European Commission

JRC TECHNICAL REPORTS

Security of Automated Border Control

Handbook of Vulnerabilities

Günter Schumacher
Sebastian Zehetbauer
Stefan Brandl
Sirra Toivonnen
Andreas Kriechbaum-Zabini
Arndt Bonitz

2017

Distribution List:
Günter Schumacher, JRC E6
Jan Löschner, JRC E6
Alessandra Zampieri, JRC E6
Thomas Barbas, JRC E6
Dario Tarchi, JRC E6
Richard Rinkens, DG HOME B3
Marc Sulon, DG HOME B3
Philippe van Triel, DG HOME B3
Rob Rozenburg, DG HOME B3
Johannes de Ceuster, DG HOME C2
Oliver Seiffarth, DG HOME C2
Edgar Beugels, FRONTEX
Rasa Karbauskaite, FRONTEX
Dragos Voicu, FRONTEX
Jorge Silva Rodrigues, FRONTEX
Tom van der Hor, FRONTEX
Ciaran Carolan, eu-LISA
Sebastian Zehetbauer, Österreichische Staatsdruckerei
Stefan Brandl, Österreichische Staatsdruckerei
Florian Humplik, Österreichische Staatsdruckerei
Sirra Toivonnen, VTT
Andreas Kriechbaum-Zabini (AIT)
Arndt Bonitz (AIT)
Markus Nuppeney, Bundesamt für die Sicherheit in der Informationstechnik
Maik Rudolf, Bundespolizei Germany
Antonino Passarelli, Ministero dell'Interno, Italia
Angela De Santis, Polizia di Stato, Italia
Ted Dunstone, Biometix

FastPass Consortium

Contact information
Name: Günter Schumacher
Address: Joint Research Centre, Via E. Fermi, 21027 Ispra, Italy
E-mail: Guenter.Schumacher@jrc.ec.europa.eu
Tel.: +39 0332 786085

JRC Science Hub
https://ec.europa.eu/jrc

JRC 105848

Contents

Executive Summary

With an ever increasing number of Schengen border crossings per year, Automated Border Control (ABC) has been introduced in order to facilitate border control of legitimate travellers. Whilst control for authorised persons should be as efficient as possible, with minimum human intervention, the control process shall remain as secure as is has been in the past. Moreover, as ABC-enhanced control implicitly validates optical and electronic parts of travel documents, there should even be a gain in security.

However, reality looks different. First of all, the systematic usage of inspection devices for travel documents does not per se exclude potential fraud. There exist already a large number of excellent falsified passports that can pass all checks of a particular inspection device if that device is not regularly updated to cover the latest known falsifications.

Secondly, and more serious, ABC systems are up to now still deployed without a systematic check against its vulnerabilities. The research of the European FastPass project has revealed the impressive number of some 100 vulnerabilities of a (generic) ABC system. This is not really a surprise. Any security system with a similar number of technical elements (both physical and electronic) is likely to have such a number of vulnerabilities. Some of them are more obvious, some are less obvious. The mentioned problem with falsified documents is clearly an obvious one. But is the operator of an ABC therefore aware of the need for regular updates (and training of personnel) regarding the latest attacks? – An example of a less obvious vulnerability is the potential distraction of the supervising border guard through the creation of an exceptional situation by an attacker in one ABC-gate, while a second attacker is exploiting the distraction in another ABC-gate that is supervised by the same border guard. Again, awareness is key to address this vulnerability.

The current report provides a kind of handbook for practitioners in Automated Border Control (ABC) with respect to security. It contains a list of known vulnerabilities of an ABC system and additional information to understand its relevance and potential countermeasures. The document is meant to serve as check list for operators during the deployment of ABC systems.

The authors believe that continuous awareness about the potential vulnerabilities is more important than any formal certification of security. Apart from the fact that such certification schemes do not exist of ABC system, certification would in any case only allow limited conclusions about the resilience of a system. Any software update, any new falsified passport, any new concept to attack an ABC would not be covered by certification done before. From a risk management point of view, it is therefore much more effective to keep the awareness on the vulnerabilities continuously alive, with flexible countermeasures and regular reality checks.

It shall not be excluded that a subset of the vulnerabilities listed here may be covered in the future by a more formal evaluation scheme. The subset could then be validated by independent authorities before deployment. However, more practical experience in the handling of the current assessment scheme is needed to identify such a subset.

1 Introduction

One of the major factors for security and mobility within the EU is border control. Travellers wish to cross external borders with maximum convenience, whilst, on the other hand, there is the need for securing EU's borders against illegal immigration, terrorism, crime and other threats. Since about 2009, an increasing number of so-called Automated Border Control (ABC) systems support this requests for convenience and security. Based on Machine Readable Travel Documents (MRTD), ABC allows legitimate travellers to pass the border through automated gateways ("eGate"). Authorisation is established through comparison of the face image stored electronically in the passport with a live image taken in the eGate (see Figure 1).

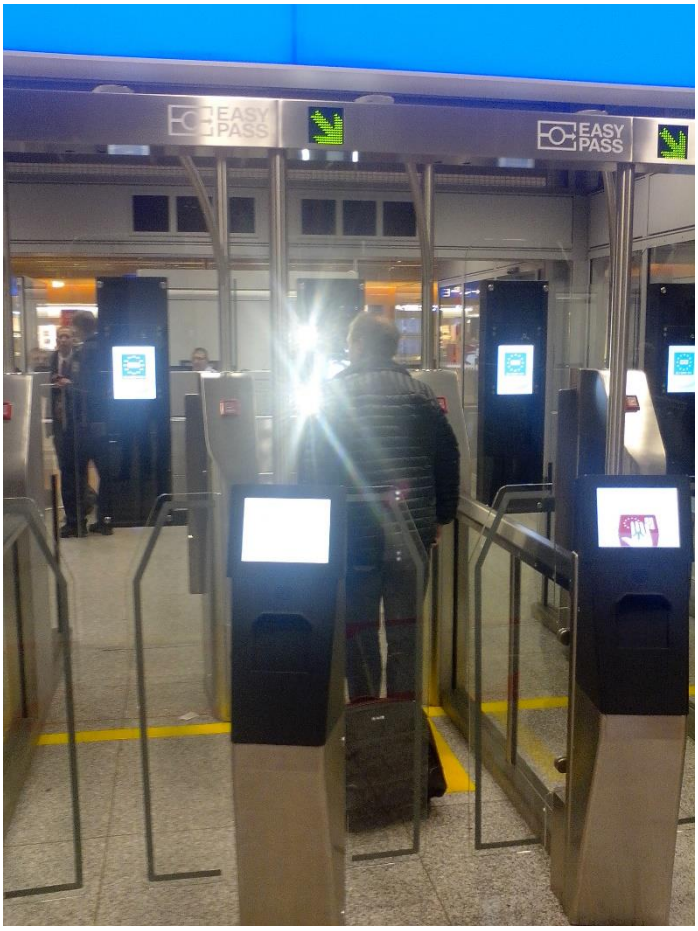


Figure 1: ABC at Frankfurt Airport ("EASYPASS")

The European Commission has addressed this situation through the integration of ABC into its recent proposal COM(2016) 196[1] to revise Schengen Borders Code. For the first time, a clear definition of ABC has been introduced and its usage integrated into border control practices. The proposal constitutes an important element of the overall Smart Borders[2] Initiative as set out in a relevant communication already in 2008[3].

[1] Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2016/399 as regards the use of the Entry/Exit System http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/securing-eu-borders/legal-documents/docs/20160406/regulation_proposal_entryexit_system_en.pdf

[2] http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/smart-borders/index_en.htm

[3] Preparing the next steps in border management in the European Union. COM(2008) 69 final. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52008DC0069&from=EN

Following this vision, FRONTEX started in 2010 to establish an informal Member States committee to discuss and share best practices on the usage of ABC in Europe ("FRONTEX ABC Working Group"). This activity has led to a series of relevant best practice guidelines:

- Best Practice Guidelines on the Design, Deployment and Operation of Automated Border Crossing Systems (2011)[4]
- Best Practice Technical Guidelines for Automated Border Control (ABC) Systems (2012, revised 2015)[5]
- Best Practice Operational Guidelines for Automated Border Control (ABC) Systems (2012, revised 2015)[6]
- Guidelines for Processing of Third Country Nationals through Automated Border Control (2013)[7]

Yet, the in-depth consideration of an ABC system as a **security system** is missing. All the available best practices released so far address functionality, design and proper operation only. The current situation as of 2016 is that deployment of ABC in Europe is done without particular analysis of potential vulnerabilities, at least there is no harmonised or otherwise shared methodology around.

This gap had been addressed by the European FastPass project[8] between 2013 and 2016. While focussing on harmonisation of ABC systems across air, sea and land borders, particular attention was put on a more systematic view to security and data protection. This resulted in the identification of some 100 vulnerabilities of an ABC system that is integrated into a border control process [1].

Even though the analysis done in FastPass is based on a particular ABC model architecture for land, sea and air borders, most of the vulnerabilities are of generic nature that apply to any known ABC system today. The purpose of this document is to make this list of generic vulnerabilities available to practitioners in the following way:

- Detailed explanation of vulnerabilities in the context of an ABC system, including potential countermeasures
- Self-assessment questionnaire to understand the relevance of these vulnerabilities for a specific installation

[4] http://frontex.europa.eu/assets/Publications/Research/ABC_Best_Practice_Guidelines.pdf
[5] http://frontex.europa.eu/assets/Publications/Research/Best_Practice_Technical_Guidelines_ABC.pdf
[6] http://frontex.europa.eu/assets/Publications/Research/Best_Practice_Operational_Guidelines_ABC.pdf
[7] http://frontex.europa.eu/assets/Publications/Research/Guidelines_for_Processing_of_Third_Country_Nationals_through_ABC.pdf
[8] https://www.fastpass-project.eu/

2 The Classification Scheme Used

Vulnerabilities have been classified similar to STRIDE/DREAD[9] methodology for risk analysis (i.e. risk identification and quantitative risk analysis) [2]. Microsoft originally developed this method purely for software systems.

STRIDE provides a classification of threats where the letters stand for certain categories:

- S Spoofing identity
- T Tampering with data
- R Repudiation
- I Information disclosure
- D Denial of service
- E Elevation of privilege.

DREAD provides a scheme to score the impact of a threat and makes them comparable by their risk value. The letters stand for

- D Damage potential
- R Reproducibility
- E Exploitability
- A Affected users
- D Discoverability

STRIDE and DREAD provide a fast way to assess threats and risks and bears the potential to be adapted for non-IT-related domains such as an ABC system through an abstraction of "data flows". In any case, those models had to be tailored to the ABC domain, resulting into dedicated $\text{STRIDE}_{\text{FastPass}}$ and $\text{DREAD}_{\text{FastPass}}$ models. The $\text{STRIDE}_{\text{FastPass}}$ evolved to

- S Spoofing information
- T Tampering (comprises system, eMRTD, tokens, information, et.al.)
- H Hijacking
- I Information disclosure
- D Denial of service
- P Privilege escalation

For $\text{DREAD}_{\text{FastPass}}$, the number of categories were limited to only 2 (out of 5):

Damage Potential (D): what is the impact on the ABC system; comprises categories Damage, Affected users of the original DREAD model?

