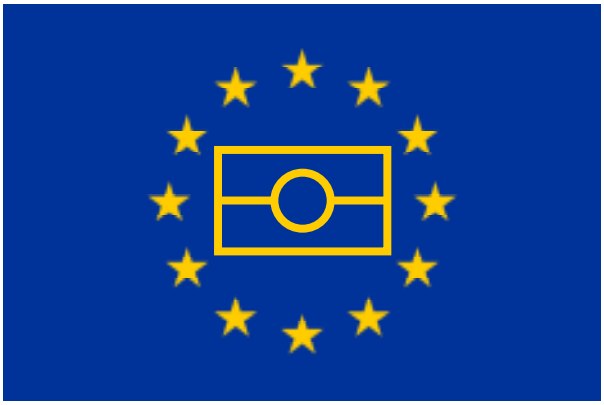
Need for standard signs, instructions and logos

Signs and any other form of graphical display are very important. They are often the first contact that the traveller has with the system, and to a large extent may condition its willingness to use.

Member States currently using or piloting ABC systems have tried several different types of signage but none has proven to be clearly more effective than the rest, probably because the concept itself of biometric passport and automated border checks are not widely known even among frequent travellers. One of the more important challenges is developing a set of signs and standard terminology that can be understood by the majority of the travellers. These have to be intuitive for travellers to assimilate, uniform across MSs, and easily deployable.

In order to facilitate and harmonize the passengers' experience at the Schengen external borders, a need for a set of harmonized icons, visual signs and instructions across EU ABC implementations has been identified. While the Schengen Border Code and the Practical Handbook for Border Guards spell out the common signage to be used for manual checks (for example to segregate EU/EEA from Third Country passport holders), no similar provisions currently exist for automated border checks.
In the absence of a European common name for referring to the ABC system, the following name is RECOMMENDED in order to denote the existence of automated border checks: **Self Service Passport Control**. The name of choice MAY be used in conjunction with a short brand "catchy" name for the service (e.g. No-Q in the Netherlands, EasyPass in Germany).

In the absence of a European common and unique logo depicting the system, the following logo is RECOMMENDED in order to denote the existence of automated border checks:



11.2. Running a User Friendly Service at the Gate

Service excellence at the ABC gates means encouraging passengers to use the system, helping them understand that they are eligible, and facilitating a successful transaction. This section describes the findings on how to make the service of automated border checks as user friendly as possible.

The findings are broken down into six areas:

- Instructions to passengers on the usage of the system;
- Effectiveness of the information delivery methods
- Managing passenger flow at the gates
- Learning by observation
- Passenger interaction with the gates
- Support to help passengers use the service;

Instructions at the gate

Passengers' cooperation at the gate is essential in order to ensure good performance of the system, a positive experience for all the users, and continuous and accrued use of the gates in time. Clear instructions are thus paramount, and human behavioural factors should be taken into consideration when designing the control process and assessing the overall performance of the system.

Instructions SHOULD be carefully crafted according to the specifics of each implementation.

It has been consistently observed that the most challenging part of the process to educate the passenger in is the correct placing of the passport. This is easily misunderstood, and if the document is incorrectly placed then it almost inevitably results in a failed transaction. This practical aspect MUST be prioritized when designing instructions at the gate. Clear instructions with an animated display on the screen have proven to be helpful.

Other steps in the process, such as capturing a facial image successfully and exiting the gates, are more easily understood, although not free of problems. Another recurrent issue is that during the face capture process, the user does not really know when to stop looking at the camera. Some feedback MUST be given. Visual feedback is preferred to audible feedback as sounds from adjacent gates may create confusion and increase exceptions rate.

"Footprints" on the floor inside the mantrap or in general in front of the camera may help the passenger to position himself/herself in the appropriate location for face capture. Footprints may however be counterproductive in some cases, as some users concentrate on the footprints and look down instead of looking straight into the camera.

Effectiveness of delivery methods

There is a variety of delivery methods that can be used to show passengers how to use the gates. These range from signage and info DVDs, to graphics displayed on the gates themselves.

There is consensus in that no one form of media was effective above another. Signage was felt to be mainly ineffective, and should not be relied upon to relay key messages as passengers tend to ignore them. Signage which is well placed and visually appealing was found to be more effective in catching the passenger's attention.

Signs SHOULD use as few words as possible. While most ABC owners noted that simple graphics work best, with fewer words (thus eliminating the problem of language), some icons mean different things to different cultures. Complex sentences are not easily understood and SHOULD be avoided.

For instructions on how to use the system, still images and animations have proved to work better than using video. This is thought to be because the viewer has more information to process when watching a video, and a ten second video simply adds an additional ten seconds to the transaction process, which is ineffective.

It was identified that info DVDs playing around the gate area are often unnoticed and passengers do not seem to use them effectively. It is possible that these would become more effective once passenger usage rises to the extent that passengers have to queue to use the gates, as they are more likely to observe the info DVD whilst queuing.

Audio announcements in the arrivals hall were also considered to be no better than average in raising passenger awareness.

Leaflets have been used to raise awareness with some success. The challenge with leaflets was in identifying a good area to distribute them where passengers would be receptive to reading them.

Managing passenger flow

Passenger flow can greatly benefit if it can be assisted by trained personnel in order to have a smooth, uninterrupted flow avoiding unnecessary delays.

It is RECOMMENDED that officers provide on the spot support for queuing users and help in distributing the load on the different gates. It has been observed that travellers tend to be more receptive when officers in this role do not wear uniforms.

Passengers holding travel documents not recognized by the ABC system SHOULD be directed to manual border checks as early as possible. Some sites have clearly segregated areas for queuing for the gates and this was found to be effective as it enables passengers to see the gates clearly.

Tactics deployed to encourage passengers to use the e-gates have included the use of signs distributed along the manual checks queuing line, and the deliberate prolongation of queue time at manual checks so that eligible passengers find the e-gates more attractive.

Queuing lines SHOULD be designed according to the specific layout and available space of each implementation. In some implementations queues are allowed to cross each other. This allows for better usage of floor space, but it has been observed that under rush situations there may be conflicts between queuing passengers.

The use of 'wait for your turn here' lines for passengers to stand behind whilst queuing was not found to be effective.

Learning by observation

Queuing contributes to the learning process of non-experienced users by observing how other users interact with the system. This is an important aspect that needs to be considered when designing the queuing space at the eGates.

During the first stages of running the system, it MAY be configured for the complete process to be slower than strictly necessary in order to facilitate the learning while queuing process. The effectiveness of this measure will also depend on many other factors like visibility, usability and previous understanding of the system.

