PROTECT (Pervasive and UseR Focused BiomeTrics BordEr ProjeCT)

Dumortier, Franck

Publication date:
2018

Document Version
Publisher's PDF, also known as Version of record

PROTECT

Pervasive and UseR Focused BiomeTrics BordEr ProjeCT

(PROTECT)

H2020 – 700259

D2.2 Legal framework of biometric border control

Author: Franck Dumortier (UNAMUR)

Deliverable nature:	Report
Dissemination level: (Confidentiality)	PU
Version:	1.0
Date:	14/03/2018
Keywords:	Privacy, data protection, Schengen Border Code, Entry/exit conditions, travel documents, EU border control databases, SIS, VIS, EES, EURODAC, API, ETIAS

Executive summary

This document is Deliverable D2.2 of Task T2.2, WP2 – Privacy of the PROTECT project. The aim of D2.2 is to explore the current and proposed European legal framework regulating biometric Schengen border control in order to identify legal, privacy and data protection constraints which should be taken into account by PROTECT scenarios described in D3.1[1].

In order to be able to identify the legal constraints under current and proposed EU law for the usage of the multimodal biometric "on the move" solutions developed within the PROTECT project scenarios in D3.1, the first preliminary question which should be raised is: "Which is the exact purpose/extent of the border checks that could be "facilitated" thanks to the PROTECT system?". Indeed, according to article 5 of the General Data Protection Regulation (GDPR), one of the main principles relating to the processing of personal data is the purpose limitation principle, according to which *"personal data shall be collected for specified, explicit and legitimate purposes".*

In this Deliverable, it is assumed that the purpose of D3.1 scenarios is to "facilitate" public border control authorities to speed up their public interest missions of border control management by enrolling additional biometrics in travel documents (or smartphone apps acting as travel documents).

Bearing this public interest purpose fact in mind, the purpose of this Deliverable is to thoroughly analyse:

- Legal constraints deriving from legislation regulating EU travel documents (E-Passports, residence permits, visas), Schengen IT systems (in particular, VIS, SIS, EES, SLTD, API and ETIAS) and more generally legislation regulating cross-border movements at the Schengen external borders (the Schengen Borders Code)
- Legal privacy constraints related to the collection, storage and processing of personal data for public interest missions, in particular biometric data. These legal constraints are mainly regulated by article 8 of the European Convention on Human Rights, Directive 95/46/EC and the General Data Protection Regulation (GDPR).

Without any will to pre-empt any conclusions, it is a fact that the scenarios proposed by D3.1 should more than certainly be considered as beyond the scope of current EU legislation. One of the main reasons of this conclusion is that consent of travellers cannot be considered as a legitimate basis of lawfulness under the GDPR to allow public border control authorities to speed up their public interest missions by enrolling additional biometrics in travel documents (which currently may not be replaced by a smartphone app).

This being said, Deliverable "D2.3 - Privacy impact of next-generation biometric border control" will analyse if, as an alternative to D3.1 scenarios, emerging biometric modalities could be processed in a "passport companion" such as a smartphone for "comfort and convenience purposes" of travellers on basis of their consent. The idea would be to analyse − from a privacy and data protection point of view − the possibility and the conditions to enrol additional biometrics in a smartphone app for travellers willing to join a "PROTECT programme" allowing them to be given priority in waiting areas for "traditional" security and border checks and/or allowing them to benefit of additional convenience services such as access to VIP parking zones or waiting lounges.

[1] D3.1 - User requirements and scenarios.

Document Information

Project Number	H2020 - 700259	**Acronym**	PROTECT
Full Title	Pervasive and UseR Focused BiomeTrics BordEr ProjeCT		
Project URL	http://www.projectprotect.eu/		
Document URL			
EU Project Officer	Agnieszka Marciniak		

Date of Delivery	**Contractual**	M15	**Actual**	M19

Authors (names and affiliations)	**Franck Dumortier (UNAMUR)**

Reviewers (names and affiliations)	

Version Log			
Issue Date	**Rev. No.**	**Author**	**Change**
28/11/2017	V1.0	Franck Dumortier	First sections of D2.2 submitted for review of D3.1 scenarios.
14/03/2018	V2.0	Franck Dumortier	Modification of the document due to changes of scenarios in D3.1 as well as changes in EU regulation (including Entry-Exit System).

Table of Contents

List of figures

List of tables

Abbreviations

CFR	Charter of Fundamental Rights
ECHR	European Convention of Human Rights
ECtHR	European Court of Human Rights
ECJ	European Court of Justice
EDPS	European Data Protection Supervisor
EEA	European Economic Area
EES	Entry-exit system
ETIAS	The European Travel Information and Authorisation System
EU	European Union
GDPR	General Data Protection Regulation
ICAO	International Civil Aviation Organization
IBM	Integrated Border Management
MS	Member State
SBC	Schengen Border Code
SIS	Schengen Information System
TCN	Third-Country National
TCNVE	Third-Country National Visa exempted
TCNVH	Third-Country National Visa holder
VIS	Visa Information System
WP29	Article 29 Working Party
PROTECT	Pervasive and UseR Focused BiomeTrics BordEr ProjeCT

Definitions

Article 29 Working Party: The Article 29 Working Party is composed of representatives from all EU Data Protection Authorities, the EDPS and the European Commission. It was set up under the Directive 95/46/EC. It has advisory status and acts independently.

Automated Border Control system: means a system which allows for an automated border passage, and which is composed of a self-service system and an eGate.

Biometric data: Article 4(14) of the GDPR defines "biometric data" *as personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.*

Biometric template: Key features can be extracted from the raw form of biometric data (e.g. facial measurements from an image) and stored for later processing rather than the raw data itself. This forms the biometric template of the data. The definition of the size (the quantity of information) of the template is a crucial issue. On the one hand, the size of the template should be wide enough to manage security (avoiding overlaps between different biometric data, or identity substitutions), on the other hand, the size of the template should not be too large so as to avoid the risks of biometric data reconstruction. The generation of the template should be a one-way process, in that it should not be possible to regenerate the raw biometric data from the template.

Biometric enrolment: Encompasses all the processes that are carried out within a biometric system in order to extract biometric data from a biometric source and link this data to an individual. The quantity and the quality of data required during enrolment should be sufficient to allow for his/her accurate identification, authentication, categorization or verification without recording excessive data. The amount of data extracted from a biometric source during the enrolment phase has to be adequate for the purpose of the processing and the level of performance of the biometric system.

Biometric storage: The data obtained during enrolment can be stored locally in the operations centre where the enrolment took place (e.g. in a reader) for later use, or on a device carried by the individual (e.g. on a smart card) or could be sent and stored in a centralized database accessible by one or more biometric systems.

Biometric matching: It is the process of comparing biometric data/template (captured during enrolment) to the biometric data/template collected from a new sample for the purpose of identification, verification/authentication or categorization.

Biometric identification: The identification of an individual by a biometric system is typically the process of comparing biometric data of an individual (acquired at the time of the identification) to a number of biometric templates stored in a database (i.e. a one-to-many matching process).

Biometric verification/authentication: The verification of an individual by a biometric system is typically the process of comparing the biometric data of an individual (acquired at the time of the verification) to a single biometric template stored in a device (i.e. a one-to-one matching process).

eGate: means an infrastructure operated by electronic means where the effective crossing of an external border takes place.

European Travel Information and Authorisation System (ETIAS): The system will apply to visa-exempt third country nationals, as well as those who are exempt from the airport transit visa requirement. They will need to obtain a travel authorisation before their trip, via an online application. The information submitted in each application will be automatically processed against other EU databases to determine whether there are grounds to refuse a travel authorisation. When no hits or elements requiring further analysis are identified, the travel authorisation will be issued automatically within a short time. If there is a hit or an element requiring analysis, the application will be handled manually by the competent authorities.

Facial image: means digital images of the face with sufficient image resolution and quality to be used in automated biometric matching.

EURODAC: The EURODAC system enables the comparison of fingerprints of asylum applicants and illegal immigrants. The Members States of the system are the 28 EU members, Iceland, Norway, Liechtenstein and Switzerland. The objective of Eurodac in the asylum process is to facilitate the application of the Dublin III Regulation. This Regulation provides a mechanism for determining which country is responsible for examining applications for international protection lodged in one of the member states.

European Data Protection Supervisor: The European Data Protection Supervisor (EDPS) is an independent institution of the EU, responsible under Article 41(2) of Regulation 45/2001 'With respect to the processing of personal data… for ensuring that the fundamental rights and freedoms of natural persons, and in particular their right to privacy, are respected by the Community institutions and bodies', and '…for advising Community institutions and bodies and data subjects on all matters concerning the processing of personal data'. Under Article 28(2) of Regulation 45/2001, the Commission is required, 'when adopting a legislative Proposal relating to the protection of individuals' rights and freedoms with regard to the processing of personal data...', to consult the EDPS.

Entry-Exit System: the Entry/Exit System (EES) is a system to register entry and exit data and refusal of entry data of third country nationals crossing the external borders of the Member States of the European Union and determining the conditions for access to the EES for law enforcement purposes.

General Data Protection Regulation (GDPR): On 4 May 2016, the official text of the Regulation has been published in the EU Official Journal in all the official languages. The Regulation will enter into force on 24 May 2016. The objective of this new set of rules is to give citizens back control over of their personal data, and to simplify the regulatory environment for business. The data protection reform is a key enabler of the Digital Single Market which the Commission has prioritized. The reform will allow European citizens and businesses to fully benefit from the digital economy.

Multi-modal biometrics: They can be defined as the combination of different biometric technologies to enhance the accuracy or performance of the system (it is also called multilevel biometrics). Biometric systems use two or more biometric traits / modalities from the same individual in the matching process. These systems can work in different ways, either collecting different biometrics with different sensors or by collecting multiple units of the same biometric.

Personal data: Article 4(1) of the GDPR defines "personal data" as *any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*.

Processing: Article 4(14) of the GDPR defines "processing" as *any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction*.

Schengen Area: The Schengen Area is one of the greatest achievements of the EU. It is an area without internal borders, an area within which citizens, many non-EU nationals, business people and tourists can freely circulate without being subjected to border checks. Since 1985, it has gradually grown and encompasses today almost all EU States and a few associated non-EU countries. While having abolished their internal borders, Schengen States have also tightened controls at their common external border on the basis of Schengen rules to ensure the security of those living or travelling in the Schengen Area.

Schengen Border Code: The Schengen Borders Code governs the crossing of the external border, facilitating access for those who have a legitimate interest to enter into the EU. A special Local Border Traffic Regime

has also been established to facilitate entry for non-EU border residents who frequently need to cross the EU external border. A common visa policy further facilitates the entry of legal visitors into the EU.