Exploitability (E): how easily can the attack be performed? Comprises categories Exploitability, Reproducibility, Discoverability of the original DREAD model.

FastPass proposed a scale to score Damage Potential (D) comprising three values:

1 … low: Short-term malfunction or failure of the eGate

2 … medium: Long-term malfunction or failure of the eGate; subject may overcome single security checks of the gate but not the complete process.

3 … high: The attacker can subvert the security system and pass through the eGate.

Likewise, the scale to score Exploitability (E) also has three values:

1 … low: The attack requires an extremely skilled person and in-depth knowledge of the eGate/ABC to exploit the system.

[9] https://msdn.microsoft.com/en-us/library/ff648644.aspx

2 … medium: Only skilled person is capable to replicate a known attack by repeating each of the steps.

3 … high: Even an unskilled person is capable to replicate a known attack by repeating each of the steps.

With regard to pure data flow within an ABC system, there exists as well a (freeware) tool support from Microsoft, called "Microsoft Threat Modelling Tool 2016" (see Figure 2). The tool both helps to identify threats related to data processing and to track its proper mitigation.

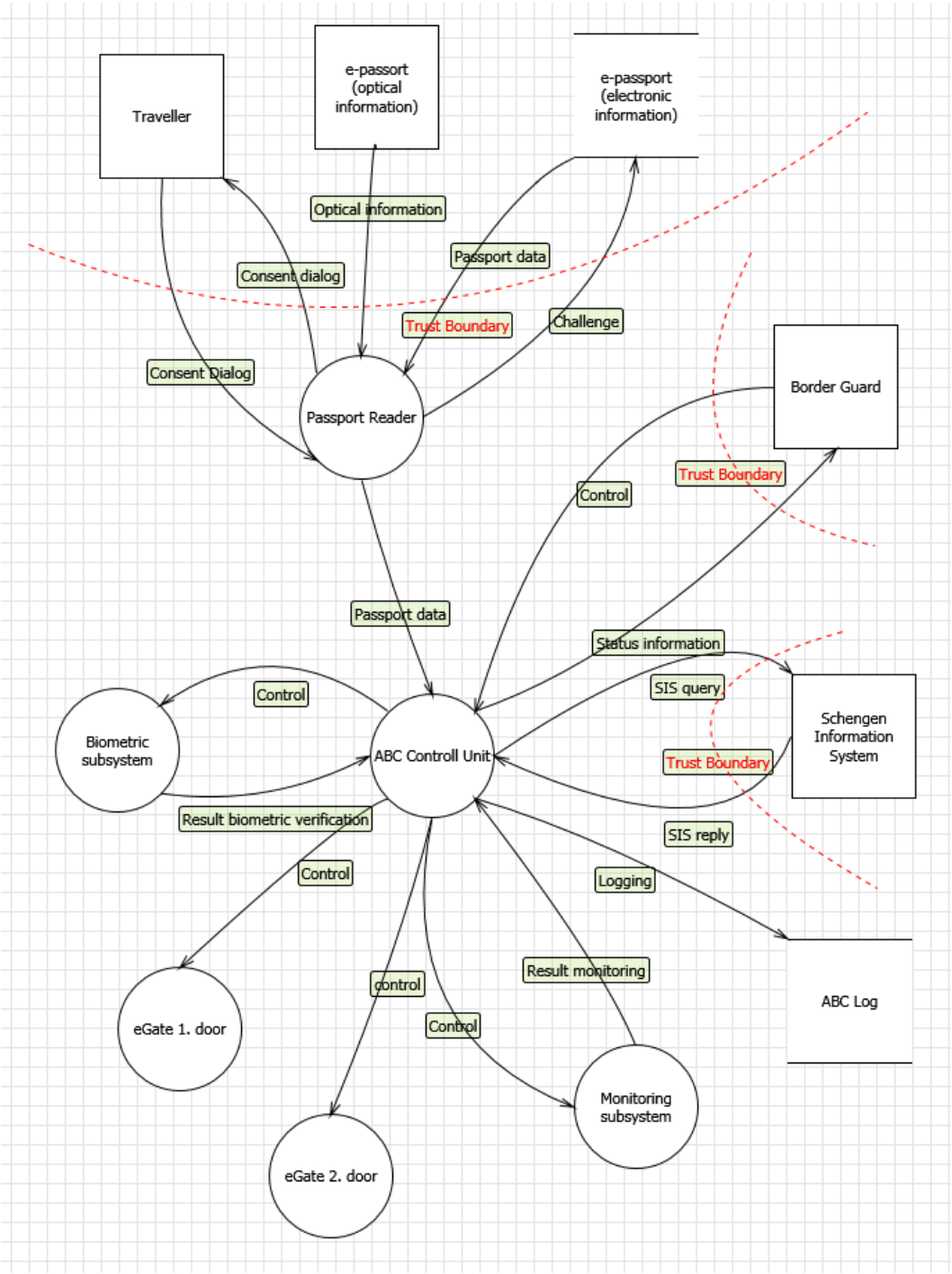
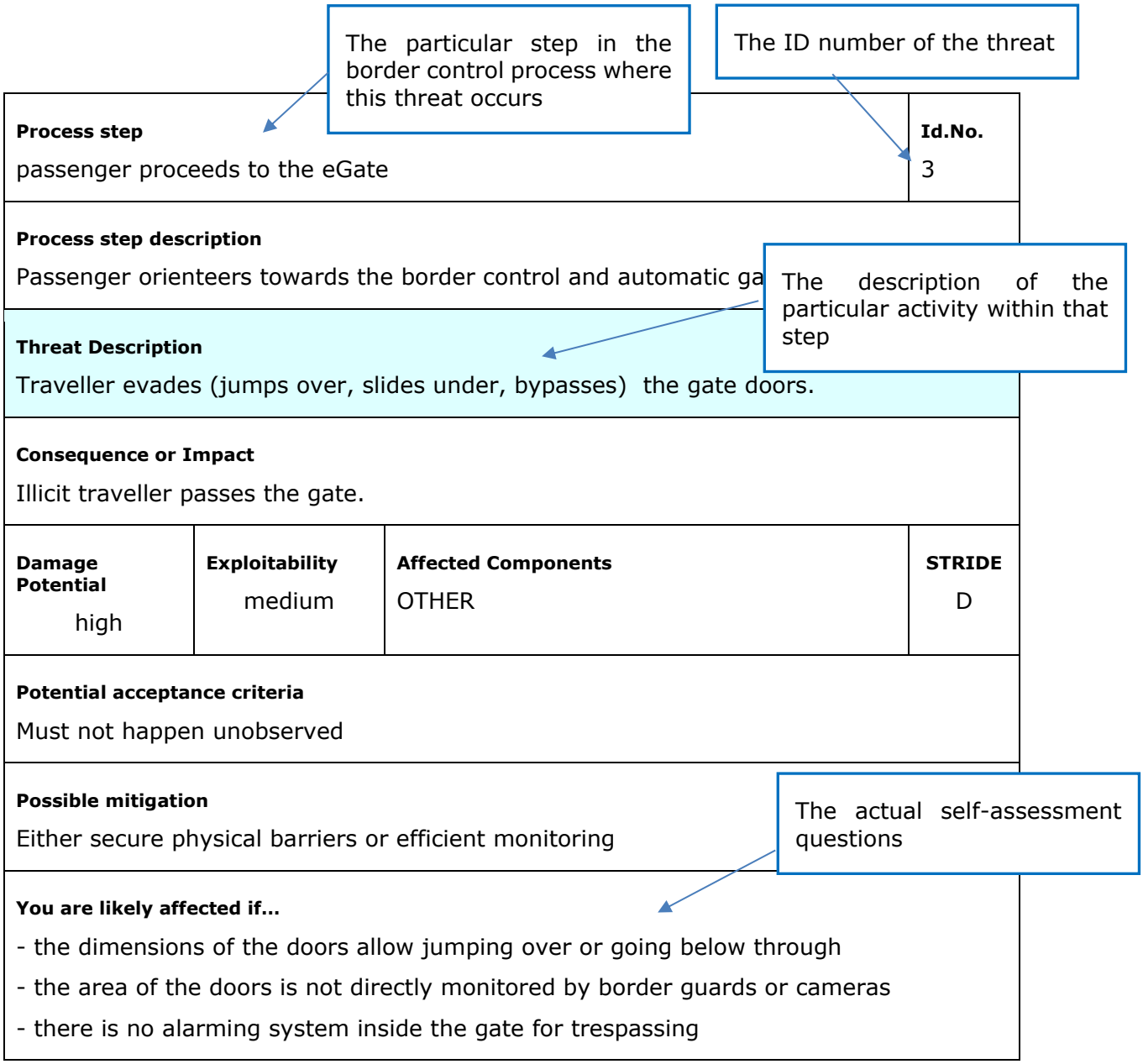


Figure 2: Data Flow Diagram of single step ABC

3 ABC Vulnerabilities

The following threat cards summarize for each threat the relevant information necessary for its understanding.