The size of the screen SHOULD be large enough for the user to interact easily AND for the user queuing behind to observe the whole process.

It has been observed that non-experienced users tend to use the gates closer to their queuing line as this reduces the sensation of uncertainty (using the specific eGates upon which the observation process took place). These non-experienced users typically have an exception rate higher than experienced users. Thus, experienced users tend to use the gates at the edges because experienced users generate fewer exceptions and have a somewhat shorter processing time (as they know how to look properly into the camera, the face capture process takes less time). This is a positive feedback process. Consequently, the gates at the edges may exhibit more throughput and less exceptions than the ones closer to the queuing lines, despite being exactly the same ones in HW, SW and configuration.

Passenger interaction with the gates

The screens used to display the graphics varied in size, but generally a larger screen works more effectively, particularly if it is large enough to be observed by the passenger queuing to use the gates. Many of the participants found their screens were not easily read in all lighting conditions, which reduced their effectiveness. Screens SHOULD be tuned to be readable in all lightning conditions.

Processes where the passenger simply goes forward rather than having to turn or alter course were considered to be most effective. It is RECOMMENDED that the design allows the passenger to move simply forward in a straight line, rather than having them turn or stop during the transaction process.

A camera mounted straight ahead has been observed to be more effective than one where a passenger has to turn their head 45 degrees or more. Where the gates were offset to allow for this, passengers would have benefited from an audio cue prompting passengers to exit the gate area.

Audio cues, such as soft ‘pings’ encouraging the passengers to move to the next stage of the process MAY be used. In the absence of other indication, some mechanical noise is RECOMMENDED to allow the passenger to realize that the gate has actually opened. Whenever audio feedback is given, there SHOULD be acoustic isolation between gates to prevent confusion or false feedback.

In mantraps where all the transaction takes place inside the mantrap (i.e. passport reading is not required to enter the mantrap), it is RECOMMENDED to give a “Have your passport ready” message in order to avoid passengers looking for their passport inside the mantrap. This can cause unwanted timeouts and frustration on travellers.

The design and the size of the e-gates (width and length) SHOULD consider the usage of trolleys and other luggage (e.g. duty free bags). Trolleybags are not easily catered for, and even the gate with the largest secure zone (measuring 90cm x 200cm) had problems. This is because passengers handle their bags in different ways, and trailing bags can easily obstruct the doors closing, which slows down transaction times.

Unicity and tailgating prevention SHOULD be carefully designed. Several methods exist to ensure that only the cleared traveller actually goes through the gate. Most of them have delivered similar results, but research is still very active in this topic and improvements are expected for the short term.

Human support at the gate

All new sites installing ABC systems SHOULD include the use of passenger assistants to show the public how to use the gates. The provision of staff to show passengers how to use the gates for the first time was considered by all the participants to be highly effective. This is because passengers have often not seen or used such technology before, particularly in the case of infrequent holiday travellers. It was felt that passenger assistants encouraged use, reduced the 'fear factor' for first time users, and were able to educate passengers more successfully than passive techniques such as signage.

It was observed that once the system had been used and was understood by the passenger then its use did not need to be shown again. This means that over time the need for staff members to show passengers how to use the gates would be reduced. This would be helped by more systems being installed across Europe as the technology becomes more common. It has also been noted that human support at the gate also distracts passengers, slowing down the self-learning process.

It should be noted that typically the main users of the system in each country were their own citizens, so it was observed that at the outset the use of passenger assistants would be beneficial.

Where passenger assistants are provided, they SHOULD be wearing civilian clothing, as passengers find them less intimidating and more approachable. Many of the operational sites use staff provided by the airport operator.

It was noted that in some instances the border officers have requested the installation of an intercom which would enable them to communicate directly with gate users from the monitoring station. Communications between passenger at the gate and officers SHOULD be kept to a minimum in order to automate the border check as much as possible and minimize passenger-border guard interactions, as these are known to be the main reason for slower throughput. Intercoms may be installed to interact with the passenger under specific circumstances (e.g. "the door is open, please proceed"). If used, communications SHOULD be initiated by the officer, not the passenger (unless there is an emergency). Preferred idioms for verbal communication are local language(s) and English.

ANNEX 1: SYSTEMS DESIGN

Systems design is the process of defining the architecture, components, modules, interfaces, and data for an ABC system to satisfy the specified requirements.

In this section a generic architecture and basic dataflow scheme will be presented. This is just one of the many feasible architectures which could be used to set up a successful ABC system infrastructure. It is presented here for illustration purposes only.

Definitions

The following terms are used throughout this section:

- **Verification module**: the set of hardware and software in charge of verifying the identity of a given traveller at an automated gate or kiosk. This includes the necessary hardware and software for document authentication as well as for biometric verification, along with other software modules to perform additional checks and connect to external/centralised services (such as background checks). Note that in this definition no preference is stated on whether the verification module should or should not be monolithic, e.g. the verification module could be split in two different locations of an automated crossing (such as the case of a 2-step mantrap with the document authenticator on the entry gate) or jointly installed (as in the case of a 1 step mantrap, a single gate or a kiosk installation).
- **Access Module**: any physical barrier and their intelligence controlling passenger flow and ensuring that only properly verified travellers actually cross the border. Access Modules range from a tightly integrated mantrap to an independent token-controlled gate.
- **Monitoring Station**: the set of hardware and software used by the Border Guard Operatives to supervise the operation of the ABC system and deal with alerts and incidents which may arise during a traveller's verification process.
- **Level 2 Station**: the set of hardware and software used by the Border Guard Operatives to perform a more thorough check on any given traveller, and which could be integrated with the ABC system transaction database to retrieve information of that traveller's interaction with the system.
- **Central server**: refers to the set of hardware and software in charge of implementing services common to a set of automated crossings (transaction databases, connection to external services, software repository, etc.). Note that no preference is given between fully centralised servers on a national scale or servers in charge of a given Border Crossing Point or installation, since the actual design choice will depend on the scope and size of the ABC system.

Systems Architecture overview

Figure 5 - High-level architecture shows a simplified view of one of the RECOMMENDED architecture.
Note that the following aspects are explicitly OUT OF THE SCOPE of this document:

- decision whether or not the ABC system is build as a two-door solution (mantrap) or a single-door solution (kiosk + gate)
- defining specific functionalities and interfaces for each of the blocks within an ABC system

The ABC Installation, that is, the verification modules, access control modules (e.g. gates), monitoring and control stations and associated level 2 controls for a given location where the ABC system is deployed (e.g. an arrivals/departures hall at an airport). A more detailed view of the blocks comprising this part of the architecture is offered in section Architecture of the ABC Installation at the BCP of this document.