Sensitive personal data: Article 9(1) of the GDPR defines "sensitive personal" data as *personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.*

Schengen Information System: The Schengen Information System (SIS) is a large-scale information system that supports external border control and law enforcement cooperation in the Schengen States. The SIS enables competent authorities, such as police and border guards, to enter and consult alerts on certain categories of wanted or missing persons and objects. An SIS alert not only contains information about a particular person or object but also clear instructions on what to do when the person or object has been found. Specialised national SIRENE Bureaux serve as single points of contact for any supplementary information exchange and coordination of activities related to SIS alerts.

Self-service system: means an automated system which performs all or some of the border checks that are applicable to a person.

Visa Information System (VIS): The Visa Information System (VIS) allows Schengen States to exchange visa data. It consists of a central IT system and of a communication infrastructure that links this central system to national systems. VIS connects consulates in non-EU countries and all external border crossing points of Schengen States. It processes data and decisions relating to applications for short-stay visas to visit, or to transit through, the Schengen Area. The system can perform biometric matching, primarily of fingerprints, for identification and verification purposes.

1 Introduction

The main message of this deliverable is to remind PROTECT partners that borders are the result of a human legal construction. Originally, the earth was a globe on which people could naturally freely walk around. Therefore, the general principle of the Universal Declaration of Human Rights (UDHR)[2] is that everyone has the right to freedom of movement and residence within the borders of each state and the right to leave any country, including his own, and to return to his country.[3] Hence, it has to be known that border control checks have huge impacts on fundamental rights, notably on right to dignity (Article 1 of the Charter of Fundamental Rights[4] of the EU, hereafter "CFR"); right to liberty and security (Article 6 CFR), respect for private and family life (Article 7 CFR), the protection of personal data (Article 8 CFR), right to asylum (Article 18 CFR), protection in the event of removal, expulsion or extradition (Article 19 CFR), the right to non-discrimination (Article 21 CFR), the rights of the child (Article 24 of the Charter) and the right to an effective remedy (Article 47 CFR). Of course, these fundamental rights are not absolute but their respect remain the principle and any interference with them must be carefully assessed.

This general principle being recalled, it has to be acknowledged that the EU is facing the most severe migration crisis since the Second World War.[5] In addition, terrorist attacks that have occurred on EU territory have heightened security concerns.[6] These events have prompted the EU Commission to consider several initiatives which include the creation of new large-scale EU information systems for border control management[7], the modification of existing ones[8] as well as the interoperability of all these systems.

---

[2] The Universal Declaration of Human Rights (UDHR) is a milestone document in the history of human rights. Drafted by representatives with different legal and cultural backgrounds from all regions of the world, the Declaration was proclaimed by the United Nations General Assembly in Paris on 10 December 1948 (General Assembly resolution 217 A) as a common standard of achievements for all peoples and all nations.

[3] Art. 13 UDHR.

[4] European Union, Charter of Fundamental Rights of the European Union, 26 October 2012, 2012/C 326/02.

[5] See p. 1. of the "Legislative train: 8 towards a new policy on migration" available at http://www.europarl.europa.eu/legislative-train/pdfs/legislative-train-schedule-theme-towards-a-new-policy-on-migration-12-2017.pdf

[6] EDPS, Reflection paper on the interoperability of information systems in the area of Freedom, Security and Justice, 17 November 2017, p.5,
available at https://edps.europa.eu/sites/edp/files/publication/17-11-16_opinion_interoperability_en.pdf

[7] See for instance Regulation (EU) 2017/2225 of the European Parliament and of the Council of 30 November 2017 amending Regulation (EU) 2016/399 as regards the use of the Entry/Exit System; Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011, Proposal for a Regulation of the European Parliament and of the Council establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 515/2014, (EU) 2016/399, (EU) 2016/794 and (EU) 2016/1624, COM (2016) 731 final.

[8] See for instance the SIS legislative package consisting of (i) the Proposal for a Regulation of the European Parliament and of the Council on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, amending Regulation (EU) No 515/2014 and repealing Regulation (EC) No 1987/2006, COM(2016) 882 final; (ii) the Proposal for a Regulation of the European Parliament and of the Council on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending Regulation (EU) No 515/2014 and repealing Regulation (EC) No 1986/2006, Council Decision 2007/533/JHA and Commission Decision 2010/261/EU, COM(2016) 883 final and (iii) the Proposal for a Regulation of the European Parliament and of the Council on the use of the Schengen Information System for the return of illegally staying third country nationals, COM(2016) 881 final. See also the Proposal for a Regulation of the European Parliament and of the Council on amending Regulation (EU) No 603/2013 on the establishment of Eurodac for the comparison of fingerprints for the effective application of [Regulation (EU) No 604/2013] establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of

In this general context, it is worth mentioning that already on 19 and 20 June 2003, the European Council of Thessaloniki stated that *"a coherent approach is needed in the European Union on biometric identifiers or biometric data for documents for third country nationals, European Union citizens' passports and information systems"*.[9]

The reasons why the EU is increasingly pushing for a coherent approach of using the same biometrics in both travel documents and IT-systems are the following:

- Alphanumerical data can be unreliable for establishing the identity of a person, due to many so-called aliases, cases of identity fraud, entry and spelling mistakes. The power of biometric data lies in their capacity to serve as universal identifiers allowing the same information about the same person to be linked across different information sources;
- The use of the same biometric features (fingerprints and facial image) in travel documents and IT-systems is considered to make the matching for background checks significantly more reliable. As Table 1 shows, this reason leads travel documents and EU border IT-systems to increasingly rely on fingerprints and facial image of travellers to have a coherent approach of identity-management at external borders crossings.

The table below illustrates biometrics being/or planned to be stored in EU travel documents and IT-systems for border control.

Travel document/IT system	Biometrics included
EU passport	Fingerprints and facial image
Residence permit	Fingerprints and facial image
Schengen visa	Not in the sticker itself but inclusion of biometrics in the VIS during the visa application
VIS	Fingerprints, photographs (facial image in the future)
SIS II (immigration control)	Fingerprints (and facial image according to SIS II proposal on borders)
EES	Fingerprints and facial image

Table 1 - Biometric data in current travel documents and IT- border control management systems

Since the goal of the "PROTECT solution" is to develop an enhanced contactless biometric-based person identification system at external border crossings involving the processing of "additional" biometric data (other than fingerprints and facial image), the main issues highlighted in this deliverable are the right to respect for private life (Article 7 CFR and Article 8 of the European Convention on Human Rights[10] – hereafter "ECHR") and the right to the protection of personal data (Article 8 CFR).

the Member States by a third country national or a stateless person, for identifying an illegally staying third country national or stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, COM(2016)272 final.

[9] The Presidency conclusions of the Thessaloniki European Council of 19 and 20 June 2003 are available at http://data.consilium.europa.eu/doc/document/ST-11638-2003-INIT/en/pdf

[10] Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 4 November 1950, ETS 5.

The collection and storage of additional personal biometric data envisaged by the "PROTECT solution" clearly amounts to an interference with the right to private life under the CFR and the ECHR. As a reminder, the European Court of Human Rights (hereafter ECtHR) has held that the *"mere storing of data relating to the private life of an individual amounts to an interference within the meaning of Article 8"*.[11] The subsequent use of the stored information has no bearing on that finding.[12] Rather, the access to that data by authorities forms a further interference with the right to privacy.[13] In terms of finding interference, it is irrelevant whether the information collected is sensitive or not or whether or not persons concerned have been inconvenienced in any way.[14]

Furthermore, in S & Marper v the UK, the ECtHR held that biometric features constitute personal data containing *"certain external identification features"* which contain *"unique information about the individual concerned [sic] allowing his or her identification [to be made] with precision in a wide range of circumstances".*[15] Biometric features hence belong to a special category of more sensitive data.[16] In relation to the decentralised storage of biometrics in passports, the European Court of Justice (ECJ) likewise held that the processing of fingerprints constituted "a threat" to the right to respect for private life and the right to protection of personal data, as biometrics play an important role in the field of identifying persons in general.[17] The ECJ has also indicated that central storage of biometrics would need to comply with more stringent requirements than their storage in the passport itself.[18]

In the same way, the General Data Protection Regulation (GDPR)[19] considers biometric data as personal data being sensitive.[20] In the GDPR, "biometric data" are defined as *"personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data".* In accordance with the GDPR definition, measures of biometric identification or their digital translation in a template form can always be considered as "information relating to a natural person" as it concerns data, which provides, by its very nature, information about a given person.[21] For this reason, the processing of biometric data needs to carefully comply with the data protection principles enshrined in EU and national law.

As the activities proposed by the "PROTECT solution" amount to an interference with the rights to private life and to data protection, the PROTECT scenarios described in D3.1 must fulfil the tests of legality, necessity and proportionality in order to be lawful. Indeed, article 8(2) ECHR sets out the grounds the State may interfere with the right to privacy: *"There shall be no interference by a public authority with the existence of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention or detection of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others".*

[11] ECtHR, S. v Marper v the United Kingdom, para. 67.
[12] Amann v Switzerland [GC], no. 27798/95, ECtHR 2000-II, at para. 69, and S. and Marper v the UK. Cases C:465/00, C:138/01 and C:139/01, Österreichischer Rundfunk and Others, EU:C:2003:294, para. 75.
[13] Leander v Sweden, ECtHR (1987), Series A, no. 116, at para. 48. Joined Cases C-293/12 (Digital Rights Ireland) and C-594/12 (Kärtner Landesregierug), EU:C:2014:238, para. 35.
[14] Österreichischer Rundfunk and Others, EU:C:2003:294, para. 75; Digital Rights Ireland, EU:C:2014:238, para. 33.
[15] ECtHR, S. & Marper v the United Kingdom, para. 84.
[16] ECtHR, S. & Marper v the United Kingdom, para. 103.
[17] ECJ, C-291/12, Schwarz v. Bochum, 17 October 2013, paras 23-30.
[18] ECJ, C-291/12, Schwarz v. Bochum, 17 October 2013, paras 59-63.
[19] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
[20] On 4 May 2016, the official texts of the Regulation and the Directive have been published in the EU Official Journal. The GDPR entered into force on 24 May 2016, it shall apply from 25 May 2018.
[21] Article 29 Working Party, Opinion 4/2007 on the concept of personal data, WP 136, Adopted on 20th June 2007, p. 8.

The ECtHR has set out three criteria which must be satisfied to ensure that any interference is in compliance with Art. 8(2). An interference must be:

1. in accordance with the law,
2. in pursuit of one of the legitimate aims set out in Art. 8(2), and
3. necessary in a democratic society.

For these reasons, two types of legal constraints should be taken into account by the PROTECT scenarios described in Deliverable D3.1:

- Legal constraints deriving from legislation regulating EU travel documents (ePassports, residence permits, visas), Schengen IT systems (in particular, SIS, SLTD, API, VIS, EES and the ETIAS proposal) as well as legislation regulating cross-border movements at the Schengen external borders (the Schengen Borders Code – hereafter "SBC");
- Legal privacy constraints related to the purpose, collection, storage and processing of additional biometric data being developed in the context of the PROTECT project. These legal constraints are mainly regulated by article 8 of the European Convention on Human Rights, Directive 95/46/EC and the General Data Protection Regulation (GDPR).