The cards are structured as the following example shows:



The pointer to the process step is in accordance with the following generic ABC enhanced border control process. The "single step" concept foresees that the traveller presents his/her passport directly at the eGate:

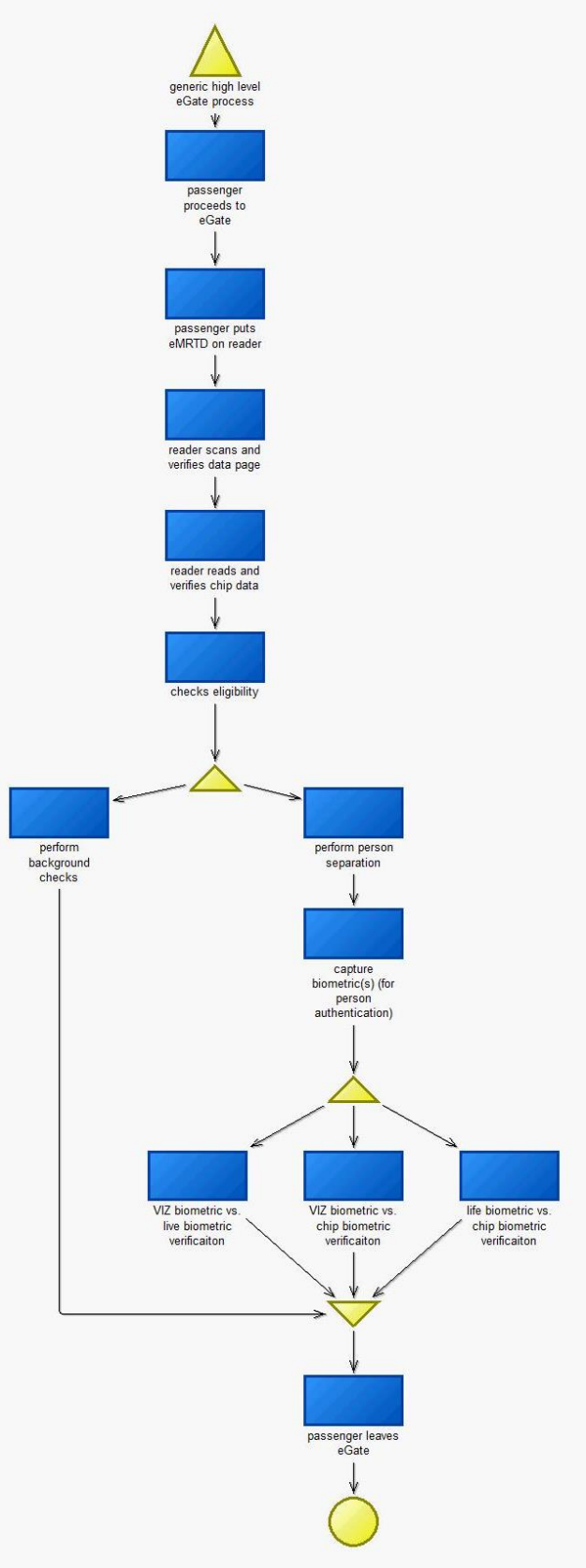


Figure 3: Single Step ABC

In contrast, the two-step concept foresees a pre-registration at a kiosk where basic information is already collected. Only then, the traveller proceeds to the eGate.

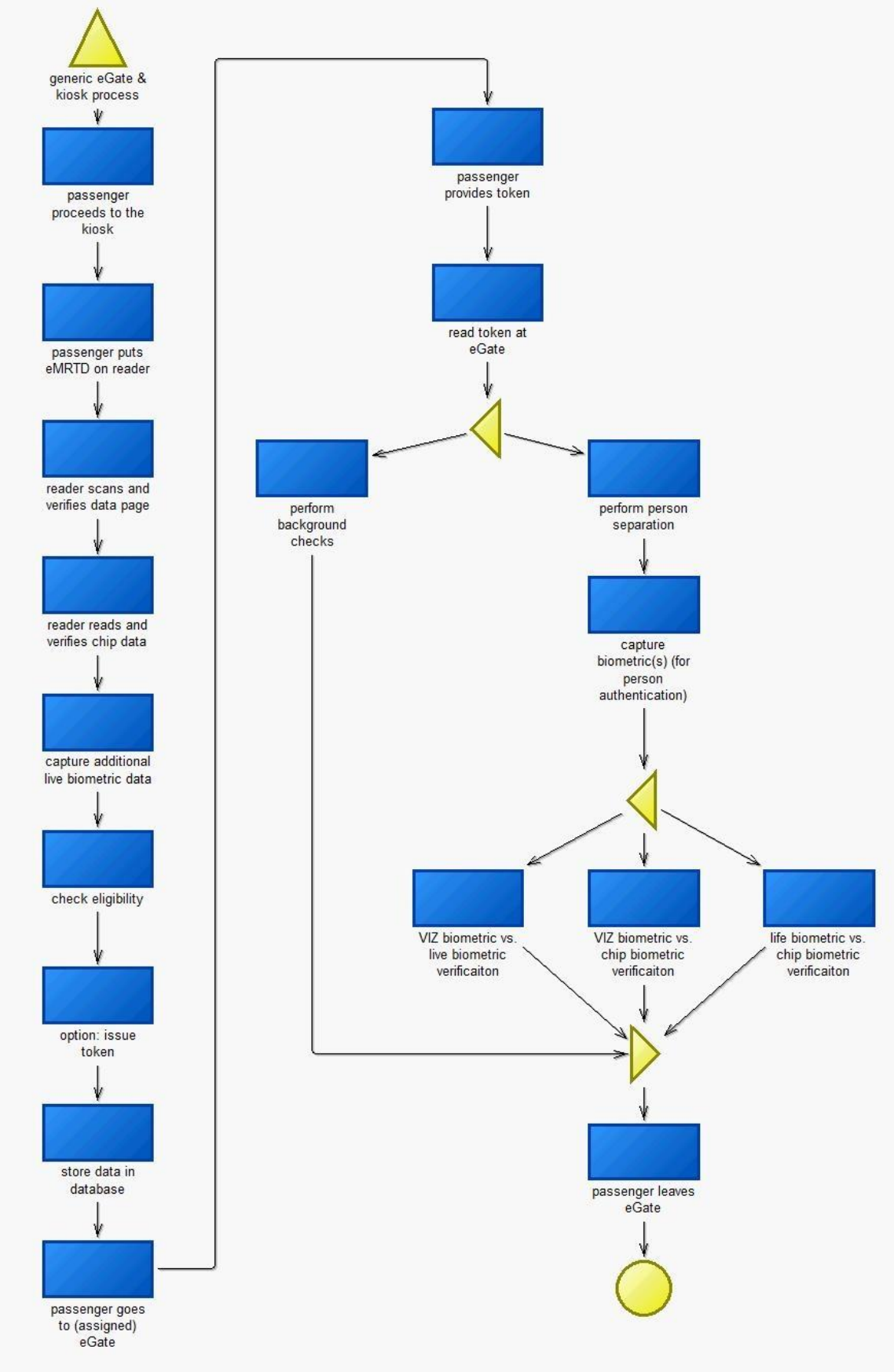


Figure 4: Segregated two-step ABC

Process step	**Id.No.**
passenger proceeds to the eGate	3

Process step description

Passenger orienteers towards the border control and automatic gates

Threat Description

Traveller evades (jumps over, slides under, bypasses) the gate doors.

Consequence or Impact

Illicit traveller passes the gate.

Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
high	medium	OTHER	D

Potential acceptance criteria

Must not happen unobserved

Possible mitigation

Either secure physical barriers or efficient monitoring

You are likely affected if...

- the dimensions of the doors allow jumping over or going below through
- the area of the doors is not directly monitored by border guards or cameras
- there is no alarming system inside the gate for trespassing

Process step			**Id.No.**
passenger proceeds to the eGate			4
Process step description			
Passenger orienteers towards the border control and automatic gates			
Threat Description			
The passenger damages the doors of the gate.			
Consequence or Impact			
Causes malfunction of the doors. Could allow illicit traveller to pass the gate.			
Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
low	high	HW	D
Potential acceptance criteria			
Must not happen unobserved			
Possible mitigation			
Use of appropriate materials, efficient monitoring and/or alarming.			
You are likely affected if…			
- there is no alarming system about broken doors - the area of the doors is not directly monitored by border guards or cameras			

Process step	**Id.No.**
passenger proceeds to the eGate	5

Process step description

Passenger orienteers towards the border control and automatic gates

Threat Description

Persons cause hassle on many of the gates in order that one could pass the gate without no-one noticing.

Consequence or Impact

Traveller passes the gate.

Border guard concentrates on the gate where the hassle is.

Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
high	low	OTHER	D

Potential acceptance criteria

Must not happen unobserved

Possible mitigation

Appropriate video monitoring; detection must be in accordance with state-of-the-art

You are likely affected if...

- the gate monitoring border guard has to supervise more than one gate
- there is no simple mechanism to stop traffic in the other gates

Process step	**Id.No.**
passenger puts eMRTD on reader	6

Process step description

Communication: Reader <=> Software

- Recognize document (Event: new document was put on reader)
- Support for the traveller

Threat Description

The reader is not working properly (soiled or damaged (e.g. vandalism))

Consequence or Impact

Exploiting non functioning of the reader, thus bypassing the whole verification process. E.g. in case of vulnarable reading process, non proper integration of reading device etc.

Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
low	high	HW	D

Potential acceptance criteria

Must not happen unobserved

Possible mitigation

Degree of soiling of device must be observed and in case of potential malfunction appropriate actions need to be taken

You are likely affected if…

- the passport reader does not have sufficient self-test capabilities
- the passport reader is not monitored otherwise
- the passport reader is not resilient against dirt or physical attacks

Process step	**Id.No.**
passenger puts eMRTD on reader	7

Process step description

Communication: Reader <=> Software

- Recognize document (Event: new document was put on reader)
- Support for the traveller

Threat Description

The reader is eavesdropped meaning the data is read from an unauthorized person and can therefore be used. (e.g. USB Device with access to the hardware of the document reader)

Consequence or Impact

Any type of eavesdropping, either cables connection to the reading device or wireless communication with passport chip or any other non shielded line inside the system

Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
medium	low	HW	S+T

Potential acceptance criteria

Must not happen unobserved, at least not with low effort

Possible mitigation

Access to any component must be clearly restricted (e.g. no access point in reach), appropriate encryption of data

You are likely affected if…

- the housing of the passport reader is not sufficiently protected
- the reader has a visible connection for external devices

Process step	**Id.No.**
passenger puts eMRTD on reader	8

Process step description

Communication: Reader <=> Software

- Recognize document (Event: new document was put on reader)
- Support for the traveller

Threat Description

The scanning process is made impossible in advance (e.g. put the document on the reader in the wrong way or removed the document too early) in order to avoid the ABC-control and change to the manual checking.

Consequence or Impact

Deliberate prevention of proper reading of the eMRTD, thus potentially bypassing electronic inspection

Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
medium	high	HW	S+T

Potential acceptance criteria

Not yet relevant because manual inspection always possible until now

Possible mitigation

Currently no action required

You are likely affected if...

- using an ABC gate is mandatory

Process step	**Id.No.**
passenger puts eMRTD on reader	9

Process step description

Interaction: Passenger <=> Reader:

- Present travel document to scanner in a right position according to the guidance provided.

Threat Description

Person inserts other objects in the passport reader on purpose (e.g. chewing gum).

Consequence or Impact

Maintance work

Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
low	high	HW	D

Potential acceptance criteria

Must not happen unobserved

Possible mitigation

Degree of soiling of device must be observed and in case of potential malfunction appropriate actions need to betaken

You are likely affected if…

- passport reader allows insertion of objects other than passports

Process step	**Id.No.**
reader scans & verifies data page	10

Process step description

Communication: Reader <=> Software

- optical scan datapage (IR, UV, WHITE)

- determine if the document ist authentic (sec. features, MRZ correct, document database)

Threat Description

A manipulated data page (changed optically or by physical manipulation) delivers information that leads to a misinterpretation "false acceptance" when reading the document. (e.g. manipulated name in MRZ delivers no match in a wanted-persons database etc.,

Consequence or Impact

Any kind of manipulation of MRZ encoding leading to wrong conclusions about the validity of the document; potentially exploiting particular properties of the reading device.

Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
medium	medium	SW	S+T

Potential acceptance criteria

Must be avoided

Possible mitigation

ICAO conform check must be performed in order to verify with electronic information

You are likely affected if...

- passport reader unable to detect all kind of manipulated data pages

Process step	**Id.No.**
reader scans & verifies data page	11

Process step description

Communication: Reader <=> Software

- optical scan datapage (IR, UV, WHITE)

- determine if the document ist authentic (sec. features, MRZ correct, document database)

Threat Description

A simulation of the datapage (e.g. usage of a mobile device) remains undetected (e.g. playback of the corresponding image sequences for IR, UV and visible light) -> usage of the digital simulation of the datapage of a genuine passport

Consequence or Impact

Replay attack, exploiting knowledge about the image processing inside the reader

Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
medium	low	HW+SW	T

Potential acceptance criteria

Must be avoided

Possible mitigation

Officer shall monitur object presented or anti-spoof protection of reader; random sequence of optical reading steps; reader does not allow the insertion of devices for replay attacks

You are likely affected if...

- passport reader not resilient against replay attacks

Process step	**Id.No.**
reader scans & verifies data page	12

Process step description

Communication: Reader <=> Software

- optical scan datapage (IR, UV, WHITE)

- determine if the document ist authentic (sec. features, MRZ correct, document database)

Threat Description

A scanning error is enforced (e.g. the involved software is attacked) in order to avoid the ABC-control and change to the manual checking

Consequence or Impact

Try to enforce software to stop working

Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
medium	low	SW	D

Potential acceptance criteria

Not yet relevant because manual inspection always possible until now

Possible mitigation

Currently no action required

You are likely affected if...

- using an ABC gate is mandatory

Process step	**Id.No.**
reader scans & verifies data page	13

Process step description

Communication: Reader <=> Software

- optical scan datapage (IR, UV, WHITE)

- determine if the document ist authentic (sec. features, MRZ correct, document database)

Threat Description

Test documents, specimen documents or void documents are not recognized and can be used instead of valid genuine documents

Consequence or Impact

Allowing illicit traveller to pass border

Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
medium	high	SW	S

Potential acceptance criteria

Documents clearly indicated as specimen, void or otherwise not valid must be detected.

Possible mitigation

Image of passport must appear on HMI

You are likely affected if...

- passport reader does not recognise specimens or void documents

Process step	**Id.No.**
reader scans & verifies data page	14

Process step description

Communication: Reader <=> Software

- optical scan datapage (IR, UV, WHITE)

- determine if the document ist authentic (sec. features, MRZ correct, document database)

Threat Description

The document verification is attacked (manipulation of the software) in order to, e.g., suppress errors or achieve forced positive results of the check routines, crash / error via document during the usage of the reader

Consequence or Impact

Enforcing wrong conclusion of the software on the consistency of the document

Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
medium	low	SW	D

Potential acceptance criteria

Must be avoided

Possible mitigation

Use of signed software

You are likely affected if…

- the software allows manipulation before or during operation

Process step	**Id.No.**
reader scans & verifies data page	15

Process step description

Communication: Reader <=> Software

- optical scan datapage (IR, UV, WHITE)

- determine if the document ist authentic (sec. features, MRZ correct, document database)

Threat Description

The document verification ist manipulated (e.g. a manipulation of the document database, change of stored patterns or the like,...)

Consequence or Impact

Attacking background information used by the software to draw conclusions

Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
medium	low	SW	T

Potential acceptance criteria

Must be avoided

Possible mitigation

Use of appropriate encryption, hashing, etc.

You are likely affected if...

- the reference data used for verification and/or the verification process is not protected

Process step			**Id.No.**
reader scans & verifies data page			16
Process step description Interaction: Passenger <=> Reader - Hold passport tight on the screen.			
Threat Description Passport is taken too early from the reader, it is moved inside the reader or it is not kept flat on the reader.			
Consequence or Impact The operation is failed or slowed down.			
Damage Potential low	**Exploitability** high	**Affected Components** HW	**STRIDE** D
Potential acceptance criteria Target is 99% successful handling			
Possible mitigation Appropriate information/training/alerting			
You are likely affected if… - using an ABC gate is mandatory			

Process step	**Id.No.**
reader reads & verifies chip data	17

Process step description

Communication: Reader <=> Software

- Read chip
- Check if chip matches to document (text + picture)
- Perform ICAO check (certificate chain, clone protection, ...)

Threat Description

A chip (signed with original or test certificate) in test documents, specimen documents or void documents will be recognized as a valid chip.

Consequence or Impact

Usage of test certificates or any other invalid certificate that are not recognised as such; related to incomplete PKD

Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
high	medium	SW	S

Potential acceptance criteria

Must be avoided

Possible mitigation

ICAO conform check must be performed in order to verify with electronic information

You are likely affected if…

- passport reading is not fully ICAO conform

Process step	**Id.No.**
reader reads & verifies chip data	18

Process step description

Communication: Reader <=> Software

- Read chip
- Check if chip matches to document (text + picture)
- Perform ICAO check (certificate chain, clone protection, ...)

Threat Description

Disruption of the communication (e.g. preparation for an attack: repeated disruption of the chip is perceived as "normal" until the ending of the automated control and change to the manual checking

Consequence or Impact

Anything that can stop communication to work, e.g. attack to the RFID communication or attack to communication algorithms

Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
medium	high	HW	D

Potential acceptance criteria

Not yet relevant because manual inspection always possible until now

Possible mitigation

Currently no action required

You are likely affected if...

- using an ABC gate is mandatory

Process step	**Id.No.**
reader reads & verifies chip data	19

Process step description

Communication: Reader <=> Software

- Read chip
- Check if chip matches to document (text + picture)
- Perform ICAO check (certificate chain, clone protection, ...)

Threat Description

Certificates are not available (e.g. certificates of smaller countries) or incomplete: outdated certificate data (missing Certificate Revocation List (CRL) or missing current version of the certificates)

Consequence or Impact

Different from test certificate attack; incomplete verification can be exploited.

Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
high	medium	SW	S

Potential acceptance criteria

Must be avoided

Possible mitigation

ICAO conform check must be performed in order to verify with electronic information. In the worst case, shutdown of ABC.

You are likely affected if...

- passport reading is not fully ICAO conform
- passport processing allows absence of certain certificates

Process step	**Id.No.**
reader reads & verifies chip data	20

Process step description

Communication: Reader <=> Software

- Read chip
- Check if chip matches to document (text + picture)
- Perform ICAO check (certificate chain, clone protection, ...)

Threat Description

Defects in certificates that are already (or still not) published in the ICAO public key directory (PKD) are exploited (e.g. a document signer certificate (DSC) from the defect list is used intentionally on the chip). Therefore the certificate check canno

Consequence or Impact

Exploiting non standard behaviour of certain types of chips.

Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
high	medium	SW	S

Potential acceptance criteria

Must go to manual inspection and border guard informed.

Possible mitigation

Connection to PKD must be available. Otherwise, must go to manual inspection and border guard informed.

You are likely affected if...

- passport reading is not fully ICAO conform
- passport processing allows absence of certain certificates

Process step	**Id.No.**
reader reads & verifies chip data	21

Process step description

Communication: Reader <=> Software

- Read chip
- Check if chip matches to document (text + picture)
- Perform ICAO check (certificate chain, clone protection, ...)

Threat Description

Insecure software is used that does not process the specified check steps in the correct order (e.g. reading/processing of chip data before the verification is completed if the chip data is authentic and unchanged)

Consequence or Impact

Improper implementation of relevant protocols

Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
high	low	SW	S

Potential acceptance criteria

Must be avoided

Possible mitigation

ICAO conform check must be performed. Use of signed software

You are likely affected if…

- the software allows manipulation before or during operation

Process step	**Id.No.**
reader reads & verifies chip data	22

Process step description

Communication: Reader <=> Software

- Read chip
- Check if chip matches to document (text + picture)
- Perform ICAO check (certificate chain, clone protection, ...)

Threat Description

Insecure software is used: e.g. the software is forced to crash due to manipulated chip data (JPGE2k-attack of Grunewald)

Consequence or Impact

Exploiting known vulnarabilities of used libraries

Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
low	medium	SW	D

Potential acceptance criteria

Must be avoided

Possible mitigation

Proper implementation accordindg to ICAO and Frontex recommendations.

You are likely affected if...

- the used software is vulnerable to injection attacks via the passport data

Process step	**Id.No.**
reader reads & verifies chip data	23

Process step description

Communication: Reader <=> Software

- Read chip
- Check if chip matches to document (text + picture)
- Perform ICAO check (certificate chain, clone protection, ...)

Threat Description

Insecure software is used that allows attacks (e.g. code injection) via manipulated chip data (e.g. JPGE2k in DG2 or usage of other datagroups in order to execute malware, usage of the data for an SQL injection if these are stored in a database). Software

Consequence or Impact

Highly sophisticated software attack

Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
high	low	SW	T

Potential acceptance criteria

Must be avoided

Possible mitigation

Input sanitation

You are likely affected if…

- the used software is vulnerable to injection attacks via the passport data

Process step	**Id.No.**
reader reads & verifies chip data	24

Process step description

Communication: Reader <=> Software

- Read chip
- Check if chip matches to document (text + picture)
- Perform ICAO check (certificate chain, clone protection, ...)

Threat Description

Through manipulation of the software some options for checks are deactivated through the changing of configuration data (e.g. check for cloned chips, change into the test mode with access to test certificates,...)

Consequence or Impact

Attack to the configuration file of the reader software in order to bypass certain checks.

Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
high	low	SW	T

Potential acceptance criteria

Must be avoided

Possible mitigation

Use of appropriate encryption, hashing, etc.

You are likely affected if…

- the software allows manipulation before or during operation
- the configuration data is not protected against manipulation

Process step	**Id.No.**
reader reads & verifies chip data	25

Process step description

Interaction: Passenger <=> Reader

- Waits of the completion of scanning process

Threat Description

Inserting a passport with defective chip in the reader.

Consequence or Impact

Avoid chip reading on purpose

Passport reading fails. When the passenger moves to the next gates the incident multiplies. The traveller gets nervous.

Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
low	high	HW	D

Potential acceptance criteria

Must be sent to manual inspection.

Possible mitigation

Manual inspection

You are likely affected if…

- using an ABC gate is mandatory

Process step	**Id.No.**
reader reads & verifies chip data	26

Process step description

Interaction: Passenger <=> Reader

- Waits of the completion of scanning process

Threat Description

The passport can't be electronically read and therefore not verified.

Consequence or Impact

Passport reading fails. When the passenger moves to the next gates the incident multiplies. The traveller gets nervous.

Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
low	high	SW	D

Potential acceptance criteria

Must be sent manual inspection.

Possible mitigation

Manual inspection

You are likely affected if...

- using an ABC gate is mandatory

Process step	**Id.No.**
check eligibility	27

Process step description

Interaction: Passenger <=> eGate

- Wait that the eligibility is accepted

Threat Description

Traveller forces the doors open – because he/she does not know how to operate them.