The Central server and its associated databases for the implementation of the following functionalities: transaction and business logic, quality control, configuration management, software repository, access token management (if required) and connection to external systems. The Central Server will implement most of the intelligence of the Border Crossing Point, based on the verification and authentication results received from a given gate and other external systems (e.g. background checks); the server also implements software update rollouts, registering of quality control and system usage, system configuration, etc. A more detailed view of the blocks within this part of the architecture is offered in section Architecture of the Central Server of this document.

External systems: although not strictly an integral part of the ABC system, the connection to external systems such as the ePassport certificate PKI and other background check databases (Police Databases, Lost and Stolen Document Databases, etc.) MUST be taken into account when designing the overall system architecture.

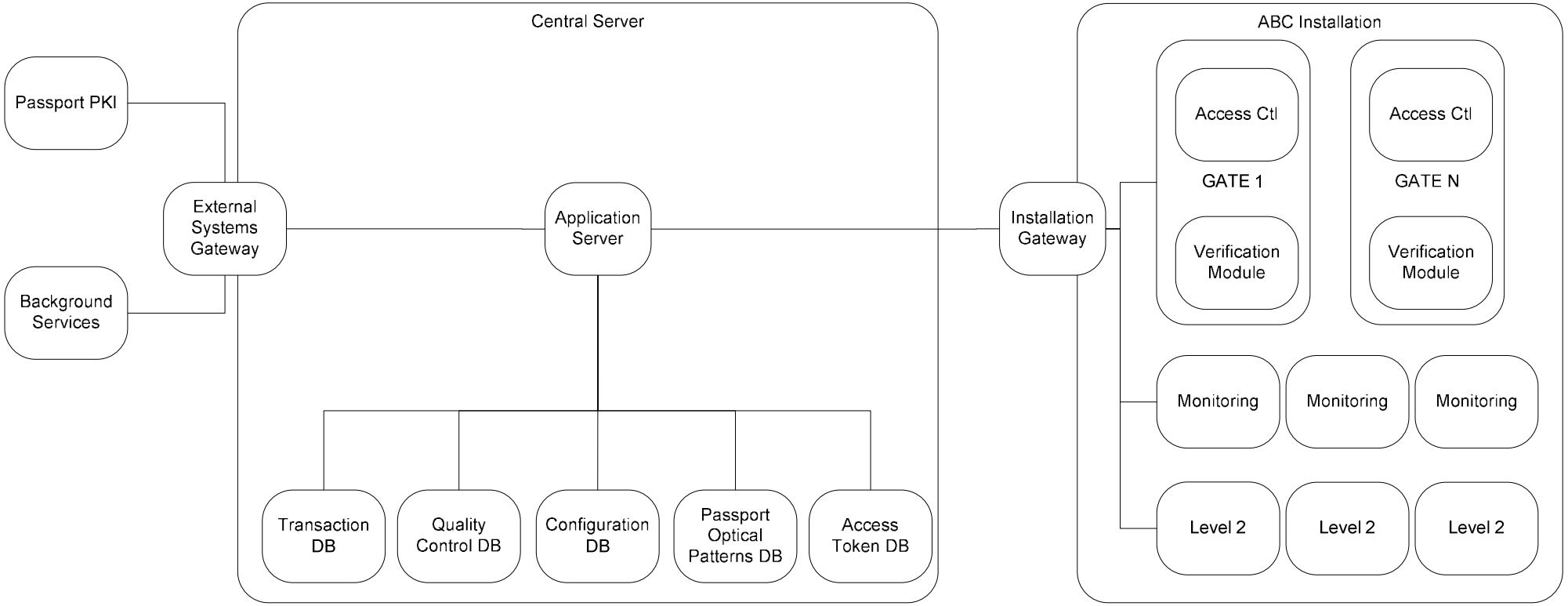


Figure 5 - High-level architecture

It is RECOMMENDED that each ABC Installation is designed as a separate and independent network which includes all verification modules, Access Control Modules, Monitoring Stations and Level 2 controls of the installation.

It is RECOMMENDED that each ABC Installation is connected to the Central Server and any other external systems through a single point.

It is RECOMMENDED for the Central Server (Application Server and Databases) of the System to be isolated from external systems through the adequate gateways and firewall equipment.

Designers MAY choose to centralise the Application Server and Databases for all ABC installations or to replicate them for different installations, depending on such constraints as communication link reliability from central systems to Border Crossing Points (BCPs), number of ABC installations in the country and their location, legal requirements on personal data storage and retention etc. If de-centralisation is chosen, it is RECOMMENDED that the software update rollout service to be kept centralised.

Architecture of the Central Server

The RECOMMENDED application server and central databases high-level architecture is shown in Figure 6 - Central Server High-Level Architecture. As it is usual in these systems, an application layer supported by a persistence/database layer are identified.