These two types of legal constraints which should be taken into account by the PROTECT scenarios mainly amount to analyse whether the additional biometrics (other than fingerprints and facial image) which are envisaged to be processed respect the data minimisation principle enshrined in article 5(c) of the GDPR. According to this principle, personal data must be *"adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed".*

1.1 Concept of PROTECT

The potential of implementing contactless multimodal biometrics at external border crossing (PROTECT system) points was stated by the European Commission, which expressed it as follows in the H2020 call "BES-6-2015: Border crossing points, topic 2: Exploring new modalities in biometric-based border checks".[22]

"Research is needed in order to explore whether it is possible to use other biometric data (potentially already used in another context and in another domain) than fingerprint, iris or facial picture to store in the e-Passport chip, which would guarantee the same or higher level of security, but would be more accurate and could be retrieved in a more efficient manner than in the case of the conventionally used biometric data types. In addition, practical experiences lead to the assumption that for non-critical travellers (EU, bona-fide etc.) a most fluent non-intrusive control process is desired. Therefore, to increase accuracy, in this case the use of contactless techniques (e.g. face, 3D face, iris) and multi-biometric fusion is likely to be preferred over contact-based technologies".

The PROTECT concept has been designed in order to address these needs stated by the Commission, even though it is regrettable that the call considered explicitly EU passengers as being "non-critical travellers". Indeed, recently, Regulation (EU) 2017/458[23] reinforced checks of EU passengers at external borders to take into account the phenomenon of foreign terrorist fighters, many of whom are Union citizens. In any case, in the proposal, the consortium proposed to develop a multimodal biometric solution for identity confirmation "on the move" of travellers with the aim to facilitate the Schengen Area external cross-border movements. The system should, therefore, process various "emerging" biometric modalities which could be processed in

[22] Information about the purpose of the H2020 call "BES-6-2015: Border crossing points, topic 2: Exploring new modalities in biometric-based border checks" is available at http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/bes-06-2015.html

[23] Regulation (EU) 2017/458 of the European Parliament and of the Council of 15 March 2017 amending Regulation (EU) 2016/399 as regards the reinforcement of checks against relevant databases at external borders

a contactless-way. For the purposes of multimodal biometric ID verification, the initial plan was to include such biometrics as: face recognition, iris recognition, vein pattern recognition, speaker recognition as well as anthropometric recognition. When operational, the beneficiaries of the multimodal biometric system being developed within the PROTECT project should be persons enjoying the Union right of free movement as well as third country nationals (TCNs). The system should be deployed in Automated Border Control (ABC) areas supporting border guards to facilitate smooth and non-intrusive rapid crossing by travellers based on deployment of the next generation of biometric identification detection methods. The ability for the system to efficiently process "low-risk travellers" – a concept which is not defined in the DoA and which has no legal definition –, combined with increased levels of accuracy, security and privacy standards and enabling border guards to concentrate resource on "higher-risk travellers" – a concept which is also not defined in the DoA – , are central ambitions of the project.

Bearing these objectives and ambitions in mind, the H2020 call BES-6-2015 also specified that ethical, societal and data protection aspects should be integral part of the research by stating that "w*hile the introduction of new biometric-based modalities in the process of person identification might lead to making this process more accurate and efficient, an integral part of the research should also embrace the related ethical, societal and data protection aspects".*

1.2 PROTECT scenarios described in D3.1

1.2.1 General overview

Chapter 8 of "Deliverable D3.1 - System requirements specification and scenarios" (hereafter D3.1) provides an overview of the PROTECT demonstration and scenarios. PROTECT demonstrations have been divided into two types: A (air and sea border) and B (land border). Both A and B types of demonstrations are using a Biometric Capture Area (BCA) and testing the 1) ePassport and 2) mobile device scenario. The figure below represents this overall approach.

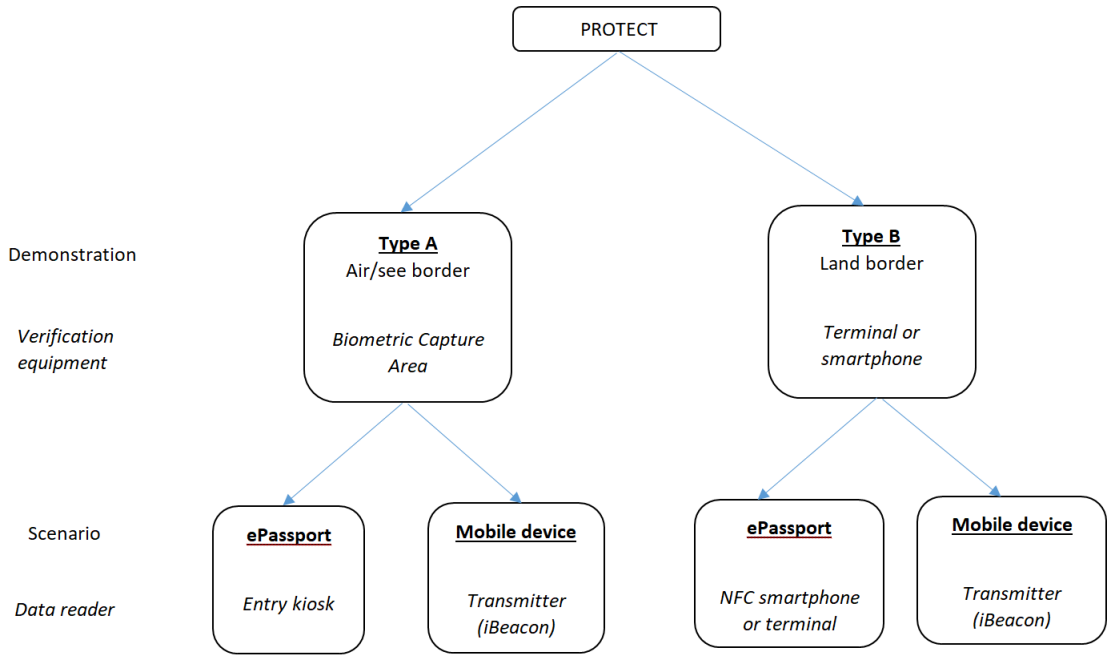

Figure 1 - PROTECT scenario and demonstration hierarchy

In more detail, the division of demonstration types A and B in D3.1 is the following:

- **Type A** ('Walk-Through Border Crossing'), where individual travellers proceed on foot, with or without baggage, from an aircraft, ship, train, vehicle or direct to and from another country as pedestrians and are examined for admissibility into – or exit from – the EU under the Schengen Borders Code or other relevant legislation.
- **Type B** ('Drive-Through Border Crossing'), where one or more travellers proceed inside a vehicle or on a wheeled conveyance through an EU external border crossing point and are examined for exit from – or admissibility into – the EU under the Schengen Borders Code or other relevant legislation.

For both types A and B demonstrations, Section 8.4 of D3.1 describes in illustrated terms the enrolment and verification phases of the 1) ePassport and 2) mobile device scenario.

1.2.2 Enrolment phase

According to D3.1, the enrolment phase would only be performed once during the lifetime of the electronic passport. Prior to the enrolment process, each passenger interested in using the PROTECT solution would be required to give formal consent for data collection and will know exactly the purpose and limits of government use of their personal data. They would be able to withdraw consent at any time during the process and be satisfied that their data will be protected and deleted where necessary.

1.2.2.1 Passport scenario

In this scenario, a passenger (EU national or third country national) holding a 4th generation electronic passport eligible for the PROTECT programme who wishes to travel to (or from) a Schengen country and would like to use the "PROTECT" solution for the first time should register via an enrolment kiosk. During the enrolment process, this passenger would undergo a background check in relevant European and national databases. Once this pre-verification is concluded with a positive result, the system would verify the electronic passport and passenger's biometric features with the templates stored on the chip. The entire enrolment process would be supervised by a border guard to provide assistance and monitor whether the process goes as planned. The positive results of the prior step would allow the passenger for the registration of additional biometric features that are applied in the PROTECT solution. The anthropometric and gait features collection requires walking through the Biometric Capture Area. The new set of data would be saved at the passenger's electronic passport.

1.2.2.2 Mobile device scenario

In this scenario, a passenger who wishes to use the PROTECT solution with the application of mobile device when travelling to (from) a Schengen country would need to install the official PROTECT app first. Once the passenger reaches the kiosk, the essential step is to establish a secure connection between the kiosk and the passenger's mobile device. In order to establish the connection, the passenger would scan the barcode that appears on the kiosk's display. Once the connection is established, the passenger would be required to scan the passport in order to read the data. Passport authenticity would be verified. The passenger would then be verified in relevant European and national databases. Following a positive verification, passenger's existing biometric data stored in the passport would be verified in the kiosk. The entire enrolment process would be overseen by a border guard, as for the Passport scenario. The next step would involve a proper collection of additional biometric features that are required by the PROTECT system. The collection of anthropometric and gait features requires walking through the Biometric Capture Area. Successfully enrolled and encrypted data would finally be transferred to the PROTECT app on passenger's mobile application.

1.2.3 Verification at air and sea border (type A)

1.2.3.1 Passport scenario

When considering the verification process, the first step would require the passenger to approach the kiosk in order to read the data from the new generation passport. This step is to ensure all necessary data for PROTECT verification are on the passport. In case additional data are required, they could be added in the

kiosk. The set of data read out from the electronic passport would be transmitted to the local border control system for the purposes of the traveller verification. Once the data are successfully transmitted to the border control system, the passenger would be allowed to walk through the biometric capture area. The PROTECT sensor lane verifies the biometric features stored in the passport against the data collected by the PROTECT system. The verification is carried out while the passenger is on-the-move. The process is supervised by a border guard who monitors the process and handles the exceptions. Once the verification is completed with a positive score, the data are removed from the temporary database.

1.2.3.2 Mobile device scenario

The verification process with the use of passenger's mobile device is slightly more advanced when compared to the passport scenario. The process begins with the traveller arriving at the destination airport or port. The traveller gets off the plane or disembarks the ship and heads toward the Biometric Capture Area. Once the traveller is in the close vicinity of the Biometric Capture Area, the PROTECT app on the passenger's mobile device processes the signals sent by the iBeacon so that the system is informed that the passenger is about to cross the Biometric Capture Area. Then, the PROTECT app transfers the set of encrypted passport and biometric data to the local border control system. The transferred data are temporarily stored in border control system only for traveller verification purposes in the Biometric Capture Area. Once the passenger crossed the Biometric Capture Area and has been successfully verified, the data are removed from the border control system.