Consequence or Impact

Traveller steps inside or gets through without the BG to notice that.

Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
high	high	HW	D

Potential acceptance criteria

Must not happen unobserved.

Possible mitigation

Appropriate information/training/alerting. Else, must raise an alarm, following appropriate monitoring

You are likely affected if…

- doors allow opening with manual force
- unauthorised opening of the doors is not properly alerted

Process step	**Id.No.**
check eligibility	28

Process step description

Interaction: Passenger <=> eGate

- Wait that the eligibility is accepted

Threat Description

Traveller opens the doors on purpose to get in unnoticed.

Quick operation, Traveller knows the mechanism of the doors; the BG does not necessarily notice the traveller entering the gate. On the other hand the safety aspects of the doors must also be consi

Consequence or Impact

Traveller steps inside or gets through without the BG to notice that.

Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
high	high	HW	D

Potential acceptance criteria

Must not happen unobserved.

Possible mitigation

Must raise an alarm, following appropriate monitoring

You are likely affected if...

- doors allow opening with manual force
- unauthorised opening of the doors is not properly alerted

Process step	**Id.No.**
check eligibility	29

Process step description

Interaction: Passenger <=> eGate

- Wait that the eligibility is accepted

Threat Description

The passport is left inside the reader and could be used a second time by the next person.

Consequence or Impact

The traveller can step in but the process will not continue until the passport is taken out of the reader. The operational speed is slowed down.

Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
low	high	PEOPLE	S

Potential acceptance criteria

Reuse of passport Must be avoided.

Possible mitigation

Particular design that does not allow unnoticed depositioning; otherwise must raise an alarm, following appropriate monitoring because it could be an attack

You are likely affected if…

- passport reader allows the deposition of the passport unnoticed

Process step	**Id.No.**
Kiosk: passenger registers	30

Process step description

Communication: Reader <=> Software

- Recognize document (Event: new document was put on reader)
- Support for the traveller

Threat Description

The reader is compromised in its correct function (e.g. jammer, damaged through vandalism or - if applicable - soiling prevents a proper functionality)

Consequence or Impact

Could be exploited for denial of service attack

Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
medium	high	SW	T

Potential acceptance criteria

Must not happen unobserved

Possible mitigation

Degree of soiling of device must be observed and in case of potential malfunction appropriate actions need to betaken

You are likely affected if…

- the passport reader does not have sufficient self-test capabilities
- the passport reader is not monitored otherwise
- the passport reader is not resilient against dirt or physical attacks

Process step	**Id.No.**
Kiosk: passenger registers	31

Process step description

Communication: Reader <=> Software

- Recognize document (Event: new document was put on reader)
- Support for the traveller

Threat Description

The reader is eavesdropped, that means the data is also read from a not authorized person and can be therefore used (e.g. USB device with access to the hardware of the reader)

Consequence or Impact

data protection breach

Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
low	low	SW	T

Potential acceptance criteria

Must not happen unobserved

Possible mitigation

Access to any component must be clearly restricted (e.g. no access point in reach), appropriate encryption of data

You are likely affected if…

- the housing of the passport reader is not sufficiently protected
- the reader has a visible connection for external devices

Process step	**Id.No.**
Kiosk: passenger registers	32

Process step description

Communication: Reader <=> Software

- Recognize document (Event: new document was put on reader)
- Support for the traveller

Threat Description

False, counterfeited or falsified tokens are used abusively

Consequence or Impact

various types of presentation possible

Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
medium	medium	SW	T

Potential acceptance criteria

Must be avoided

Possible mitigation

Must be detected and alarm raised.

You are likely affected if...

- passport reader is not regularily updated on false documents

Process step	**Id.No.**
Kiosk: passenger registers	33

Process step description

Communication: Reader <=> Software

- Recognize document (Event: new document was put on reader)
- Support for the traveller

Threat Description

The correct tokens are exchanged between two persons and are used abusively.

Consequence or Impact

e.g. to enforce manual inspection

Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
medium	medium	PEOPLE	S

Potential acceptance criteria

Accuracy of biometric verificaction

Possible mitigation

Generally, this is part of biometric verification. However, to avoid cases of undeliberate presentation of wrong passport, feedback to the user shall be given when presenting the passport (e.g. name or image)

You are likely affected if…

- biometric verification not strong enough to distinguish all persons

Process step	**Id.No.**
Kiosk: capture live biometric data	34

Process step description

Communication: Reader <=> Software

- Feature detection
- Feature capture
- Feature verification (live vs. Chip): Feature chain live to chip
- Support for the traveller
- Ensure feature chain

Threat Description

Through the manipulation of the software a positive result when matching the biometric data on the chip (e.g. photo in DG2) with the additionally captured biometrics at the kiosk (e.g. IR-picture captured on the same day) is achieved

Consequence or Impact

Illicit traveller could pass the border

Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
medium	low	SW	T

Potential acceptance criteria

Must be avoided

Possible mitigation

Use of signed software

You are likely affected if…

- the software allows manipulation before or during operation
- the configuration data is not protected against manipulation

Process step	**Id.No.**
Kiosk: capture live biometric data	35

Process step description

Communication: Reader <=> Software

- Feature detection
- Feature capture
- Feature verification (live vs. Chip): Feature chain live to chip
- Support for the traveller
- Ensure feature chain

Threat Description

The software can be attacked due to an insecure/bad implementation (e.g. thresholds are set to low or errors in the software itself or missing implementation of all check requirements).

Consequence or Impact

Exploiting vulnarabilities of the software

Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
medium	medium	SW	T

Potential acceptance criteria

Must be avoided

Possible mitigation

Verify quality of implementation

You are likely affected if…

- the usage software has not been tested against a large set of test data, including real imposters

Process step	**Id.No.**
Kiosk: capture live biometric data	36

Process step description

Communication: Reader <=> Software

- Feature detection
- Feature capture
- Feature verification (live vs. Chip): Feature chain live to chip
- Support for the traveller
- Ensure feature chain

Threat Description

The communicaiton is eavesdropped, that means the data is also read from a not authorized person and can be therefore used

Consequence or Impact

Someone would steal the biometric data -> data protection

Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
medium	medium	HW+SW	I

Potential acceptance criteria

Must not happen unobserved, at least not with low effort

Possible mitigation

Access to any component must be clearly restricted (e.g. no access point in reach), appropriate encryption of data

You are likely affected if...

- the communication line from and to the passport reader is not sufficiently protected

Process step	**Id.No.**
Kiosk: capture live biometric data	37

Process step description

Communication: Reader <=> Software

- Feature detection
- Feature capture
- Feature verification (live vs. Chip): Feature chain live to chip
- Support for the traveller
- Ensure feature chain

Threat Description

Verification failure e.g. by replay attack of an image not belonging to the person in front of the kiosk (false positive) or weakness of the comparison algorithm (false negative)

Consequence or Impact

Illicit traveller could pass the border

Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
high	high	SW	T

Potential acceptance criteria

Must be avoided

Possible mitigation

Spoof detection must be in accordance with state-of-the-art

You are likely affected if...

- the biometric verification component is not spoof resistant

Process step	**Id.No.**
Kiosk: capture live biometric data	38

Process step description

Communication: Reader <=> Software

- Feature detection
- Feature capture
- Feature verification (live vs. Chip): Feature chain live to chip
- Support for the traveller
- Ensure feature chain

Threat Description

A manipulated data page (changed optically, physical manipulation) delivers information that leads to a misinterpretation "false acceptance" when reading the document. (e.g. manipulated name in MRZ delivers no match in a wanted-persons database etc., the

Consequence or Impact

E.g., attacker has mounted a (printed) manipulated image in the eMRTD which gives high biometric matching score with live image.

Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
high	medium	SW	S+T

Potential acceptance criteria

Must be avoided

Possible mitigation

ICAO conform check must be performed in order to verify with electronic information

You are likely affected if...

- passport reader unable to detect all kind of manipulated data pages

Process step	**Id.No.**
Kiosk: capture live biometric data	39

Process step description

Communication: Reader <=> Software

- Feature detection
- Feature capture
- Feature verification (live vs. Chip): Feature chain live to chip
- Support for the traveller
- Ensure feature chain

Threat Description

Inappropriate presentation attack detection facilitates attacks (e.g. photo on paper or tablet, usage of masks, silicon finger, …) (see ISO ISO/IEC CD 30107)

Consequence or Impact

Illicit traveller could pass the border

Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
high	medium	SW	T

Potential acceptance criteria

Must be avoided

Possible mitigation

Spoof detection must be in accordance with state-of-the-art

You are likely affected if…

- the biometric verification component is not spoof resistant

Process step	**Id.No.**
Kiosk: store data in database	40

Process step description

Communication: Kiosk <=> Software

Threat Description

Total or partial manipulation of data that was already verified and transmitted or stored for verification of the person in the eGate (e.g change of biometrics data to a different person)

Consequence or Impact

With other elements could lead to allow illicit traveller pass the border

Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
high	low	SW	T

Potential acceptance criteria

Process dependent data may be stored for a certain time (locally or centrally); data protection related, including privacy; quantification application and context dependent

Possible mitigation

Proper access control to involved compoents; encryption/signing of data

You are likely affected if...

- the communication line from and to the passport reader is not sufficiently protected
- the communication protocol does not check for data integrity

Process step	**Id.No.**
Kiosk: store data in database	41

Process step description

Communication: Kiosk <=> Software

Threat Description

Total or partial loss of data from the kiosk data base due to unauthorized access.

Consequence or Impact

Could be exploited for denial of service attack

Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
medium	low	SW	T

Potential acceptance criteria

Must be avoided

Possible mitigation

Proper access control to involved components

You are likely affected if…

- the communication line from and to the passport reader is not sufficiently protected
- the communication protocol does not check for data integrity

Process step	**Id.No.**
perform background check	42

Process step description

Communication: Software <=> System for Background checks

- Result to the Person (e.g.. search)
- Result to the document (e.g.. search due to theft)

Threat Description

Through manipulation of the software the response of background systems (wanted-persons database) are (partially) suppressed or (partially) replaced in order to feign an uncritical result.

Consequence or Impact

any attack to the decision module of the egate

Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
high	low	SW	T

Potential acceptance criteria

Must be avoided

Possible mitigation

Use of signed software; encrypted data transfer

You are likely affected if…

- the software allows manipulation before or during operation
- the configuration data is not protected against manipulation

Process step	**Id.No.**
perform background check	43

Process step description

Communication: Software <=> System for Background checks

- Result to the Person (e.g.. search)
- Result to the document (e.g.. search due to theft)

Threat Description

Due to the illicit implementation, attacks are possible (e.g. through incorrect software responses from background systems are not shown properly or shown in a way that they may be skipped easily)

Consequence or Impact

software vulnarabilities, including bad design of HMI

Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
high	low	SW	T

Potential acceptance criteria

Must be avoided

Possible mitigation

Verify quality of implementation

You are likely affected if…

- the usage software has not been tested against a large set of test data, including real imposters

Process step	**Id.No.**
perform background check	44

Process step description

Interaction: Passenger <=> eGate

- doors open, passenger takes the passport from the reader and steps in the gate. The background checks will not start earlier.