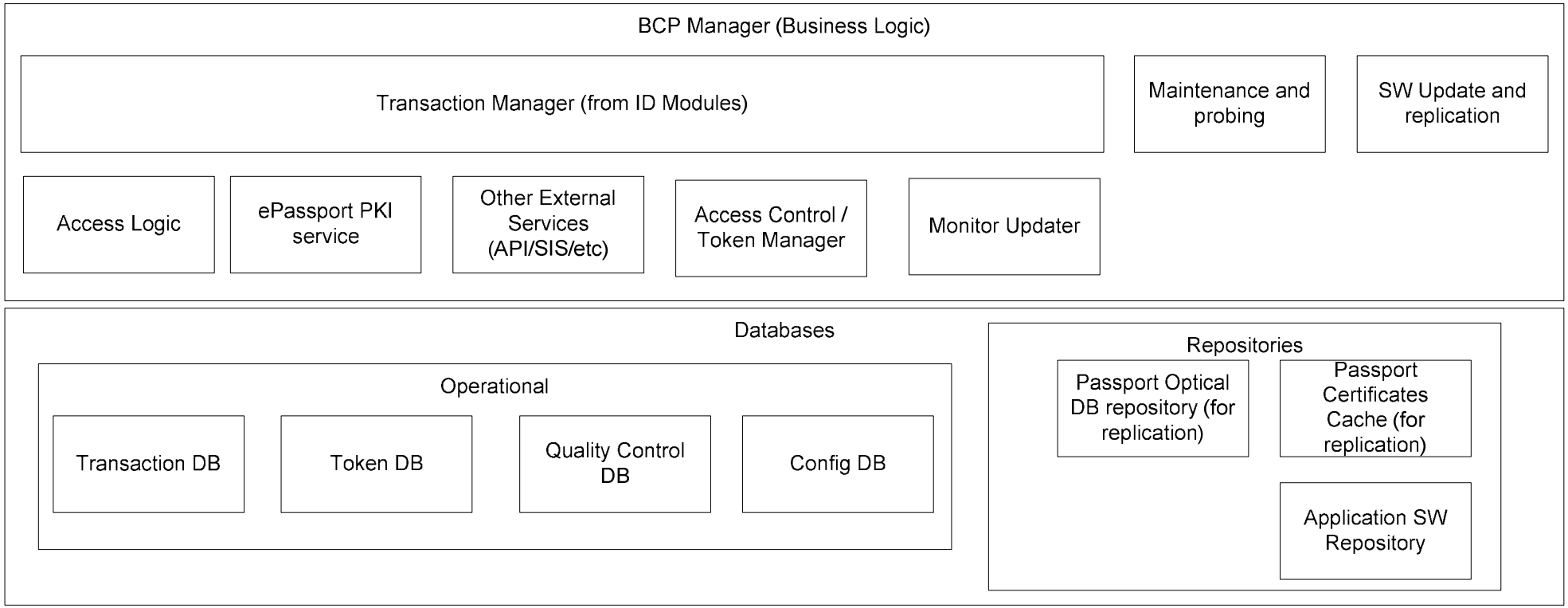


Figure 6 - Central Server High-Level Architecture

Table 1 - Central Server Application Block Description shows a brief description of each of the RECOMMENDED blocks within the application/business logic layer.

Block Name	Description
Transaction manager	Manages the creation and update of ID processes which started at the gates. This service makes use of underlying services to complete all the checks for an ID process (e.g. background checks) and then applies the Access Logic to the results in order to grant/deny access to the traveller.
Access Logic	Decision matrix implementing the operational aspects on traveller management, depending on the results obtained from all performed checks.
ePassport PKI service	If no direct access exists from the gates to the ePassport PKI, this service manages connection to the PKI for certificate updates and any other functionality offered by the national ePassport PKI.
Other external services	Manages connection and queries to other external system which may be necessary to perform all ID checks on a traveller (e.g. lost and stolen documents queries and other background checks).
Access Control/ Token Manager	In those ABC installations requiring access tokens (kiosk + separate gate installations), this service manages both logging of issued/captured tokens as well as the verification of tokens presented by travellers at the access modules (e.g. if fingerprints are captured as token on the ID modules, this service manages the stored fingerprint database, along with the 1:N biometric identification matcher for fingerprints presented at the access module). Note that in cases where many access modules are controlled by the same server, performance MAY be improved by relocating the identification part of this service directly in the Access Modules.
Monitor Updater	Service in charge of ensuring that each monitoring station receives all relevant information it is entitled to. If the monitoring stations are allowed to poll directly to the transaction and configuration databases, this service MAY be a simple transparent connection to these databases.
Maintenance and probing	Service retrieving the status from all the components (Access and verification modules) controlled by the server.
SW Update service.	This service MUST be present in the central server to manager the deployment of new SW versions, passport optical pattern databases and, if necessary, certificate lists across all the elements controlled by the server.

Table 1 - Central Server Application Block Description

In order to facilitate the implementation of the central services, it is RECOMMENDED to include at least the databases/data storage services described in Table 2 - Central Server Database Description within the central server of the ABC system. Note that the database taxonomy depicted in this document seeks to illustrate minimum data storage and management requirements, the designer MAY choose to merge two or more of the databases into overarching databases:

Block Name	Description
Transaction Database	Temporary database where all details from an ongoing verification process are kept. In order to simplify scalability it is RECOMMENDED that all details from a verification process are temporarily stored within a transaction database. This allows for monitoring stations to asynchronously poll for relevant information from gates under its supervision. The exact contents of a transaction database entry depend on operational requirements and thus are out of the scope of this section of the document. Nevertheless, it is RECOMMENDED that all data within this database is only temporarily stored, that is, successful verification processes SHOULD be deleted after a delay, whereas information from unsuccessful ones MUST only be kept IN MEMORY until the Border Guard has acted upon them accordingly to process the traveller, and only for this reason.
Configuration Database	It is RECOMMENDED that this database covers the following: • The full configuration tree of ABC installations, along with their updated status to be stored in this database. • The association between monitoring stations and groups of gates. • User logging and authentication data. • Operational parameters for each installation and type of traveller (e.g. biometric thresholds for a given nationality or type of document, timeout for a given installation depending on its layout, etc.)
Quality Control and Business Statistics Database	It is RECOMMENDED that the ABC system stores non-confidential/non-personal data on the transactions (verification processes) which have taken place in the system. The minimum recommended data to be logged is described in more detail in section [EXTERNAL REFERENCE] of this document.

Block Name	Description
Access Token Database	For those installations where a token is issued to allow for the travellers to actually cross the border through the access modules, it is RECOMMENDED that token management and storage is kept in a central database. Depending on the type of token, this database MAY include fingerprint or other biometric details of the traveller, serial numbers of physical tokens, etc.
Passport Optical Pattern Repository	In order to maintain consistency in the optical checks performed in all ABC installations, a central pattern database MUST be maintained. This would be the single modification point when modifying optical pattern checks, while the SW update services would manage replication across all gates.
Passport Certificates Cache	If direct access to the Passport PKI from the gates is not allowed, it is RECOMMENDED that a central cache of relevant certificates is kept in the central servers. The SW update services would manage replication across all gates.
Application SW Repository	The current version of all SW pieces of the ABC system MUST be stored here to enable its deployment. It is RECOMMENDED that past versions of all the SW components within the ABC are also kept in a central database.

Table 2 - Central Server Database Description

Architecture of the ABC Installation at the BCP

An example of a RECOMMENDED basic architecture for the ABC Installation at the border crossing point can be seen on Figure 5 - High-level architecture. As shown, the following blocks are identified:

- Verification Modules (document authentication and biometric verification HW/SW)
- Access Modules
- Monitoring stations
- Level 2 stations

Verification modules

Verification Modules are the main point of traveller interaction with the system Figure 7 - Verification Module High-Level Architecture shows a simplified version of the RECOMMENDED internal architecture of the Verification Module. Table 3. Verification Module Application Block Descriptionshows a brief description of each block.

It is RECOMMENDED that passport reading and authentication and Biometric verification take place in this logic block of the system. Note that no preference is stated on whether these processes have to be implemented in a single step or in two different steps/locations of the Verification Module.