1.2.4 Verification Process at land border crossing points (type B)

1.2.4.1 Passport scenario

A traveller in a vehicle approaches the land border crossing point and stops at the border control post. The border guard may remain in the booth. The traveller will be requested to submit the personal data to the border guard. This might be done via 2 methods. Either the passport data can be transmitted via traveller smartphone or via dedicated terminal at border crossing point. The data are transferred to the local border control system. Following the successful data transmission, the next step is the biometric verification procedure. This step is performed either by capturing all of the requested data by the sensors in the biometric terminal alongside and external to the vehicle or by submitting the biometric features via mobile device. More in-depth analysis of submitting the biometric data through mobile device is presented in Deliverable D6.7. The border guard is presented all the data submitted by a traveller in real-time. Following a successful check, the passenger data are deleted from the local border control system.

1.2.4.2 Mobile device scenario

The traveller in a vehicle drives towards the land border crossing point and stops at the border post. The border guard may remain inside the border control booth. With the help of PROTECT app, the traveller will communicate with the local border control system and submit all requested biographical and biometric data. The application will allow the traveller to transmit additional data to the border guard if need be. Biometric verification will be performed at the dedicated terminal positioned alongside and external to the vehicle, which will have integrated biometric sensors. An alternative method of capturing traveller biometric data is the use of mobile device and using the incorporated sensors for such purposes. Following a positive verification, the passenger might proceed his/her journey. The data are removed from the local database.

1.3 Purpose of the document

This document is Deliverable D2.2 of Task T2.2, WP2 – Privacy of the PROTECT project. The aim of D2.2 is to explore the current and proposed European legal framework regulating both biometric border control and personal data protection in order to identify the legal constraints which should be taken into account by the scenarios being defined in Deliverable D3.1.

The main objective of the PROTECT project being to develop a contactless multimodal biometric solution for identity confirmation of travellers with the aim to facilitate and fasten their border crossings, it is essential to analyse the following main legal questions:

1) Under current EU law, is there a possibility for electronic machine-readable documents to support an enhanced set of contactless biometrics? In other words, could emerging biometrics (other than facial image and fingerprints) be included in travel documents under current EU law?
2) Under current EU law, could a smartphone be considered as a travel document to support traditional biometrics (fingerprints and facial image) as well as an enhanced set of contactless biometrics?
3) Under current EU law, could consent of a traveller be the legal basis to enrol additional biometrics in a travel document for "government use of their personal data"[24] ?
4) Under current EU law, which constraints related to the entry/exit external border checks for both persons enjoying the EU right to free movement and TCNs should be taken into account by the PROTECT scenarios?
5) Under current EU law, which constraints should be taken into account by the PROTECT scenarios when making use of technologies such as self-service systems, eGates and automated border control systems?
6) Under current EU law, which checks against databases should be taken into account by the PROTECT scenarios and which legal constraints derive from these in relation to the development of a contactless solution?
7) Does the PROTECT scenarios fit in with the EU's own future border control plans, in particular the EC's proposal for a Regulation on establishing a framework for interoperability between EU information systems?

.

1.4 Document scope

The document consists of an introduction and 4 main sections:

- **Section 2** presents the rules governing the format of EU travel documents and the biometric features included in these for the purpose of identifying the related legal constraints which should be taken into account by D3.1 scenarios;
- **Section 3** describes the current conditions of entry/exit to the Schengen Area of both persons enjoying the Union right of free movement and third country nationals for the purpose of identifying the related legal constraints which should be taken into account by D3.1 scenarios;
- **Section 4** provides for an overview of the EU databases and systems for border control management (SIS, VIS, EES, EURODAC, SLTD, API and ETIAS), the purposes of these and the information contained therein for the purpose of identifying the related legal constraints which should be taken into account by D3.1 scenarios;
- **Section 5** presents the recent EC's proposal for a Regulation on establishing a framework for interoperability between EU information systems, and in particular the proposed shared biometric matching service which is based on the two following biometric features: fingerprints and facial image.

[24] "government use of their personal data" is the sentence used in p. 71.

2 Format of EU travel documents and biometrics included

2.1 Introduction

As reminded in Section 1.2, Section 8 of D3.1 provides an overview of the PROTECT demonstration and scenarios.

- In the passport scenario (both types A and B), additional biometric (other than fingerprints and facial image) would be stored in a 4th generation electronic passport.
- In the mobile scenario (both types A and B), additional biometric (other than fingerprints and facial image) would be stored in a smartphone app.

2.2 Format of E-passports and biometrics included

2.2.1 Legal requirements

In the aftermath of the tragic events of 11 September 2001, the Commission was asked by Member States to take immediate action to improve document security. The Council therefore decided to integrate biometrics in European passports in order to strengthen the link between the passport and the carrier of the passport, as well as to make it easier to verify the authenticity of the passport.

By consequence, on 13 December 2004, the EU Council adopted Regulation (EC) No 2252/2004[25] which prescribes the compulsory implementation of biometrics in EU passports. Article 1(2) of this text states that *"Passports and travel documents shall include a highly secure storage medium which shall contain a facial image. Member States shall also include two fingerprints taken flat in interoperable formats. The data shall be secured and the storage medium shall have sufficient capacity and capability to guarantee the integrity, the authenticity and the confidentiality of the data".* These requirements do not apply to identity cards issued by Member States to their nationals or to temporary passports and travel documents having a validity of 12 months or less.[26]

The purpose of the collection and storage of biometric features in passports in indicated in article 4(3) as follows: *"Biometric data shall be collected and stored in the storage medium of passports and travel documents with a view to issuing such documents. For the purpose of this Regulation the biometric features in passports and travel documents shall only be used for verifying:*

- *the authenticity of the passport or travel document;*
- *the identity of the holder by means of directly available comparable features when the passport or travel document is required to be produced by law".*

Article 2 of Regulation (EC) No 2252/2004 states that *"Additional technical specifications in accordance with international standards, including in particular the recommendations of the International Civil Aviation Organisation (ICAO)"* shall be established relating to:

- additional security features and requirements, including enhanced anti-forgery, counterfeiting and falsification standards;
- technical specifications for the storage medium of the biometric features and their security, including prevention of unauthorised access;

[25] Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States (OJ L 385, 29.12.2004, p. 1).
[26] Art. 1(3) of Council Regulation (EC) No 2252/2004.

- requirements for quality and common technical standards for the facial image and the fingerprints.

In this context, on 28 February 2005, the Commission adopted the first part of the technical specifications which relate to the storage of the facial image of the holder on a contact-less chip. On 28 June 2006, the Commission adopted a second Decision[27] relating to the additional storage of two fingerprints on the passport chip which was amended in 2011[28] and in 2013.[29] In these specifications, some elements concerning security requirements can be found such as compliance to the BSI Technical Report on Advanced Security Mechanisms for Machine Readable Travel Documents[30]. In this BSI document a specific implementation of the Extended Access Control (EAC)[31] security mechanism as mentioned in ICAO 9303 is given. The implementation of these technical specifications by Member States is mandatory and failure to fulfil these obligations can lead to sentences pronounced by the European Court of Justice (ECJ).[32]

On 28 May 2008, Regulation EC 2252/2004 was amended by Regulation (EC) No 444/2009[33]. The main reason was that Regulation (EC) No 2252/2004 provided for a general obligation to provide fingerprints to be stored on a contactless chip in the passport or travel document. However, experience from tests showed that exceptions are needed. During pilot projects in some Member States it appeared that the fingerprints of children under the age of 6 seemed not to be of a sufficient quality for one-to-one verification of identity. Furthermore, children are subject to significant changes which make it difficult to check them during the entire period of validity of the passport or travel document. Therefore, the Regulation was amended in order to harmonize the exceptions to the general obligation to provide fingerprints and to maintain common security standards with a view to simplifying border controls. A second reason for amendment was the introduction of the principle of "one person-one passport". This principle was already recommended by the International Civil Aviation Organisation (ICAO) to ensure that the passport and the biometric features are only linked to the person holding the passport. In order to cease the revealed deficiencies, the European Parliament and the Council issued Regulation (EC) no 444/2009 with these essential amendments:

- The passport and travel documents should be issued as individual documents to respect the principle of one person one document;

[27] Commission Decision of 28/6/2006 laying down the technical specifications on the standards for security features and biometrics in passports and travel documents issued by Member States, C(2006) 2909 final. Available at http://ec.europa.eu/transparency/regdoc/?fuseaction=list&coteId=3&year=2006&number=2909&language=en

[28] Commission Decision C(2011) 5499https://www.pep.pt/wp-content/uploads/2017/07/Decisao-da-comissao-C2011-5499-final-de-04.08.2011-en.pdf

[29] Commission implementing Decision of 30/9/2013 amending Commission Decision C(2006) 2909 final laying down the technical specifications on the standards for security features and biometrics in passports and travel documents issued by Member States and Commission Decision C(2008) 8657 laying down a certificate policy as required in the technical specifications on the standards for security features and biometrics in passports and travel documents issued by Member States and updating the normative reference documents, C(2013) 6181 final. Available at https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/policies/borders-and-visas/document-security/docs/comm_decision_c_2013_6181_en_.pdf

[30] Advanced Security Mechanisms for Machine Readable Travel Documents, BSI TR-03110 Part 1 and 3, Version 2.10 of 20 March 2012.

[31] Extended Access Control is a mutual authentication mechanism between the terminal and the chip based on public key infrastructures (PKI). Terminal Authentication restricts access to data stored on the chip to authorized terminals. Chip Authentication not only authenticates the chip as genuine, it also enforces strong encryption and integrity protection of the transmitted data.

[32] ECJ, Judgment of the Court (Ninth Chamber) of 13 February 2014 — European Commission v Kingdom of Belgium, Case C-139/13.

[33] Regulation (EC) No 444/2009 of the European Parliament and of the Council of 28 May 2009 amending Council Regulation (EC) No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States.

- Children under the age of 12 and persons where fingerprinting is physically impossible are exempted from the obligation to provide fingerprints.[34]

Concerning the material of the passport or travel document which must be issued in machine-readable form, the annex of Regulation EC 2252/2004[35] accepts:

1) Paper meeting the following minimum requirements: no optical brighteners, duotone watermarks, security reagents to guard against attempts at tampering by chemical erasure, coloured fibres (partly visible and partly fluorescent under UV light, or invisible and fluorescent in at least two colours), UV-fluorescent planchettes are recommended (mandatory for stickers), the use of security thread is recommended. An optically variable (OVD) or equivalent device, which provides for the same level of identification and security as currently used in the uniform format for visas, shall be used on the biographical data page and shall take the form of diffractive structures which vary when viewed from different angles (DOVID) incorporated into the hot-sealed or an equivalent laminate (as thin as possible) or applied as an OVD overlay.

2) Stickers. In that case, the watermark in the paper used for that page may be dispensed with. The watermark may also be dispensed with in the paper used for the inside of the passport or travel document covers. Security reagents are required on the inside covers only if data are entered there. Stitching thread should be protected against substitution. If stickers or non-laminated paper inside pages are used for biographical data, intaglio printing with latent image effect, microtext and ink with optically variable properties and a DOVID (diffractive optically variable image device) shall also be employed.