Threat Description

Someone else (the traveller at the next gate) steps in the gate (substitute).

Consequence or Impact

Possibility to get through cf. impostor. Threat to the border security. Multiple identification.

Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
high	high	PEOPLE	D

Potential acceptance criteria

Accuracy of biometric verificaction

Possible mitigation

Generally, this is part of biometric verification. However, to avoid cases of undeliberate presentation of wrong passport, feedback to the user shall be given when presenting the passport (e.g. name or image)

You are likely affected if…

- biometric verification not strong enough to distinguish all persons

Process step	**Id.No.**
perform person separation	45

Process step description

Communication: Software <=> eGate

- Close doors
- Check if just one person is in the eGate

Threat Description

Through manipulation of the software the single person recognition is deactivated; alternatively indirect via other systems that are able to open doors in emergency situations (e.g. fire alarm,...)

Consequence or Impact

A second person could pass the border undetected

Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
high	low	SW	T

Potential acceptance criteria

Must be avoided

Possible mitigation

Use of signed software; encrypted data transfer

You are likely affected if...

- person separation component is not sufficiently protected against attacks

Process step	**Id.No.**
perform person separation	47

Process step description

Communication: Software <=> eGate

- Close doors
- Check if just one person is in the eGate

Threat Description

Through clever performance ("piggyback") facilitated through inadequate software the single person recognition can be fooled

Consequence or Impact

spoofing or distracting of the recognition software

Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
medium	medium	SW	T

Potential acceptance criteria

Must be avoided

Possible mitigation

Spoof detection must be in accordance with state-of-the-art

You are likely affected if...

- the usage software has not been tested against a large set of test data, including real imposters
- the presence of another person in the gate cannot be detected otherwise

Process step	**Id.No.**
perform person separation	48

Process step description

Interaction: Passenger <=> eGate

- doors are closed

Threat Description

A child is carried nestled or under the clothes of an adult.

Consequence or Impact

Process is interrupted when the BG notices the situation. Border security at risk. Risk of international child abduction. Age limit of using the ABC and physical guarding.

Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
high	high	PEOPLE+SW	T

Potential acceptance criteria

Detection must be in accordance with state-of-the-art

Possible mitigation

Appropriate video monitoring; detection must be in accordance with state-of-the-art

You are likely affected if...

- the usage software has not been tested against a large set of test data
- the presence of a hidden child inside the gate cannot be detected otherwise

Process step	**Id.No.**
perform person separation	49

Process step description

Interaction: Passenger <=> eGate

- doors are closed

Threat Description

The person is sitting on the shoulders of the other person and only the upper one is recognised.

Consequence or Impact

Border security at risk. Person is able to cross the border. Physical guarding to control the possible misuse of the gates.

Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
high	medium	PEOPLE+SW	T

Potential acceptance criteria

Detection must be in accordance with state-of-the-art

Possible mitigation

Appropriate video monitoring; detection must be in accordance with state-of-the-art

You are likely affected if…

- there is no additional monitoring of the presence in the gate

Process step	**Id.No.**
biometric capture (face, finger, iris)	50

Process step description

Communication: Biometric capture device <=> Software

- Feature detection
- Feature capture

Threat Description

The software can be attacked due to an insecure/bad implementation (e.g. thresholds are set to low or errors in the software itself (missing implementation of all check requirements)).

Consequence or Impact

Illicit traveller could pass the border

Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
medium	medium	SW	T

Potential acceptance criteria

Sufficiently tested according to best practices

Possible mitigation

Sufficient level of software testing, including pentration tests

You are likely affected if…

- the usage software has not been tested against a large set of test data, including real imposters

Process step	**Id.No.**
biometric capture (face, finger, iris)	51

Process step description

Communication: Biometric capture device <=> Software

- Feature detection
- Feature capture

Threat Description

The communicaiton is eavesdropped, that means the data is also read from a not authorized person and can be therefore used

Consequence or Impact

data protection breach

Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
medium	medium	HW+SW	I

Potential acceptance criteria

Must be avoided

Possible mitigation

Encryption; hardening of communication infrastructure

You are likely affected if…

- Communication lines between various components are not sufficiently protected

Process step	**Id.No.**
biometric capture (face, finger, iris)	52

Process step description

Communication: Biometric capture device <=> Software

- Feature detection
- Feature capture

Threat Description

Verification failure e.g. by replay attack of an image not belonging to the person in front of the eGate camera (false positive) or weakness of the comparison algorithm (false negative)

Consequence or Impact

Illicit traveller could pass the border

Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
high	high	SW	T

Potential acceptance criteria

Sufficiciently small error rates

Possible mitigation

Testing in order to verify error rates

You are likely affected if…

- the usage software has not been tested against a large set of test data, including real imposters

Process step	**Id.No.**
biometric capture (face, finger, iris)	53

Process step description

Communication: Biometric capture device <=> Software

- Feature detection
- Feature capture

Threat Description

Inappropriate presentation attack detection facilitates attacks (e.g. photo on paper or tablet, usage of masks, silicon finger, …) (see ISO ISO/IEC CD 30107)

Consequence or Impact

Illicit traveller could pass the border

Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
high	medium	SW	T

Potential acceptance criteria

Sufficiciently small error rates according to state-of-the-art

Possible mitigation

State-of-the-art PAD; Testing in order to verify error rates

You are likely affected if…

- the biometric verification component is not spoof resistant

Process step	**Id.No.**
biometric capture (face, finger, iris)	54

Process step description

Interaction: Passenger <=> Biometric sensor

- Passenger provides biometrics – e.g. finger
- Passenger puts finger(s) on the reader according to the instructions

Threat Description

Spoofing of fingerprints (eg. Fingerprints from an other peron are used, use of silicon mould, ...)

Consequence or Impact

Possible to pass.

Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
high	low	SW	S

Potential acceptance criteria

Must be avoided

Possible mitigation

Use state-of-the-art algorithms

You are likely affected if…

- the fingerprint reader is not spoof resistant

Process step	**Id.No.**
perform biometric verification (face, finger, iris, ...)	55

Process step description

Communication: Camera <=> Software

- Face detection
- Face capture
- Face verification (live face vs. face am Chip)
- Support for the traveller

Threat Description

Through manipulation of the software the result of the face recognition is changed (e.g. usage of certain combination document number +...)

Consequence or Impact

e.g. backdoors in the software

Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
high	low	SW	T

Potential acceptance criteria

Must be avoided

Possible mitigation

Use of signed software; encrypted data transfer

You are likely affected if...

- the software allows manipulation before or during operation
- the configuration data is not protected against manipulation

Process step	**Id.No.**
perform biometric verification (face, finger, iris, ...)	56

Process step description

Communication: Camera <=> Software

- Face detection
- Face capture
- Face verification (live face vs. face am Chip)
- Support for the traveller

Threat Description

Due to illicit implementation, attacks are possible (e.g. errors in the software for the face recognition due to weaknesses in the algorithm / environment parameters, low threshold parameters,...)

Consequence or Impact

software vulnarabilities, including bad design of HMI

Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
high	medium	SW	T

Potential acceptance criteria

Must be avoided

Possible mitigation

Verify quality of implementation

You are likely affected if...

- the usage software has not been tested against a large set of test data, including real imposters

Process step	**Id.No.**
perform biometric verification (face, finger, iris, ...)	57

Process step description

Communication: Camera <=> Software

- Face detection
- Face capture
- Face verification (live face vs. face am Chip)
- Support for the traveller

Threat Description

Inappropriate presentation attack detection facilitates attacks (e.g. photo on paper or tablet, usage of masks, fake fingerprints, …) (see ISO ISO/IEC CD 30107)

Consequence or Impact

Spoofing attack

Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
high	high	SW	T

Potential acceptance criteria

Must be avoided

Possible mitigation

Generally, this is part of biometric verification. However, to avoid cases of undeliberate presentation of wrong passport, feedback to the user shall be given when presenting the passport (e.g. name or image)

You are likely affected if...

- the biometric verification component is not spoof resistant

Process step	**Id.No.**
perform biometric verification (face, finger, iris, ...)	58

Process step description

Interaction: Passenger <=> Camera

- doors are closed

Threat Description

Presentation attack, (e.g. presenting a face on a t-shirt, or video screen in front of the face, or wearing a mask) and the liveness detection is circumvented.

Consequence or Impact

Wrong person can pass the gate.

Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
high	high	SW	T

Potential acceptance criteria

Must be avoided

Possible mitigation

Use state-of-the-art algorithms

You are likely affected if...

- the biometric verification component is not spoof resistant

Process step	**Id.No.**
perform biometric verification (face, finger, iris, ...)	59

Process step description

Interaction: Passenger <=> Camera

- doors are closed

Threat Description

Identical twin presents the passport/identifier of the sibling.

Consequence or Impact

When only face verification is performed, wrong person (similar in apparence) can pass the gate.

Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
high	low	SW	T

Potential acceptance criteria

Must be avoided

Possible mitigation

Use state-of-the-art algorithms

You are likely affected if...

- Twins cannot be distinguished by the physical presence

Process step	**Id.No.**
perform biometric verification (face, finger, iris, ...)	60

Process step description

Interaction: Passenger <=> Camera

- doors are closed

Threat Description

Inappropriate false acceptance and false rejection rates (FAR/FRR) facilitates attacks

Consequence or Impact

Spoofing attack

Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
high	medium	SW	S+T

Potential acceptance criteria

Must be avoided

Possible mitigation

Use state-of-the-art algorithms

You are likely affected if...

- the usage software has not been tested against a large set of test data, including real imposters

Process step	**Id.No.**
perform biometric verification (face, finger, iris, ...)	61

Process step description

Interaction: Passenger <=> Biometric sensor

- Passenger waits of the completion of scanning process

Threat Description

The biometric capture device is not working properly (soiled or damaged (e.g. vandalism))

Consequence or Impact

Recognition fails. (depending on the technology), spreading deceases possible – not possible to clean the reader after each reading occasion.

Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
low	high	HW	D

Potential acceptance criteria

Must not happen unobserved

Possible mitigation

Degree of soiling of device must be observed and in case of potential malfunction appropriate actions need to be taken

You are likely affected if…

- the biometric device does not have sufficient self-test capabilities
- the biometric device is not monitored otherwise
- the device is not resilient against dirt or physical attacks

Process step	**Id.No.**
X-Check Document / Person / Token	62

Process step description

- Check Document vs. Person:
  - VIZ vs. MRZ
  - VIZ vs. Chip
  - MRZ vs. Chip
- Person Face live vs. Chip vs. VIZ

Threat Description

A (partial) manipulation remains undetected if the verification chain is not executed completely.