For installations where an Identification token is required (i.e. for kiosk and separate gate installations), access token generation (if physical) or token capture functionalities MUST be integrated within the verification module. Token management SHOULD NOT be done at the Verification module but at the Application Server (or alternatively at the Access Module if required due to performance limitations).

The Verification modules SHOULD NOT implement by themselves the access logic, nor access external systems directly. Designers MAY choose to directly access the ePassport PKI for certificate updates from the verification modules.

The Verification modules SHOULD NOT log any quality control data by themselves, other than debug and maintenance logs, but SHOULD relay all such data to the Central Server.

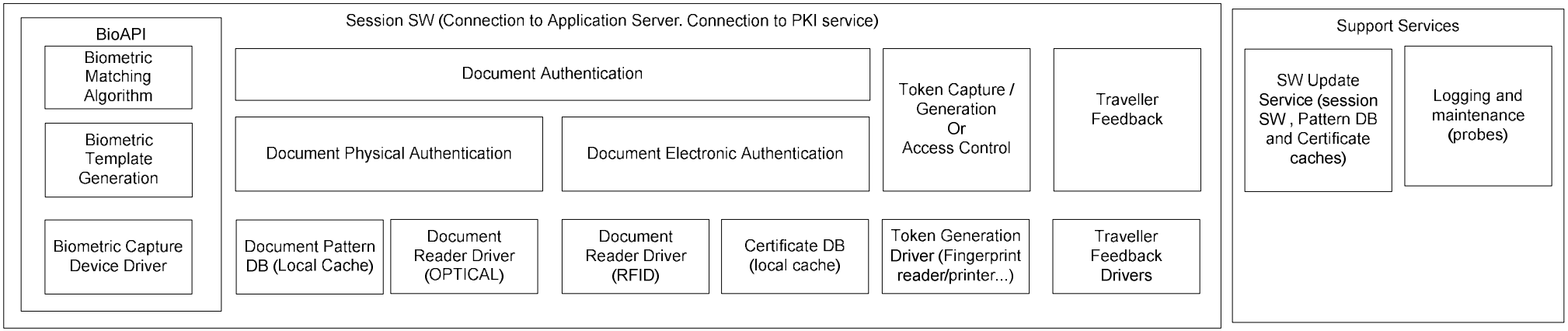


Figure 7 - Verification Module High-Level Architecture

Block Name	Description
Session SW	Session and connection to Central Server manager for regular operation of the system, including transaction messaging, etc.
BioAPI	Biometric verification stack. BioAPI compliant stacks are RECOMMENDED, but the designer MAY make use of vendor specific SDKs for biometric capture, processing and verification.
Document Authentication	Covering both optical and electronic checks. The Verification module SHOULD contain a local cache of the optical pattern database and the certificate list for document verification. The Verification Module MAY connect directly to the PKI service for certificate list updates (and to enable future expansion for supporting TA for 2nd generation passports).
Token capture/generation Access Control	For kiosk and gate systems, access token generation/capture MUST be implemented at the Verification Module. If no token generation is required, it is RECOMMENDED that access module control is implemented as part of the Verification Module (integrated 1-step o 2-step mantrap or single gate).
Feedback units	All messaging with the traveller.
SW Update service.	This service MUST be present in the Verification Module to allow for consistency in the updates of the verification SW and optical patterns database. If the Verification module does not connect directly to the Passport PKI, this service MUST also manage the update of the certificate list from the Application server.
Logging and maintenance.	The Verification module MUST include logging functionalities to enable maintenance and supervision. It is RECOMMENDED that the module communicates its status to the Central Server, to simplify maintenance and supervision of the deployment.

Table 3. Verification Module Application Block Description

Access modules

Where required, access modules MAY implement specific functionalities for token management (i.e. in a kiosk + separate gate scenario).

To avoid unnecessary delays and communication loops, it is RECOMMENDED this block is as integrated with the Verification Module as possible (as in the case of a tightly integrated mantrap); if possible, the designer MAY choose not separate Access Module intelligence from the Verification Module functionalities.

The Access modules SHOULD NOT log any quality control data by themselves, other than debug and maintenance logs, but SHOULD relay all such data to the Application Server.

Monitoring stations

Monitoring stations are the main point for interaction of the Border Guard with the system. Figure 8 - Monitoring Station High-level architecture shows a simplified version of the minimum RECOMMENDED internal architecture of the Monitoring Station. Table 4. Monitoring Application Block Description shows a brief description of each block.

To simplify the management of scalability, it is RECOMMENDED that each monitoring station can be associated (through the Configuration DB in the central server) with a given range of gates.

It is RECOMMENDED that the monitoring station acts as the start-up point for a given installation, in the sense that by starting the monitoring station, the Border Guard can also start all associated gates.

It is RECOMMENDED that the monitoring stations can control the Verification and Access Modules even if the Central Server is not reachable (e.g. for emergency gate management).

In order to simplify software and performance requirements for the application servers, it is RECOMMENDED that the monitoring station polls the Central Server for transactions of interest (Border Crossings), rather than the Central Server actively send such information.

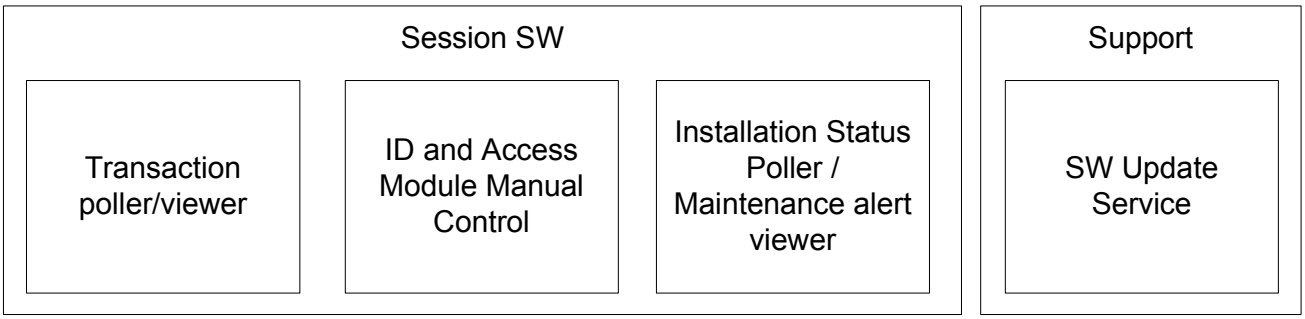


Figure 8 - Monitoring Station High-level architecture

Block Name	Description
Session SW	Session and connection to Central Server manager for regular operation of the system, including transaction messaging, etc
Transaction poller/viewer	Service polling for transactions occurring in the ABC system gates controlled by the monitoring station.
Installation Status Poller /Maintenance alert viewer	Service retrieving the status from all the components (Access and verification modules) controlled by the station.
Verification and Access Module Manual Control	Service for remotely controlling the status of all verification and access modules controlled by the station. The service MUST offer enable/disable control for each separate module. It is RECOMMENDED that the service allows for manual control of the access modules.
SW Update service.	This service MUST be present in the Monitoring Station to allow for consistency in the updates across all ABC installations.