3) Cards made entirely of a synthetic substrate. In such cards, it is not usually possible to incorporate the authentication marks used in passport or travel document paper. In the case of cards, the lack of marks in the materials shall be compensated for by measures in respect of security printing, use of an anti-copying device, or an issuing technique according to sections 3, 4 and 5 of the aforementioned annex. These include additional optically variable security devices shall, at least through the use of a DOVID or equivalent measures. If a synthetic card is personalised by laser engraving, and an optically variable laser written device is incorporated therein, the diffractive OVD shall be applied at least in the form of a positioned metallised or transparent DOVID, to achieve enhanced protection against reproduction.

In short, currently, at European level, ePassports which format is strictly regulated, must contain the following biometrics modalities in a mandatory manner:

- Facial image
- Two fingerprints (left and right index finger[36]) taken flat.

2.2.2 Privacy considerations

On 18 August 2004, the Chairman of the Article 29 Working Party addressed a letter to the President of the European Parliament, the President of the LIBE Committee, the Secretary General of the Council of the

[34] Where fingerprinting of the designated fingers is temporarily impossible, Member States shall allow the fingerprinting of the other fingers. Where it is also temporarily impossible to take fingerprints of any of the other fingers, they may issue a temporary passport having a validity of 12 months or less.

[35] The annex of Regulation EC 2252/2004 is available at http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32004R2252

[36] For each hand, if the index finger is injured or missing, or has an ISO/IEC 19794-4 score of 0 to 25, a plain impression of the middle finger, ring finger or thumb of the same hand shall be recorded where a higher ISO score is available. If all fingers on one hand are of the low quality score indicated above, a plain impression of the finger with the best score shall be taken.

European Union, the President of the European Commission, the Director General of DG Enterprise and the Director General of DG Justice and Home Affairs.[37] Amongst others, he pointed the following:

1. The Working Party strictly opposes the storage of all EU passport holders´ biometric and other data in a centralised database of European passports and travel documents;
2. The purpose of introducing biometric features in passports and travel documents as defined by the Regulation has to be explicit, appropriate, proportionate and clear;
3. The Member States should guarantee in a technically sound way that the passports include a storage medium with sufficient capacity and the capability to guarantee the integrity, the authenticity and the confidentiality of the data;
4. The Regulation should define who may have access to the storage medium and for which purposes (reading, storing, modifying or erasing data);
5. The Member States should set up a register of competent authorities.

In a further letter of 30 November 2004 addressed to the President of the LIBE Committee and to the President of the Council of the European Union, the Chairman of the Article 29 Working Party argued against a second mandatory biometric feature. The Chairman stressed that the introduction of an additional biometric feature makes it all the more necessary to create a secure and waterproof system making sure that the fundamental right of privacy is not endangered.

On 16 September 2005, the 27th International Conference of Data Protection and Privacy Commissioners in Montreux adopted the Resolution on the use of biometrics in passports, identity cards and travel documents.[38] In this Resolution the International Conference is pointing out that the widespread use of biometrics will have a far-reaching impact on the global society and therefore should be subject to an open worldwide debate. The International Conference is calling for:

1. effective safeguards to be implemented at an early stage to limit the risks inherent to the nature of biometrics;
2. the strict distinction between biometric data collected and stored for public purposes (e.g. border control) on the basis of legal obligations and for contractual purposes on the basis of consent;
3. the technical restriction of the use of biometrics in passports and identity cards to verification purposes comparing the data in the document with the data provided by the holder when presenting the document.

In September 2005, the Article 29 Working Party issued an opinion[39] on Regulation (EC) No 2252/2004. In this opinion, WP29 recalled that the European Parliament's legislative resolution of 2 December 2004[40], which was adopted by 471 votes in favour to 118 against and 6 abstentions, rejected the mandatory inclusion of fingerprints and the creation of a central database of EU passports and travel documents. By consequence, fearing that privacy and data protection rights could be infringed by increasing "the risk of abuse and function creep" and that the scheme would "violate the purpose and the principle of proportionality" the Parliament, introduced an amendment to the Regulation text specifically stipulating that "*no central database of European Union passports and travel documents containing all EU passport holders' biometric and other data*

[37] Letter of the Chairman of the Art. 29 Working Party to the President of the European Parliament, the President of the LIBE Committee, the Secretary General of the Council of the European Union, the President of the European Commission, the Director General of DG Enterprise and the Director General of DG Justice and Home Affairs, dated the 18 August 2004 (not published).

[38] https://edps.europa.eu/sites/edp/files/publication/05-09-16_resolution_biometrics_en.pdf

[39] Article 29 Working Party, Opinion 3/2005 on Implementing the Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States, WP112, adopted on 30 September 2005.

[40] European Parliament legislative resolution on the proposal for a Council regulation on standards for security features and biometrics in EU citizens' passports (COM(2004)0116 — C5-0101/2004 — 2004/0039(CNS))

shall be set up". In the same way, according to the report of the Committee on Civil Liberties, Justice and Home Affairs of 25 October 2004, "*the setting up of a centralised database would violate the purpose and the principle of proportionality. It would also increase the risk of abuse and function creep. Finally, it would increase the risk of using biometric identifiers as 'access key' to various databases, thereby interconnecting data sets".*[41] In its opinion, the Working Party supported this demand and stated that *"the objection against a European central database of European Union passports and travel documents are the same objections against national central databases of passports and travel documents as well as against central databases for ID-cards".* However, the Council did not take account of the suggestions and requests of change laid down by the Parliament. According to an in-depth survey[42]conducted by the Article 29 Data Protection Working Party at the request of the LIBE committee of the European Parliament and focused on the implementing practices as regards as Regulation (EC) No 2252/2004, several Member States have foreseen the implementation of a central database for storing the biometric data of the passport. Although it is possible for the Member States to implement only a verification procedure of biometric data using a centralised database, as it is strictly limited to in the Regulation, this option presents additional risks regarding the protection of personal data, such as the development of further purposes not foreseen in the regulation, or even fishing expeditions into the database which will be difficult to mitigate.[43]

In August 2008, the European Data Protection Supervisor (EDPS) issued an opinion[44] on the proposal for a Regulation of the European Parliament and of the Council amending Council Regulation (EC) No 2252/2004. Firstly, the EDPS regretted that the Commission did not comply with its legal obligation to consult him. Secondly, the EDPS regretted that the Commission did not conduct an impact assessment on this proposal: *"It is unclear therefore how the Commission was in a position to properly evaluate necessity and proportionality of the proposal in relation to data protection issues without the support of a rigorous impact assessment".* Thirdly, the EDPS recommended the Commission to propose further harmonisation measures in order to implement only the use of decentralised storage (in the wireless chip of the passport) regarding biometric data collected for EU Member States' passports. Furthermore, according to the EDPS, the age limit for children in giving fingerprints should be defined by a consistent and in-depth study which is to identify properly the accuracy of the systems obtained under real conditions, and which is to reflect the diversity of the data processed. The pilot projects as such do not provide sufficient information on which fundamental choices of the legislator can be based. An age limit for elderly, which can be based on similar experiences should be introduced as an additional exemption. Such exemptions should in no case stigmatize or discriminate the individuals concerned.

The EDPS also raised some remarks concerning the Commission's Decision C(2006) 2909 which defined only the format and the quality of the fingerprint images which should be processed as well as the way in which they have to be protected (Extended Access Control). There is no indication in the proposal either on the possible Failure to Enrol Rate (FER) and the rates related to the matching process. The proposal has indeed foreseen a fallback procedure for young children (age limit), but the threshold which indicates when fingerprints are not good enough for being enrolled is not defined. According to the EDPS, regarding the

[41] Committee on Civil Liberties, Justice and Home Affairs, Report on the Commission proposal for a Council regulation on standards for security features and biometrics in EU citizens' passports, 28 October 2004.
(COM(2004)0116 – C5-0101/2004 – 2004/0039(CNS))

[42] See letter of 10 December 2007, with annex, from the Chairman of the Article 29 Working Party to the Chairman of the LIBE Committee on EU passports, at these links:
http://collections.internetmemory.org/haeu/20171122154227/http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2007/2007_12_10_letter_cavada_biopassports_en.pdf
and
http://collections.internetmemory.org/haeu/20171122154227/http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2007/2007_12_10_letter_cavada_biopassports_replies_en.pdf

[43] See the Article 29 Working Party's opinion No 3/2005 of 30 September 2005 (WP 112).

[44] Opinion of the European Data Protection Supervisor on the proposal for a Regulation of the European Parliament and of the Council amending Council Regulation (EC) No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States

matching process, the proposal failed also to define which False Rejection Rate (FRR) should be applied at the border and how to deal with persons who have been apparently falsely rejected. This lack of uniform rates could lead to different processes of biometric data of EU citizens, depending on the border the person would select for entering the Schengen area, and could thus result in a lack of equal treatment of European citizens regarding the residual risk of biometric systems. Because the process is a one to one verification, the EDPS recognises that the FRR will be lower than the one applied for an identification process and there will therefore be fewer cases to deal with. However, fallback procedures need also to be defined in a harmonised and satisfactory way for those persons. Therefore, the EDPS recommends the Commission to propose common rates for the enrolment and matching process completed by fallback procedures together with the Member States' authorities.

2.2.3 Legal constraints for PROTECT scenarios

In the context of the PROTECT project, several constraints derived from current EU rules on ePassports should be taken into account:

1) It is important to note that Article 4 of Regulation EC 2252/2004 stipulates that *"No information in machine-readable form shall be included in a passport or travel document unless provided for in this Regulation, or its Annex, or unless it is mentioned in the passport or travel document by the issuing Member State in accordance with its national legislation"*. To be pragmatic, this means that under the current EU Regulation, it is very unlikely that inclusion of additional multimodal biometrics features (being not facial image or fingerprints) developed within the PROTECT project could legally be integrated in ePassports without a national legislation of a Member State allowing it. Furthermore, even if a national law would allow such integration of additional biometrics, it would certainly be challenged in Court for privacy reasons (proportionality principle) described in Section 2.2.2.
2) In order to comply with European privacy recommendations of the EDPS, no central database of European Union passports and travel documents containing all EU passport holders' biometric and other data should be set up.
3) Under current EU law, it also seems very doubtful that mobile devices such as smartphones could legally be used as carriers of biometrics features as means to replace the materials imposed by the annex of Regulation EC 2252/2004: smartphones cannot be considered as "Passports or travel documents" in the meaning of article 1 of said Regulation. Nonetheless, this constraint does not oppose to carefully examining the possibility of using a smartphone as a "passport companion" on which additional multimodal biometric features would be stored for "comfort and convenience purposes" of travellers on basis of their consent. This scenario and its data protection implications will be examined in Deliverable D2.3- Privacy impact of next-generation biometric border control.