Consequence or Impact

vulnarabilities of the decision module

Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
high	high	HW+SW	T

Potential acceptance criteria

Must not happen unobserved

Possible mitigation

System should not allow such incomplete execution, verified by testing

You are likely affected if…

- verification softwares allows incomplete processing
- the configuration data is not protected against manipulation

Process step	**Id.No.**
X-Check Document / Person / Token	63

Process step description

- Check Document vs. Person:
  - VIZ vs. MRZ
  - VIZ vs. Chip
  - MRZ vs. Chip
- Person Face live vs. Chip vs. VIZ

Threat Description

Through manipulation of the software the result is changed

Consequence or Impact

e.g. backdoors in the software

Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
high	low	SW	T

Potential acceptance criteria

Must be avoided

Possible mitigation

Use of signed software

You are likely affected if…

- the software allows manipulation before or during operation

Process step	**Id.No.**
X-Check Document / Person / Token	64

Process step description

- Check Document vs. Person:
  - VIZ vs. MRZ
  - VIZ vs. Chip
  - MRZ vs. Chip
- Person Face live vs. Chip vs. VIZ

Threat Description

Due to a missing match between liveness detection and biometric verification it is possible that instead of the "living biometric" an alternative input (e.g. mobile phone, tablet, t-shirt) from the verification module is used.

Consequence or Impact

Spoofing attack addressed at the decision module

Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
high	medium	SW	T

Potential acceptance criteria

Sufficiciently small error rates according to state-of-the-art

Possible mitigation

State-of-the-art PAD; Testing in order to verify error rates

You are likely affected if...

- the biometric verification component is not spoof resistant

Process step	**Id.No.**
passenger leaves eGate	65

Process step description

Communication: Software <=> Gate

- Open door
- Hint for the traveller (forgot suitcase etc., to which gate he has to go, ...)

Threat Description

A so-called replay attack can be executed, that means recording and play-back of communication in the system (e.g. recording of the communication for opening the door; play-back this communication in order to be able to open the door although the face rec

Consequence or Impact

illicit person could pass the border

Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
high	low	SW	T

Potential acceptance criteria

Must be avoided

Possible mitigation

Components (including comm. Infrastructure) must be protected accordingly

You are likely affected if...

- Communication lines between various components are not sufficiently protected

Process step	**Id.No.**
passenger leaves eGate	66

Process step description

Communication: Software <=> Gate

- Open door
- Hint for the traveller (forgot suitcase etc., to which gate he has to go, ...)

Threat Description

Due to illicit implementation, attacks are possible (e.g. bad usability or handling errors enable the border agent to change a negative result to a positive one, that means manual admittance of the passenger - "false acceptance")

Consequence or Impact

exploiting software vulnarabilities

Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
high	high	SW	T

Potential acceptance criteria

Sufficiently tested according to best practices

Possible mitigation

Sufficient level of software testing, including pentration tests

You are likely affected if...

- the usage software has not been tested against a large set of test data, including real imposters

Process step	**Id.No.**
passenger leaves eGate	67

Process step description

Communication: Software <=> Gate

- Open door
- Hint for the traveller (forgot suitcase etc., to which gate he has to go, ...)

Threat Description

Missing security measures in cases of extreme situations (e.g. fire alarm, power blackout, etc.) allow the passenger to leave the eGate unlawfully

Consequence or Impact

e.g. exploiting safety measures

Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
high	medium	HW+PEOPLE+SW	T

Potential acceptance criteria

A plan must exist to address this

Possible mitigation

Should be harmonised with general emergency plans

You are likely affected if...

- the impact of emergency or failure situation is not fully elaborated

Process step	**Id.No.**
passenger leaves eGate	68

Process step description

Communication: Software <=> Gate

- Open door
- Hint for the traveller (forgot suitcase etc., to which gate he has to go, ...)

Threat Description

Inadequate usability leads to handling errors of the border agents in the case of exceptional and intentionally induced situations

Consequence or Impact

e.g. exploiting measures in case of emergencies involving the border guard

Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
high	medium	HW+SW	T

Potential acceptance criteria

Sufficiently tested according to best practices

Possible mitigation

Sufficient level of software testing; particular training of personnel

You are likely affected if...

- the impact of emergency or failure situation is not fully elaborated

Process step	**Id.No.**
passenger leaves eGate	69

Process step description

Interaction: Passenger <=> eGate exit

- Passenger walks out of the gate

Threat Description

Luggage is left between the doors and a following person can slip through (single door solutions)

Consequence or Impact

The gate can’t close. The operation is slowed down for the next passenger.

Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
medium	high	HW	T

Potential acceptance criteria

Status of doors must be monitored

Possible mitigation

Appropriate error message to the border guard

You are likely affected if…

- there is no alarming system about non closing doors
- the area of the doors is not directly monitored by border guards or cameras

Process step	**Id.No.**
Software / HW Operations	70

Process step description

- cached/mirror TCC/PKD/...
- Softwareupdates
- cache/mirror document data base

Threat Description

The systems reacts to the failure of certain hardware/software (components), whereby doors open or close

Consequence or Impact

Denial of service or exploting confusion to pass border

Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
medium	high	HW+SW	T

Potential acceptance criteria

Must be avoided

Possible mitigation

Appropriate controls should take over

You are likely affected if...

- system errors can lead to opening of doors
- insufficient alert of system failures

Process step	**Id.No.**
Software / HW Operations	71

Process step description

- cached/mirror TCC/PKD/...
- Softwareupdates
- cache/mirror document data base

Threat Description

The recovery of the system in the case of failure is not possible (e.g. missing backups)

Consequence or Impact

Denial of service

Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
medium	high	HW+SW	D

Potential acceptance criteria

Must be avoided

Possible mitigation

Redundant system and regular backups

You are likely affected if...

- the impact of emergency or failure situation is not fully elaborated
- the system does not have a recovery mode

Process step	**Id.No.**
Software / HW Operations	72

Process step description

- cached/mirror TCC/PKD/...
- Softwareupdates
- cache/mirror document data base

Threat Description

There are open maintenance accesses to the eGate infrastructure (e.g. the prime contractor of the system can perform maintenance works remotely, alternatively special local maintenance accesses (with extensive rights), ...)

Consequence or Impact

System could be remotely manipulated

Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
high	medium	SW	T

Potential acceptance criteria

Must be avoided

Possible mitigation

Appropriate access controls

You are likely affected if...

- the system can be maintained remotely
- remote access is not sufficiently secured

Process step	**Id.No.**
Software / HW Operations	73

Process step description

- cached/mirror TCC/PKD/...
- Softwareupdates
- cache/mirror document data base

Threat Description

A manipulation of the eGate is facilitated through inadequate physical protection devices

Consequence or Impact

All types of consequences

Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
high	high	HW	T

Potential acceptance criteria

Must be avoided

Possible mitigation

Physical protection must withstand the most likely attacks

You are likely affected if...

- the physical protections of sensitive components (controller, passport reader, communication lines, etc.) are not strong enough to withstand certain physical attacks

Process step	**Id.No.**
Software / HW Operations	74

Process step description

- cached/mirror TCC/PKD/...
- Softwareupdates
- cache/mirror document data base

Threat Description

The compliance to governance guidelines is not guaranteed (e.g. missing guidelines or processes in order to safe-guard privacy)

Consequence or Impact

Inappropriate or missing rules how to operate the system properly; relevant for data protection; continuous monitoring

Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
medium	low	HW+SW	R

Potential acceptance criteria

Must be avoided

Possible mitigation

Existence of clear rules and conduct of regular audits to verify compliance

You are likely affected if...

- the compliance with governance guidelines is not enforced

Process step	**Id.No.**
Software / HW Operations	75

Process step description

- cached/mirror TCC/PKD/...
- Softwareupdates
- cache/mirror document data base

Threat Description

Persons able to access the system (border guards, technicians, airport staff, …) could manipulate the system for illegal pass through.

Consequence or Impact

illicit person could pass the border; eligible persons could be unnecessarily hindered to pass

Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
high	low	HW+SW	T

Potential acceptance criteria

Must not happen unobserved

Possible mitigation

Segregation of duties, background check of personnel

You are likely affected if…

- there is no segregation of access rights, in particular for operation and maintenance

Process step	**Id.No.**
Software / HW Operations	76

Process step description

- cached/mirror TCC/PKD/...
- Softwareupdates
- cache/mirror document data base

Threat Description

Risk of unauthorized access to sensitive databases (like VIS, SIS, etc.) through the kiosk and/or e-Gate

Consequence or Impact

Aim is to extract data not the bypassing the traveller verification

Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
medium	low	SW	S

Potential acceptance criteria

Must be avoided

Possible mitigation

Appropriate and strong access control

You are likely affected if...

- sensitive databases can be directly accessed through user terminals at kiosk or eGate

Process step	**Id.No.**
Communication-infrastructure	77

Process step description

- Cabling
- Interfaces
- Protocols

Threat Description

A so-called replay attack can be executed, that means recording and play-back of communication in the system (e.g. recording of the communication for opening the door; play-back this communication in order to be able to open the door although the face rec

Consequence or Impact

Would include communication with the manual inspection booth

Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
high	low	SW	T

Potential acceptance criteria

Must be avoided

Possible mitigation

Integrity checks of communication packets, encrpytion/authentication, statemachine

You are likely affected if...

- Communication lines between various components are not sufficiently protected

Process step	**Id.No.**
Communication-infrastructure	78

Process step description

- Cabling
- Interfaces
- Protocols

Threat Description

It is possible to manipulate the content of the data connection (software interfaces, control of the eGate, …)

Consequence or Impact

Any type of manipulation, even to crash the system; could harm data integrity (data protection)

Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
high	low	SW	T

Potential acceptance criteria

Must be avoided

Possible mitigation

Integrity checks of communication packets, encrpytion/authentication

You are likely affected if…

- Communication lines between various components are not sufficiently protected

Process step			**Id.No.**
Communication-infrastructure			79
Process step description - Cabling - Interfaces - Protocols			
Threat Description The transfer/data line can be interrupted or delayed			
Consequence or Impact Required information will not be available, leading to wrong decisions			
Damage Potential medium	**Exploitability** medium	**Affected Components** HW+SW	**STRIDE** D
Potential acceptance criteria Must be avoided			
Possible mitigation Timeouts should be defined; alerting			
You are likely affected if... - Communication lines between various components are not sufficiently protected			

Process step			**Id.No.**
Communication-infrastructure			80
Process step description - Cabling - Interfaces - Protocols			
Threat Description Vulnarabilities (of protocols, etc.) could be exploited			
Consequence or Impact E.g., a backdoor can be exploited or weak authentication mechanisms			
Damage Potential high	**Exploitability** low	**Affected Components** SW	**STRIDE** T
Potential acceptance criteria Must be avoided			
Possible mitigation Operational security/vulnerability management			
You are likely affected if... - the used software has not undergone a particular security scrutiny			

Process step	**Id.No.**
Communication-infrastructure	81

Process step description

- Cabling
- Interfaces
- Protocols

Threat Description

The communication or the content of the communication can be eavesdropped or manipulated

Consequence or Impact

data protection issue, any type of manipulation (Integrity, Confidentiality are not fullfilled)

Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
medium	medium	SW	I

Potential acceptance criteria

Must be avoided

Possible mitigation

Integrity checks of communication packets, encrpytion/authentication

You are likely affected if...