Table 4. Monitoring Application Block Description

Level 2 stations

If Level 2 stations functionality is required, they MAY be integrated with the ABC installation through the Central Server (transaction database), so that details of a traveller being double checked can be retrieved if necessary.

Basic Dataflow

In order to illustrate the rationale behind the RECOMMENDED architecture, the following example dataflow diagrams are provided:

- Opening of a session from a Monitoring Station
- Closing of a session from a Monitoring Station
- Successful verification process in a single gate or mantrap ABC installation
- Successful verification process in a kiosk ABC installation.

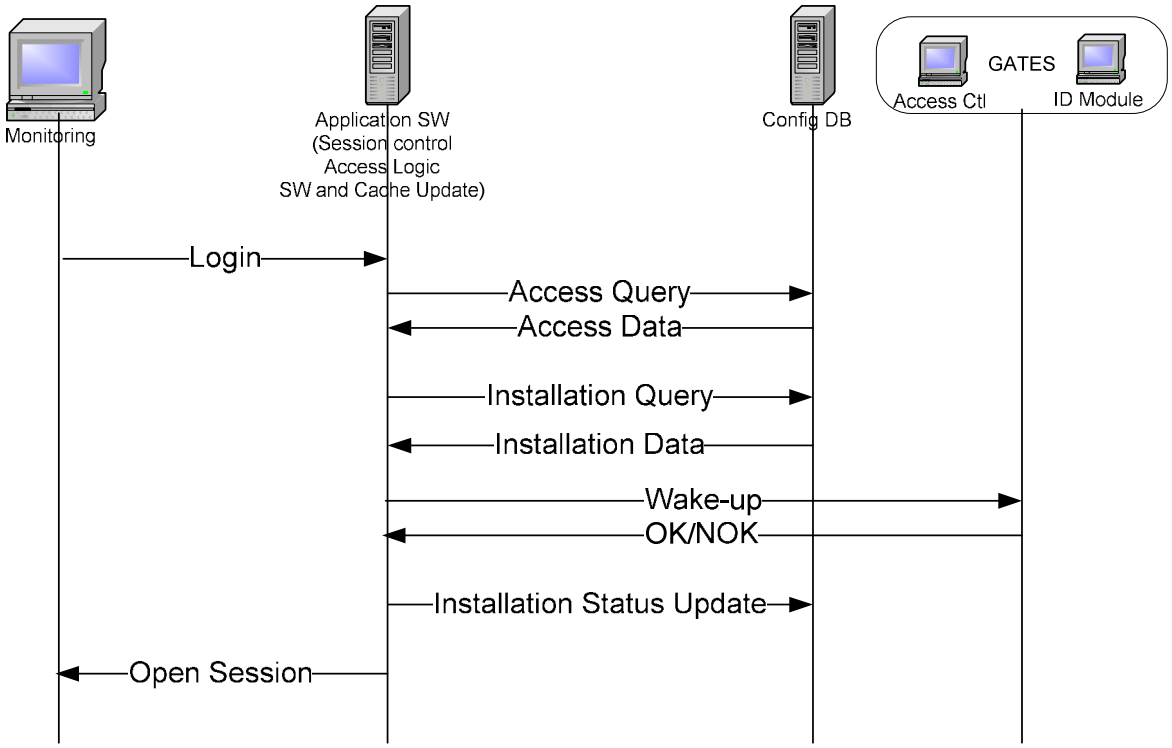


Figure 9 - Opening of a session from a Monitoring Station

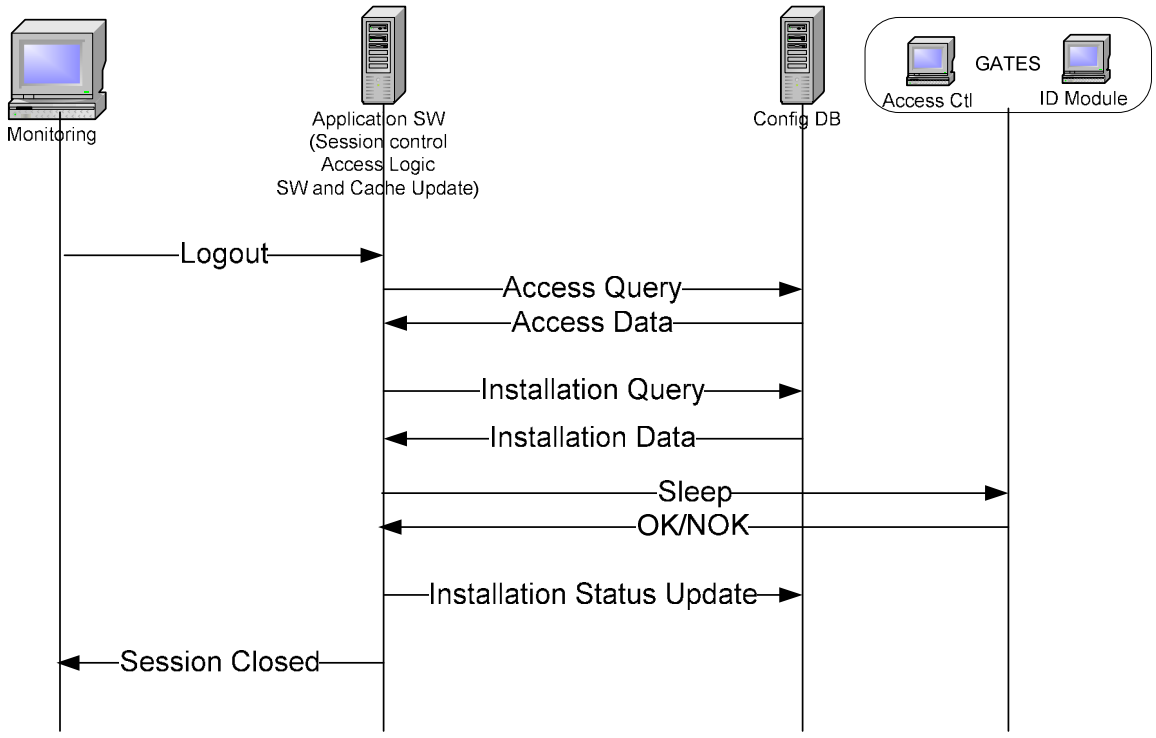


Figure 10 - Closing of a session from a Monitoring Station

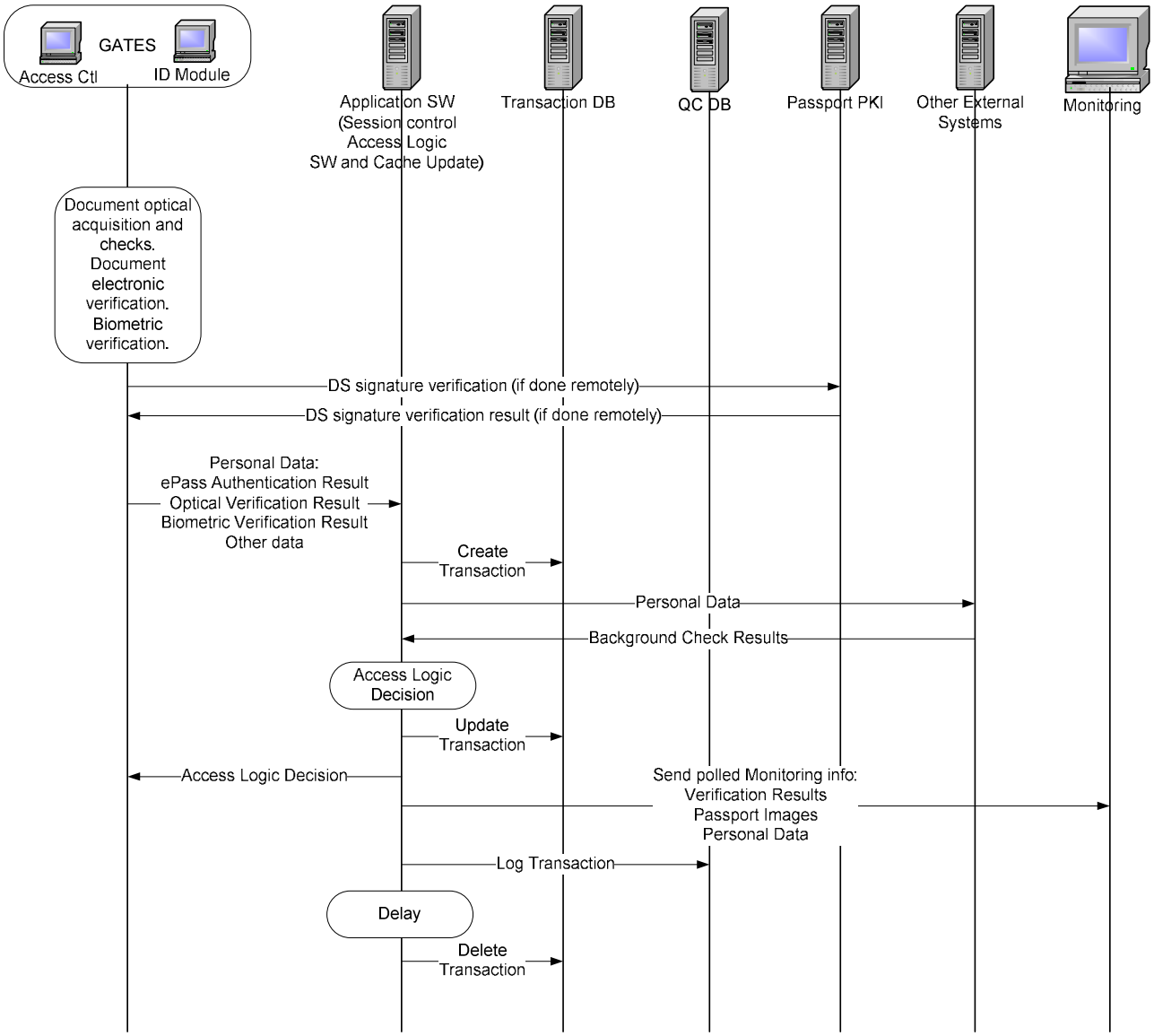


Figure 11 - Successful verification process in a single gate or mantrap ABC installation. Note that continuous polling from the Monitoring Station is not shown.