2.3 Format residence permits and biometrics included

2.3.1 Legal requirements

Article 4a of Regulation (EC) No 380/2008[45] integrates biometric identifiers into residence permits which much conform to a uniform format.[46] This article reads as follows:

[45] Council Regulation (EC) No 380/2008 of 18 April 2008 amending Regulation (EC) No 1030/2002 laying down a uniform format for residence permits for third-country nationals

[46] Article 2 of this Regulation defines "residence permit" as *"any authorisation issued by the authorities of a Member State allowing a third-country national to stay legally on its territory, with the exception of: (i) visas; (ii) permits issued pending examination of an application for a residence permit or for asylum; (iii) authorisations issued for a stay of a duration not exceeding six months by Member States not applying the provisions of Article 21 of the Convention*

"The uniform format for residence permits shall include a storage medium containing the facial image and two fingerprint images of the holder, both in interoperable formats. The data shall be secured and the storage medium shall be of sufficient capacity and capability to guarantee the integrity, authenticity and confidentiality of the data."

These biometric features in residence permits may only be used for verifying:

a) the authenticity of the document;

b) the identity of the holder by means of directly available comparable features when the residence permit is required to be produced by national legislation.

The capture of fingerprints is compulsory as of six years of age. Persons for whom fingerprinting is physically impossible are exempted from the requirement to give fingerprints.

Furthermore, this Regulation provides that the procedure for taking these identifiers must respect national legislation and the safeguards contained in the UN human rights and child conventions and that the data from the biometric identifiers must be stored and secured so that their integrity, authenticity and confidentiality are guaranteed. The technical specifications for the capture of biometric identifiers must be set out in accordance with ICAO standards and the technical specifications for passports issued by Member States to their nationals pursuant to Council Regulation (EC) No 2252/2004 of 13 December 2004.

Furthermore, Regulation (EC) No 1030/2002 as amended by[47] establishes a uniform format for residence permits which must be stand-alone documents in card form (initially they could also be stickers attached to another official paper) in ID 1 format. The specifications set out in the International Civil Aviation Organisation (ICAO) document on machine-readable travel documents (Document 9303, seventh edition, 2015) should be taken into account.

Figure 2 - Front and reverse of the residence permit

implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders".

[47] Regulation (EU) 2017/1954 of the European Parliament and of the Council of 25 October 2017 amending Council Regulation (EC) No 1030/2002 laying down a uniform format for residence permits for third-country nationals

In brief, currently, at European level, resident permits of third-country nationals must contain the following biometrics modalities in a mandatory manner[48]:

- Facial image;
- Two fingerprints taken flat and digitally captured.

2.3.2 Privacy considerations

On 11 August 2004, the Article 29 Working Party issued an opinion related the inclusion of biometrics in residence permits.[49] In this opinion, the Working Party understands the concern about combating "identity theft", which has most unfortunate consequences for the victims. However, in accordance with the points made in its working document on biometrics adopted on 1 August 2003[50], if biometric features are included in residence permits and the corresponding personal data is processed, *"a number of principles would have to be observed with a view to protecting the fundamental rights and freedoms of persons, particularly as regards their rights concerning processing of their personal data. Respect of these principles is particularly essential in connection with the processing of biometric data which, by their very nature, provide information on specific persons, especially as some can leave traces in people's everyday lives, without the people in question knowing that they can be collected (digital fingerprints are a notable example").* The Working Party also thinks that there must be:

- measures enabling the persons concerned to have access to the data on the chip, if only to be able to check the contents particularly as regards their own biometric characteristics;
- guarantees for persons who cannot provide some of the biometric data used, such as fingerprints (for example, if they have lost fingers, or their fingerprints have been damaged);
- guarantees, particularly in the event of false rejections in border checks, that the persons in question will be informed of the reasons for the rejection and the means by which they may assert their own point of view before any decision is taken and that the facts will be clarified without delay.

Furthermore, the Working Party stresses that the interoperability provided for in Article 4a of the Regulation would permit access to data stored on the chip in the form of images by an authority other than the one that entered the data. Given that the proposed medium is a contactless chip, the Working Party would have liked to receive, at an appropriate time before decisions are made to adopt the Regulation, a document demonstrating that the specifications envisaged for the incorporation of data in chips and access to these data ensure that:

- the data cannot be modified by an authority other than the one responsible for issuing the document in accordance with ICAO Recommendation 9303, as referred to in Recital 2 (electronic signature certified by the ICAO);
- the data cannot be accessed without the persons concerned being aware of it, by public bodies other than those legally authorised or by private entities; it would be appropriate to provide for encryption of the data in order to ensure confidentiality; access for reading the electronic elements could also be protected by an individual code known only to the holder;
- authorities with the right to access the data have access only to the information necessary for them to perform the tasks for which they are responsible.

[48] Article 4a of Regulation (EC) No 1030/2002 as amended by Regulation (EC) No 380/2008.
[49] Article 29 Working Party, Opinion No 7/2004 on the inclusion of biometric elements in residence permits and visas taking account of the establishment of the European information system on visas (VIS).
[50] Article 29 Working Party, WP 80, adopted 1 August 2003.

On 28 December 2006, the European Data Protection Supervisor (EDPS) also issued an opinion on the inclusion of biometrics in residence permits.[51] In this opinion, the EDPS recognises the advantages of the use of biometrics but stresses the major impact of the use of such data and suggests the insertion of stringent safeguards for any kinds of use of biometric data. Firstly, as the residence permit is not a travel document, EDPS emphasize that there is no consistent reason for following the ICAO standards and therefore to use a contact-less chip. This technology has not been proven to be safer than a contact chip and will only bring additional risks to the deployment of the residence permits. ICAO standards should also be replaced by high security specifications corresponding to the situations under which a residence permit is used.

Furthermore, the EDPS makes the following remarks concerning the insertion of an additional chip for e-services purposes. According to Article 4, the Member States could embed a second chip in the stand-alone card of the residence permit. This second chip would be a contact chip and be dedicated to e-services. The EDPS specifically stresses the inadequacy of such measure since it does not respect basic and elementary rules of security policy required for sensitive data. This additional chip offers a full range of new applications and purposes for the residence permit card. The structure of the security protection profile of the first contactless chip which will store biometric features can only be rigorously and properly defined in the light of the risks produced by the other purposes such as e-business and e-government applications. There is no guarantee indeed that these applications will not take place for example in a relatively unsafe environment for the contactless chip. It would indeed be unfortunate if the use of this additional chip jeopardizes the security of the sensitive data stored in the primary chip. For those reasons, the EDPS strongly recommends following elements to be defined:

- a limited list of purposes envisaged for the additional chip:
- a list of data which will be stored in the additional chip;
- the need for an impact assessment and a risk assessment of the co-existence of the two chips on the same stand-alone card.

2.3.3 Legal constraints for PROTECT scenarios

In the context of the PROTECT project, several constraints derived from current EU rules on residence permits should be taken into account:

1) It is important to note that article 4 of Regulation (EC) No 1030/2002 as amended by Regulation (EC) No 380/2008 provides that *"No information in machine-readable form shall be included on the resident permit or on the storage medium of the residence permit referred to in Article 4a, unless provided for in this Regulation, or its Annex or unless it is mentioned in the related travel document by the issuing State in accordance with its national legislation".* To be pragmatic, this means that under the current EU Regulation, it is very unlikely that inclusion of additional multimodal biometrics features (being not facial image or fingerprints) developed within the PROTECT project could legally be integrated in residence permits without a national legislation of a Member State allowing it. Furthermore, even if a national law would allow such integration of additional biometrics, it would certainly be challenged in Court for privacy reasons (proportionality principle) described in Section 2.2.2.
2) Article 4 of Regulation (EC) No 1030/2002 as amended by Regulation (EC) No 380/2008 also provides *"that Member States may also store data for e-services such as e-government and e-business as well as additional provisions relating to the residence permit on a chip referred to in point 16 of the Annex. However, all national data must be logically separated from the biometric data referred to in Article 4a"*. Point 16 of the annex clarifies that *"a RF chip shall be used as a storage medium in accordance with Article 4a. Member States may store data on this chip or incorporate in the residence permit a dual interface or*

[51] Opinion of the European Data Protection Supervisor on the modified proposal for a Council Regulation amending Regulation (EC) 1030/2002 laying down a uniform format for residence permits for third-country nationals, 2006/C 320/10.

a separate contact chip for national use which shall be placed at the back of the card complying with ISO standards and shall in no way interfere with the RF chip". The possibility to rely on this legal basis in order to integrate additional "contactless" biometrics data on a "second" chip of residence permits for "comfort and convenience purposes" of travellers seems to be not possible since that this second chip should be a contact chip.

4) Under current EU law, article 1 of Regulation (EC) No 1030/2002 stipulates that "*residence permits issued by Member States to third-country nationals shall be drawn up in a uniform format and provide sufficient space for the information set out in the Annex hereto"*. The said annex does not list mobile devices such as smartphones as material which can be used as carriers of biometric features for the purposes of a resident permit. Nonetheless, this constraint does not oppose to carefully examining the possibility of using a smartphone as a "travel document companion" on which additional multimodal biometric features would be stored for "comfort and convenience purposes" of travellers on basis of their consent. This scenario will be examined in D2.3- Privacy impact of next-generation biometric border control.

2.4 Format of Schengen visas and absence of biometrics

2.4.1 Legal requirements

Council Regulation (EC) 539/2001 of 15 March 2001 lists the third countries whose nationals must be in possession of visas when crossing the external borders and those whose nationals are exempt from that requirement.[52]

In 1995, Council Regulation (EC) No 1683/95[53] created a uniform format for an EU visa taking the form of a sticker[54] to be affixed to the travel document of non-EU nationals under visa obligation.

This regulation lays down the rules for the uniform format for visas, not only for the Schengen countries but also for Ireland and the United Kingdom.

The uniform format applies to[55]:

- an intended stay in one or more countries of the Schengen area of no more than 3 months in total;
- a transit through the international transit areas of airports of the Schengen countries ('airport transit visa').

In the case of the Schengen countries, a short-stay visa issued by one of them entitles its holder to travel throughout the 26 countries for up to 90 days in any 180-day period. Visas for visits exceeding that period remain subject to national procedures (i.e. to allow its holder to take up employment or establish a business, trade or profession).

Information on the visa sticker is the following:

- The uniform visa sticker specifies the number of days that a non-national of an EU country may stay in the Schengen area and in Ireland and the United Kingdom. In the case of a Schengen visa, the days should be counted from the date he or she enters the Schengen area to the date he or she exits the Schengen area, both days included.

[52] A consolidated version of Regulation (EC) 539/2001 for documentation purposes only is available at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02001R0539-20170611

[53] Council Regulation (EC) No 1683/95 of 29 May 1995 laying down a uniform format for visas. Subsequent amendments to Regulation (EC) No 1683/95 have been incorporated into the basic text. A consolidated version with documentary value only is available at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:01995R1683-20131018

[54] Art. 1. of Council Regulation (EC) No 1683/95 as amended.