- communication of components in the system do not use encrytion

Process step	**Id.No.**
Overall system	82

Process step description

n/a

Threat Description

The necessity for a service technician is triggered (e.g. the service technician is then replaced by a not authorized person)

Consequence or Impact

generic insider attack

Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
high	low	SW	T

Potential acceptance criteria

Not applicable

Possible mitigation

Operational security management (verification of authorized personnel)

You are likely affected if...

- maintanance personnel or contractors are not security checked
- there is no operational security management in place

Process step			**Id.No.**
Overall system			83
Process step description			
n/a			
Threat Description			
A person with access to the eGate is bribed (service technician, airport staff,…)			
Consequence or Impact			
generic insider attack			
Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
high	medium	PEOPLE	T
Potential acceptance criteria			
Not applicable			
Possible mitigation			
Security clearances, segreggation of duties, job rotation, ...			
You are likely affected if…			
- involved personnel or contractors have no security clearance - operators have full access to the system control units			

Process step			**Id.No.**
Overall system			84
Process step description			
n/a			
Threat Description			
An APT (advanced persistent threat) is executed (intentional manipulation of the system, e.g. during standard processes such as cleaning, maintenance, security,...)			
Consequence or Impact			
Important threat to access control systems			
Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
high	low	HW+SW	T
Potential acceptance criteria			
Must be avoided			
Possible mitigation			
Operational security/vulnerability management			
You are likely affected if...			
- the used software has not undergone a particular security scrutiny			

Process step			**Id.No.**
Overall system			85
Process step description			
n/a			
Threat Description			
An emergency situation can be induced intentionally, that can be exploited for an attack			
Consequence or Impact			
generic insider attack			
Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
high	low	HW+PEOPLE+SW	T
Potential acceptance criteria			
Must be avoided			
Possible mitigation			
Failsafe states, emergency procedures			
You are likely affected if…			
- the system has not been tested exhaustively under emergency conditions			

Process step	**Id.No.**
Overall system	86

Process step description

n/a

Threat Description

An attack that is based on the probabilistic nature of procedures is executed (e.g. determination of algorithmic twins in connection with probabilistic algorithms for face recognition)

Consequence or Impact

E.g., hill climbing attacks; appears also in person separation

Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
high	low	SW	T

Potential acceptance criteria

Not applicable

Possible mitigation

Exhaustive testing

You are likely affected if…

- the usage software has not been tested against a large set of test data, including real imposters

Process step	**Id.No.**
Overall system	87

Process step description

n/a

Threat Description

Due to missing / bad preparation of the results of the system (e.g. no details why a face recognition was negative that give hints to the operator if a borderline case is on hand, or e.g. fundamental discrepancies are on hand, that let assume an attempt o

Consequence or Impact

Exploiting bad design HMI

Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
high	medium	SW	T

Potential acceptance criteria

Must be avoided

Possible mitigation

Training, UI tests

You are likely affected if...

- training of border guards is limited to standard cases and does not include exceptional, ambigious, or inconsistent cases

Process step			**Id.No.**
Overall system			88
Process step description			
n/a			
Threat Description			
An unlawful cooperation between the border control agent and the passenger lead to the bypassing of all security measures .			
Consequence or Impact			
generic insider attack			
Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
high	medium	PEOPLE	T
Potential acceptance criteria			
Not applicable			
Possible mitigation			
Security clearances, segreggation of duties, job rotation, ...			
You are likely affected if...			
- involved personnel or contractors have no security clearance			

Process step Overall system			**Id.No.** 89
Process step description n/a			
Threat Description System could operate in an unlawful manner (accidentially or deliberately)			
Consequence or Impact illicit person could pass the border			
Damage Potential low	**Exploitability** low	**Affected Components** OTHER	**STRIDE** R
Potential acceptance criteria Not applicable			
Possible mitigation Acceptance by legal/compliance officer			
You are likely affected if... - there is a tendency to automatically follow the reasoning of the ABC system			

Process step			**Id.No.**
Overall system			90
Process step description			
n/a			
Threat Description			
A Passport, token or parts of passport (chip) can be used several times or at the ABC system and manual border.			
Consequence or Impact			
illicit person could pass the border			
Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
high	medium	SW	T
Potential acceptance criteria			
Must be avoided			
Possible mitigation			
History check through log files and particular alerts			
You are likely affected if...			
- detection of multiple usage of the same passport within a certain time window is disabled			

Process step			**Id.No.**
Overall system			91
Process step description			
n/a			
Threat Description			
An unprotected/not surveillanced kiosk can be subject to vandalism.			
Consequence or Impact			
Overall process slowed down, maintanace work necessary			
Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
medium	high	HW+SW	D
Potential acceptance criteria			
Must not happen unobserved			
Possible mitigation			
CCTV, security staff			
You are likely affected if...			
- kiosks are not sufficiently protected against vandalism - kiosks are not directly surveilled			

Process step			**Id.No.**
Overall system			92
Process step description			
n/a			
Threat Description			
The eGate systems efficiency is not sufficient and its operation leads to long queues (this is essential because one passenger ship could impose that the border will be crossed by over 2000 people)			
Consequence or Impact			
denial of service to enforce manual inspection			
Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
low	medium	HW+SW	D
Potential acceptance criteria			
Must be avoided			
Possible mitigation			
"load tests" under real circumstances			
You are likely affected if...			
- there was no comprehensive high pressue test of the system			

Process step			**Id.No.**
Overall system			93
Process step description			
n/a			
Threat Description			
Privacy and data protection risks are not continuously assessed and mitigated on time in the course of the data processing activity			
Consequence or Impact			
Data protection breach			
Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
low	low	OTHER	R
Potential acceptance criteria			
Not applicable			
Possible mitigation			
Acceptance by legal/compliance officer			
You are likely affected if...			
- there is no explict data protection policy - the data protection policy lacks certain elements, in particular continous improvement			

Process step			**Id.No.**
Overall system			94
Process step description			
n/a			
Threat Description			
The process steps do not follow a predefined order/ruleset; eg opening a door should only be allowed if the predecessor step was conducted successfully			
Consequence or Impact			
could create unforesable system behaviour			
Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
high	low	HW+SW	T
Potential acceptance criteria			
Must be avoided			
Possible mitigation			
Exhaustive testing; control of process sequence against reference			
You are likely affected if...			
- there is no mechanism that would check the correct order of process or that would alert the operator about any failure in this respect			

Process step			**Id.No.**
Overall system			95
Process step description			
n/a			
Threat Description			
Kiosk and eGate components can be subject to IEMI attacks			
Consequence or Impact			
denial of service attack			
Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
medium	medium	HW+SW	D
Potential acceptance criteria			
Must be avoided			
Possible mitigation			
Physical protection must withstand the most likely attacks			
You are likely affected if…			
- the system has not demonstrated to be resilient against IEMI attacks			

Process step	**Id.No.**
Overall system	96

Process step description

n/a

Threat Description

Missing guidance and training of bordergards in repsect to the operation of the eGate System could lead to erroneous actions

Consequence or Impact

Confusion could be exploited for illegal border crossing

Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
medium	low	PEOPLE	T

Potential acceptance criteria

Must be avoided

Possible mitigation

Training, UI tests

You are likely affected if...

- training of border guards is limited to standard cases and does not include exceptional, ambigious, or inconsistent cases

Process step	**Id.No.**
Overall system	97

Process step description

n/a

Threat Description

Process is interrupted at any point and for whatever reason and the passenger is left in an unclear situation about his/her data

Consequence or Impact

Unlawful processing of personal data; Data subjects hindered to exercise their rights.

Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
low	low	PEOPLE	I

Potential acceptance criteria

Must be avoided

Possible mitigation

Satemachine

You are likely affected if...

- the system cannot demonstrate to properly handle data even in extreme or emergency cases

Process step			**Id.No.**
Overall system			98
Process step description			
n/a			
Threat Description			
False positive match with a wanted individual could lead to harmful situation for the traveller, e.g. wrong attribution of SIS results			
Consequence or Impact			
passenger could falsly be accused			
Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
low	low	PEOPLE+SW	S
Potential acceptance criteria			
Must be avoided			
Possible mitigation			
Training, UI tests			
You are likely affected if...			
- there is a tendency to automatically follow the reasoning of the ABC system			

Process step			**Id.No.**
Overall system			99
Process step description			
n/a			
Threat Description			
Lack, incompleteness or inconsistency of data protection policy and its implementation			
Consequence or Impact			
Unlawful processing of personal data; Data subjects hindered to exercise their rights.			
Damage Potential	**Exploitability**	**Affected Components**	**STRIDE**
low	low	OTHER	R
Potential acceptance criteria			
Not applicable			
Possible mitigation			
Acceptance by legal/compliance officer			
You are likely affected if...			
- there is no explict data protection policy - the data protection policy lacks certain elements - the adherence to the data protection policy is not regularily monitored			

References

[1] Security Evaluation (Version 1). FastPass Deliverable D10.2, FastPass Consortium (2015)

[2] Security Evaluation (Final). FastPass Deliverable D10.6, FastPass Consortium (2017)

[3] A. Shostak: Threat Modeling – designing for security. Wiley, Indianapolis (2014)

List of abbreviations and definitions

ABC Automated Border Control

MRTD Machine Readable Travel Documents

List of figures

Europe Direct is a service to help you find answers to your questions about the European Union.

Freephone number (*)**:**

00 800 6 7 8 9 10 11

(*) The information given is free, as are most calls (though some operators, phone boxes or hotels may charge you).

More information on the European Union is available on the internet (http://europa.eu).

HOW TO OBTAIN EU PUBLICATIONS

Free publications:

- one copy:
  via EU Bookshop (http://bookshop.europa.eu);
- more than one copy or posters/maps:
  from the European Union's representations (http://ec.europa.eu/represent_en.htm);
  from the delegations in non-EU countries (http://eeas.europa.eu/delegations/index_en.htm);
  by contacting the Europe Direct service (http://europa.eu/europedirect/index_en.htm) or
  calling 00 800 6 7 8 9 10 11 (freephone number from anywhere in the EU) (*).

  (*) The information given is free, as are most calls (though some operators, phone boxes or hotels may charge you).

Priced publications:

- via EU Bookshop (http://bookshop.europa.eu).

JRC Mission

As the science and knowledge service of the European Commission, the Joint Research Centre's mission is to support EU policies with independent evidence throughout the whole policy cycle.

EU Science Hub
ec.europa.eu/jrc

@EU_ScienceHub

EU Science Hub - Joint Research Centre

Joint Research Centre

EU Science Hub

Publications Office