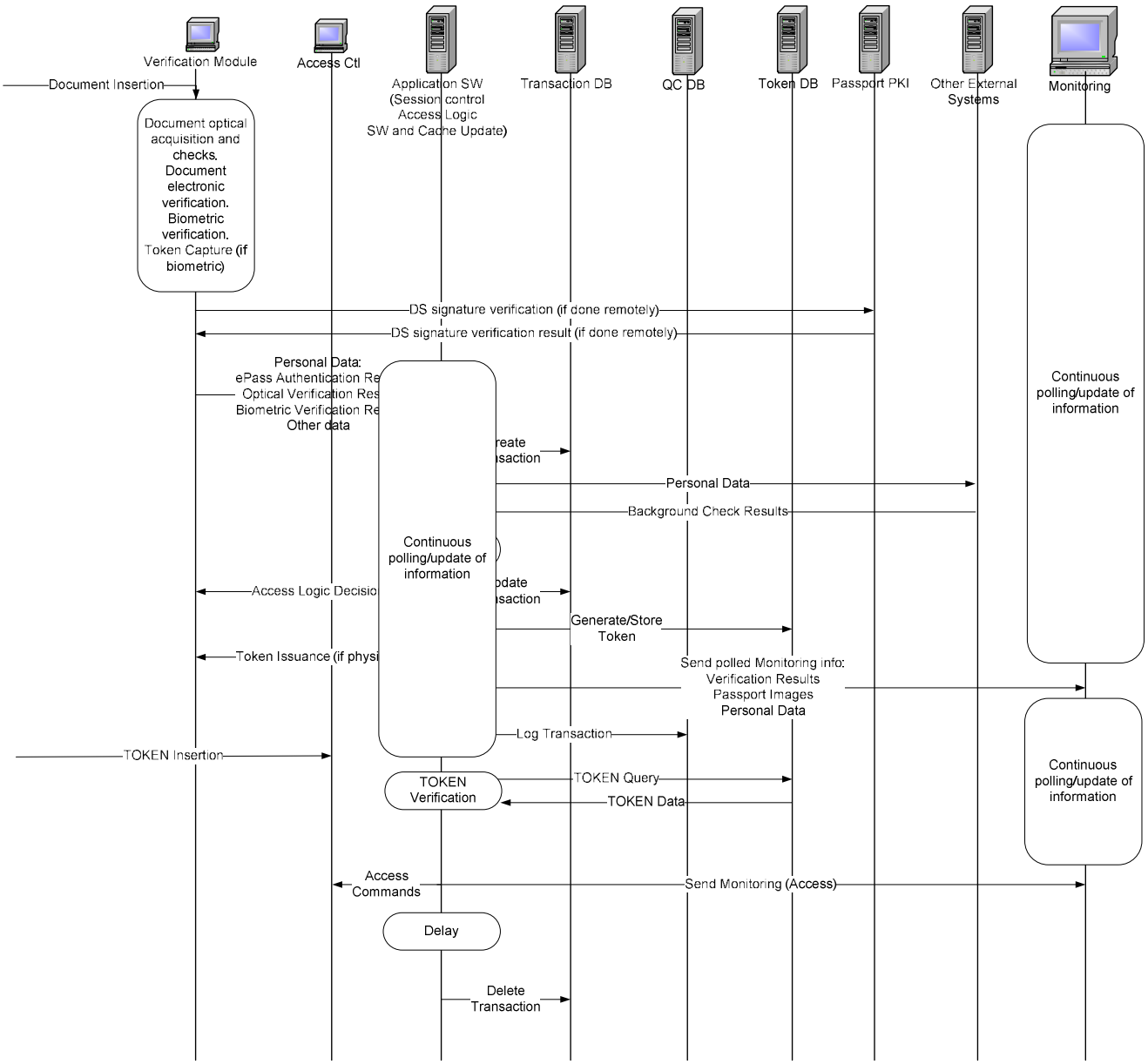


Figure 12 - Successful verification process in a kiosk ABC installation. Note that continuous polling from the Monitoring Station is not shown.

ANNEX 2: ADDITIONAL READING

Biometrics

This section lists additional, public available references on biometrics for ABC systems.

Software Architecture	An example for detailed requirements on the software architecture can be found in [BSI03121-1] and [BSI03121-2].
Process of Biometric Verification	An example for detailed requirements on the process of biometric verification based on live captured face images can be found in [BSI03121-2], section "Verification ePassport and Identity Card using facial biometrics" and [BSI03121-3], section "P-PH-VID".
Face Capture Unit	An example for detailed requirements on the functionality of the face capture unit can be found in [BSI03121-3], sections "BIP-PH-VID", "QA-PH-VID", and "COM-PH-VID".
Operational Issues	An example for detailed requirements on the operational issues and can be found in [BSI03121-3], section "O-PH-VID".
User Interface	An example for detailed requirements on the user interfaces can be found in [BSI03121-3], section "UI-PH-VID".
Evaluation of Error Rates	An example workflow and architecture for obtaining impostor and genuine comparison scores for calculating FAR and FRR is described in [BSI03121-3], section "P-PH-VID".
Quality Control and Business Statistics	An example for a detailed logging scheme can be found in [BSI03121-3], sections "COD-PH-VID", and "LOG-PH-VID".

Certification of document readers

This section lists additional, publicly available references on document readers and document authentication processes for ABC systems.

In order to verify the compliance of an eMRTD authentication sub-systems (e.g. electronic document reader hard- and software) to the relevant ISO and ICAO standards (especially [ISO14443], [ISO7816] and [ICAO9303]) it is common to rely on established evaluation and certification schemes. Examples for

independent or official evaluation and certification schemes are [BSI03105-4] and [BSI03105-51].

ANNEX 3: REFERENCES

[BSI03105-4] Federal Office for Information Security: Technical Guideline TR-03105 – Conformity Tests for Official Electronic ID Documents, Part 4: Test plan for ICAO compliant Proximity Coupling Device (PCD) on Layer 2-4, Version 2.2

http://www.bsi.bund.de/ContentBSI/EN/Publications/Techguidelines/TR03105/BSITR03105.html

[BSI03105-51] Federal Office for Information Security: Technical Guideline TR-03105 – Conformity Tests for Official Electronic ID Documents, Part 5.1: Test plan for ICAO compliant Inspection Systems with EAC 1.11, Version 1.2

http://www.bsi.bund.de/ContentBSI/EN/Publications/Techguidelines/TR03105/BSITR03105.html

[BSI03110] Federal Office for Information Security: Technical Guideline TR-03110 – Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Version 1.11

http://www.bsi.bund.de/ContentBSI/EN/Publications/Techguidelines/TR03110/BSITR03110.html

[BSI03121-1] Federal Office for Information Security: Technical Guideline TR-03121 – Biometrics for Public Sector Applications, Part 1: Framework, Version 2.1

http://www.bsi.bund.de/ContentBSI/EN/Publications/Techguidelines/TR03121/BSITR03121.html

[BSI03121-2] Federal Office for Information Security: Technical Guideline TR-03121 – Biometrics for Public Sector Applications, Part 2: Software Architecture and Application Profiles, Version 2.1

http://www.bsi.bund.de/ContentBSI/EN/Publications/Techguidelines/TR03121/BSITR03121.html

[BSI03121-3] Federal Office for Information Security: Technical Guideline TR-03121 – Biometrics for Public Sector Applications, Part 3: Function Modules, Version 2.1

http://www.bsi.bund.de/ContentBSI/EN/Publications/Techguidelines/TR03121/BSITR03121.html

[ICAO9303] International Civil Aviation Organization: Doc9303 – Machine Readable Travel Documents, Part 1 Vol. 2 and Part 3 Vol. 2

http://www.icao.int/mrtd

[ISO7816] Identification cards - Integrated circuit cards

http://www.iso.org

[ISO14443] Identification cards - Contactless integrated circuit cards - Proximity cards

http://www.iso.org

[ISO19784-1] ISO/IEC 19784-1:2006, Information technology -- Biometric application programming interface -- Part 1: BioAPI specification

[ISO19794-5] ISO/IEC 19794-5:2005, Information technology -- Biometric data interchange formats -- Part 5: Face image data

[RFC3369] RFC 3369, Cryptographic Message Syntax (CMS), August 2002

http://www.ietf.org/rfc/rfc3369.txt

FRONTEX
LIBERTAS SECURITAS JUSTITIA

Rondo ONZ 1, 00 124 Warsaw, Poland
Telephone +48 22 544 95 00, Fax +48 22 544 95 01

European Agency for the Management of Operational Cooperation at the External Borders
of the Member States of the European Union