[55] Article 2(2)(a) of Regulation (EC) No 810/2009 of the European Parliament and of the Council of 13 July 2009 establishing a Community Code on Visas (Visa Code)

- The precise length of validity of the visa is indicated on the visa sticker under the heading 'Duration of visit'.

The uniform visa must conform to:

- a list of technical specifications[56] specified in the EU legislation that lay down universally recognisable security features clearly visible to the naked eye[57];
- other technical specifications which aim to prevent counterfeiting and falsification of the visa and provide methods to fill in the visa.

The figure below illustrates the model which must be inserted[58]:

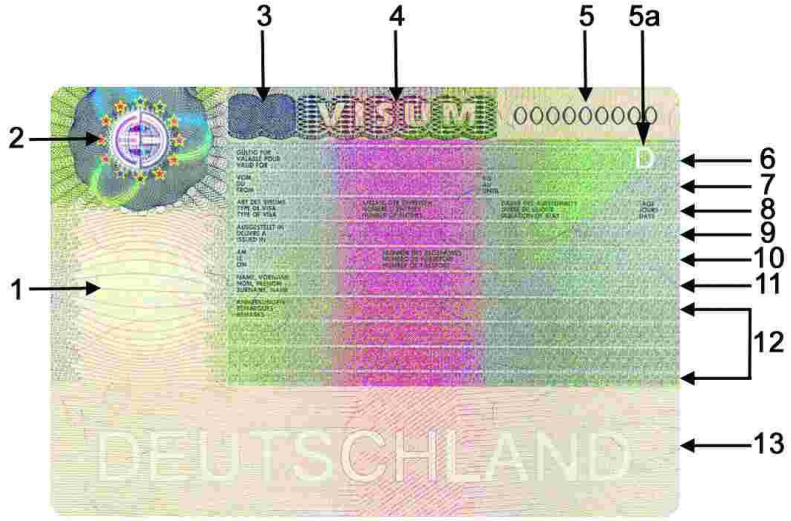

Figure 3 - Schengen Visa model

At the end of September 2003, the European Commission submitted a draft Council Regulation amending Regulation 1683/95.[59] The amendment to the uniform formats for visas proposed to include, as obligatory elements, two items of biometric data stored on a highly secure medium (contactless chip), i.e. a full-face digital photograph of the holder as the principal element for biometric identification together with two digital images of the holder's fingerprints taken flat. However, a report[60] sent to the Council in 2004 concluded that: *"the solution envisaged by the draft regulation is not technically feasible".* The main reason consisted in the so called "collision" problem, which leads to difficulties for the reader to read out the valid visa in case there are several contactless chips on different visa in the same passport. The reading of the valid chip in the visa would require difficult handling procedures. In that report, collision is described as: *"the interference between various chips and the reading device, eg: due to the de-tuning of the resonance frequency, resulting in malfunction".* The "collision problem" is twofold: first there is a "risk of failure due to interference between eVisa chips (if several states have inserted chip visas) and second, there is even the risk of failure due to interference between ePassport and eVisa. As the report puts it, if non-EU countries use "ePassports" and each visa has a biometric chip this: *"Will "kill" ePassport chip functionality".*

[56] Art.2. of Council Regulation (EC) No 1683/95 as amended.
[57] See Annex of Council Regulation (EC) No 1683/95 as amended.
[58] For an overview of the information to which refer the references in the figure 8, see Annex of Council Regulation (EC) No 1683/95.
[59] Proposal for a Council Regulation amending Regulation (EC) 1683/95 laying down a uniform format for visas, Brussels, 24.09.2003, COM(2003)558 final.
[60] Chairman of the Committee created by Article 6 of Regulation 1683/95 laying down a uniform format for visas, Technical feasibility of the integration of biometric identifiers into the uniform format for visa and residence permits for third country nationals, passports and other travel documents issued by Member States, Brussels, 11 November 2004, doc no: 14534/04, available at http://www.statewatch.org/news/2004/dec/bio-visas.pdf

For these reasons, **the visa stickers do not contain any biometric traits**. However, once an application is found admissible as set out in the Visa Code, the visa authority creates the application file by entering data into the Visa Information System (VIS) such as the applicant's personal and travel details provided in the application form, photograph and fingerprints. Indeed, article 13 of the Visa Code[61] require Member States to collect the following biometric identifiers from applicants in order to enter those information in the (VIS):

- a photograph, scanned or taken at the time of application, and
- 10 fingerprints taken flat and collected digitally.

The collection and processing of biometric identifiers within the VIS are detailed in Section 4.3.

2.4.2 Legal constraints for PROTECT scenarios

In the context of the PROTECT project, a major constraint derived from current EU rules on Schengen visas should be taken into account:

No biometric features are included in Schengen visas. The consequence is that verification of the identity of the holder of the visa and of the authenticity of the visa currently is done by consulting the Visa Information System (VIS) using the visa number and the fingerprint of the traveller (see Section 4.3). The fact that TCNVHs could be required to provide their fingerprints at the entry of the Schengen Area on request of border guards should be taken into account when developing a complete contactless biometric-based cross-border control solution. The use the facial image for biometric matching against the VIS has not yet been implemented. This issue could be resolved once the EES will become functional and that TCNVHs would be able to pre-enrol their facial image into that system.

2.5 Is consent of travellers a legitimate basis of lawfulness for processing additional biometrics in travel documents?

2.5.1 Introduction

According to D3.1, *"the enrolment phase would only be done once during the lifetime of the electronic passport. Prior to enrolment process, each passenger interested in using PROTECT solution would be required to give formal consent for data collection and will know exactly the purpose and limits of government use of their personal data. They would be able to withdraw consent at any time during the process and be satisfied that their data will be protected and deleted where necessary".*

This section aims to answer the following legal question: under current EU law, could consent of a traveller be the legal basis to enrol additional biometrics in travel documents for "government use of their personal data"?

2.5.2 Legal analysis

The GDPR[62] lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data. Article 4(14) of the GDPR defines *"biometric data" as "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique*

[61] Regulation (EC) No 810/2009 of the European Parliament and of the Council of 13 July 2009 establishing a Community Code on Visas (Visa Code).

[62] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

identification of that natural person, such as facial images or dactyloscopic data". In its Opinion 4/2007[63], the Article 29 Working Party specified that biometric data are *"biological properties, behavioural aspects, physiological characteristics, living traits or repeatable actions where those features and/or actions are both unique to that individual and measurable, even if the patterns used in practice to technically measure them involve a certain degree of probability."* By consequence, biometric data (raw and templates) are considered as "sensitive data" under the GDPR. As stated by article 9(1) of the GDPR, the principle is that *"processing biometric data for the purpose of uniquely identifying a natural person […] shall be prohibited"*. Exceptions to that principle are listed in article 9(2) of the GDPR. Amongst others, processing of biometric data is possible only if *"the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition may not be lifted by the data subject".*

"Consent" is defined in art. 4(11) of the GDPR as *"any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her"*. Additionally, for biometric data, consent must be "explicit". Furthermore, according to article 7 the GDPR, conditions for consent are the following:

"1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data. 2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding. 3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent. 4. When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract".

Moreover, it should be emphasised that Recital 43 expressly states that: *"in order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation".* This means that consent of travellers could not be used by public border control authorities to process additional biometrics for the purpose to speed up their public interest missions.

2.5.3 Legal constraints for PROTECT scenarios

Recital 43 of the GDPR expressly states that: *"in order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation".* It is also clear in most cases that the data subject will have no realistic alternatives to accepting the processing (terms) of this controller. WP29[64] considers that there are other lawful bases that are, in principle, more appropriate to the activity of public authorities, notably paragraphs (1c) and (1e) of article 6 GDPR.

This means that it seems that consent of travellers cannot be considered as a legitimate basis of lawfulness in PROTECT scenarios to allow public border control authorities to speed up their public interest missions by enrolling additional biometrics in travel documents.

This being said:

[63] Article 29 Working Party, Opinion 4/2007 on the concept of personal data, WP 136, adopted on 20th June 2007.
[64] Article 29 Working Party, Guidelines on Consent under Regulation 2016/679, WP259, Adopted on 28 November 2017.

- Consent could still be a possible legal basis for "commercial" purposes. For example, in a 2005 deliberation, the CNIL (French DPA) authorized the use of fingerprints on a fidelity chipcard (not a travel document) for frequent travellers of the airport of Nice. The system was designed for convenience purposes (facilitate access to parking zones, additional services, etc): Important criteria were the 1) the voluntary use, and 2) the storage on an object (no centralized database).[65]
- The possibility to use consent of travellers for enrolling additional biometric features in a "passport companion" such as a smartphone for "comfort and convenience purposes" of travellers on basis of their consent will be examined in Deliverable D2.3- Privacy impact of next-generation biometric border control.

3 Conditions of entry/exit to the Schengen Area

Both in the A (air and sea border) and B (land border) types of demonstrations described in Chapter 8 of "D3.1 - System requirements specification and scenarios" (hereafter D3.1), "background checks" are performed on passengers willing to use the "PROTECT" solution.

In order to assess which "background checks" should be performed by the PROTECT system at the entry/exit of Schengen external crossing points it is essential to identify the legal constraints derived the EU legal framework regulating movements at the external borders. Therefore, this section is dedicated to the analysis of the conditions of entry/exit to the Schengen area of persons enjoying the Union right of free movement, at the one hand, and third country nationals, on the other.

The Lisbon Treaty[66] attaches great importance to the creation of an area of freedom, security and justice (AFSJ). The legal basis of the AFSJ lies in Article 3(2) of the Treaty on European Union (TEU) which reads as follows: *"The Union shall offer its citizens an area of freedom, security and justice without internal frontiers, in which the free movement of persons is ensured in conjunction with appropriate measures with respect to external border controls, asylum, immigration and the prevention and combating of crime".* The Schengen area, an area of free movement without internal borders that now covers most of Europe, is one of the greatest achievements of the EU with regard to the AFSJ.

Within the Schengen Area, people may freely move from one country to another without being subjected to passport controls. The Schengen area was initiated in 1985, when five EU Member States[67] signed the Schengen Agreement, thus marking the beginning of cooperation to dismantle controls at their internal borders.[68] In subsequent years, most EU Member States, along with a few non-EU countries, joined this cooperation (see Figure 4).[69] This means that the countries that are part of Schengen cooperation no longer

[65] CNIL, 26ème rapport d'activité, 2005, p.50.

[66] The Treaty of Lisbon is an international agreement which amends the two treaties which form the constitutional basis of the European Union (EU). The Treaty of Lisbon was signed by the EU member states on 13 December 2007, and entered into force on 1 December 2009. It amends the Maastricht Treaty (1993), known in updated form as the Treaty on European Union (2007) or TEU, and the Treaty of Rome (1957), known in updated form as the Treaty on the Functioning of the European Union (2007) or TFEU. It also amends the attached treaty protocols as well as the Treaty establishing the European Atomic Energy Community (EURATOM).

[67] The first Member States were Belgium, France, Germany, Luxembourg and the Netherlands.

[68] If there is a serious threat to public policy or internal security, a Schengen country may exceptionally temporarily reintroduce border control at its internal borders for, in principle, a limited period of no more than thirty days. The reintroduction of border control at the internal borders must remain an exception and must respect the principle of proportionality. Reintroducing border control at the internal border should only ever be used as a measure of last resort. If such controls are reintroduced, the other Schengen countries, the European Parliament and the Commission should be informed, as should the public.

[69] Now there are 26 Schengen countries - 22 EU members and four non-EU. Those four are Iceland and Norway (since 2001), Switzerland (since 2008) and Liechtenstein (since 2011). Only six of the 28 EU member states are outside the Schengen zone - Bulgaria, Croatia, Cyprus, Ireland, Romania and the UK.

carry out border checks at the borders they share with each other. The removal of internal borders means that the Schengen countries need to cooperate with each other to maintain a high level of security within the Schengen area. It also means that they need to share responsibility for and cooperate in managing their common external borders and should, in that context, establish good cooperation with their non-Schengen neighbours outside the EU. Schengen cooperation entails common criteria for controlling the external borders, common rules for entering/exiting the Schengen area and increased police cooperation between the participating countries.

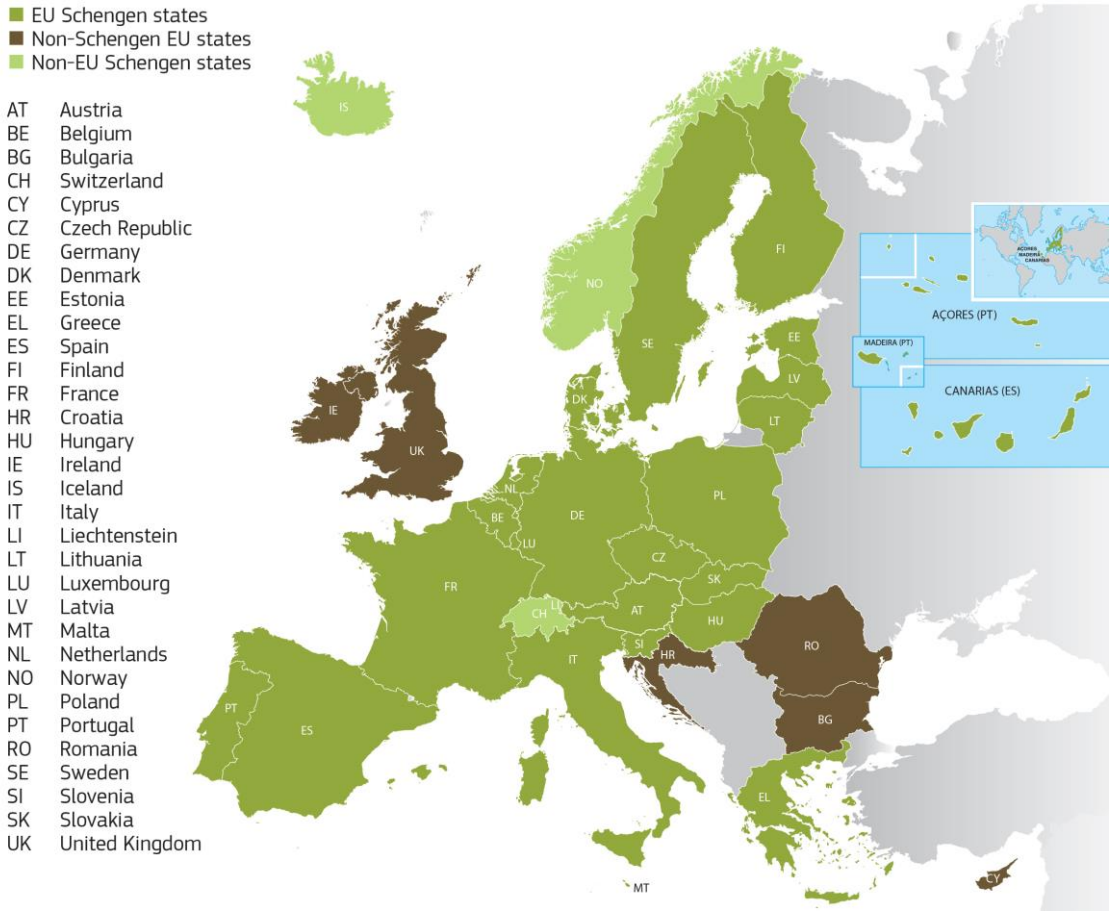

Figure 4 - Map of the Schengen area and the Schengen States

Regulation (EU) 2016/399[70], also known as the Schengen Border Code (hereafter "SBC") governs the movement of persons across the external Schengen borders. In order to guide border guards in respect of the measures and decisions to be taken along the external borders, the EU commission adopted a "Practical Handbook for Border Guards" (hereafter "Schengen handbook") in 2006 which was amended several times until 2015. [71]

[70] Regulation (EU) 2016/399 of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code) as amended by Regulation (EU) 2017/458 and by Regulation (EU) 2017/2225.

[71] However please note that this handbook does not cover the modifications of the SBC introduced by Regulation (EU) 2017/458 and by Regulation (EU) 2017/2225. See Commission Recommendation establishing a common "Practical Handbook for Border Guards (Schengen Handbook)" to be used by Member States' competent authorities when carrying out the border control of persons, Brussels, 06/11/2006, C (2006) 5186 final. A consolidated version taking into account the amendments adopted by the Commission on 25 June 2008 (C (2008)2976 final), on 29 September 2009 (C

According to the SBC, persons enjoying the Union right of free movement, at the one hand, and third country nationals (hereafter "TCNs"), on the other, are subject to different border control checks. Members of the first group are subject only to a "minimum check" while members of the second to a more thorough one.

3.1 Systematic checks on persons enjoying the Union right of free movement

3.1.1 Description

On entry and on exit of the Schengen area, persons enjoying the right of free movement under Union law are subject to systematic checks. Indeed, on 7 March 2017, the EU Council adopted a regulation amending the SBC to reinforce checks against relevant databases at the external borders.[72] This amendment of the SBC was presented by the European Commission in December 2015. It is a response to the increase in terrorist threats and to the call from the Council in its conclusions of 9 and 20 November 2015 for a targeted revision of the SBC in the context of the response to "foreign terrorist fighters". While Member States were already obliged to check TCNs systematically on entry against all databases for reasons of public order and internal security, the SBC did not provide for such a check on exit in all databases. Moreover, persons enjoying the right to free movement were only subject to a minimum check to establish their identities. Regulation (EU) 2017/458 aligns the obligations to carry out systematic checks both at entry and at exit on third country nationals, as well as on persons who enjoy the right of free movement. The databases against which checks must be carried out include the Schengen Information System (SIS II) and Interpol's database on stolen and lost travel documents (SLTD). The checks will also enable Member States to verify that those persons do not represent a threat to public policy, internal security or public health. This obligation applies at all external borders (air, sea and land borders), both at entry and exit.[73] An interesting novelty provided by Regulation (EU) 2017/458 is the fact that the new article 2e of the SBC specifies that checks against SIS and SLTD may be carried out in advance on the basis of API data received in accordance with Council Directive 2004/82/EC.[74]

(2009)7376 final), on 16 August 2010 (C(2010) 5559 final) , on 20 June 2011 (C(2011)3918 final), on 14 December 2012 (C(2012)9330 final) and on 15 June 2015 (C(2015)3894 final) is available at https://www.udiregelverk.no/PageFiles/2778/Practical%20Handbook%20for%20Boarder%20Guards_26.06.2015.pdf

[72] Regulation (EU) 2017/458 of the European Parliament and of the Council of 15 March 2017 amending Regulation (EU) 2016/399 as regards the reinforcement of checks against relevant databases at external borders.

[73] However, where systematic consultation of databases could lead to a disproportionate impact on traffic flows at a sea or land border, Member States are permitted to carry out only targeted checks against databases, following an assessment of the risks related to the public policy, internal security, public health or international relations of any of the Member States. The scope and duration of the temporary reduction to targeted checks against the databases shall not exceed what is strictly necessary and shall be defined in accordance with a risk assessment carried out by the Member State concerned. The Member State concerned shall transmit its risk assessment and updates thereto to the European Border and Coast Guard Agency ("the Agency"), established by Regulation (EU) 2016/1624 of the European Parliament and of the Council, without delay and shall report every six months to the Commission and to the Agency on the application of the checks against the databases carried out on a targeted basis. The Member State concerned may decide to classify the risk assessment or parts thereof. The risk assessment shall state the reasons for the temporary reduction to targeted checks against the databases, take into account, inter alia, the disproportionate impact on the flow of traffic and provide statistics on passengers and incidents related to cross-border crime. It shall be updated regularly. Persons who, in principle, are not subject to targeted checks against the databases, shall, as a minimum, be subject to a check with a view to establishing their identity on the basis of the production or presentation of travel documents. Such a check shall consist of a rapid and straightforward verification of the validity of the travel document for crossing the border, and of the presence of signs of falsification or counterfeiting, where appropriate by using technical devices. With regard to air borders, Member States may only carry out targeted checks against databases for a transitional period of 6 months from 7 April 2017. This period may be extended by up to 18 months in exceptional and specific cases, where there are infrastructural difficulties requiring a longer period of time to make the necessary changes.

[74] Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data.

Where those checks are carried out in advance on the basis of such data, the data received in advance shall be checked at the border crossing point against the data in the travel document.

According to article 8(2) of the SBC as amended by Regulation (EU) 2017/458 and by Regulation (EU) 2017/2225[75], this systematic check on entry and exit consists of:

1. Verification of the identity and the nationality of the person and of the authenticity and validity of the travel document for crossing the border, including by consulting the relevant databases, in particular: the SIS; Interpol's Stolen and Lost Travel Documents (SLTD) database; national databases containing information on stolen, misappropriated, lost and invalidated travel documents. If the travel document contains an electronic storage medium (chip), the authenticity and integrity of the chip data shall be confirmed using the complete valid certificate chain, unless this is technically impossible or, in the case of a travel document issued by a third country, impossible due to the unavailability of valid certificates;

2. Verification that a person enjoying the right of free movement under Union law is not considered to be a threat to the public policy, internal security, public health or international relations of any of the Member States, including by consulting the SIS and other relevant Union databases. This is without prejudice to the consultation of national and Interpol databases. Where there are doubts as to the authenticity of the travel document or the identity of its holder, at least one of the biometric identifiers integrated into the passports and travel documents issued in accordance with Regulation (EC) No 2252/2004 shall be verified. Where possible, such verification shall also be carried out in relation to travel documents not covered by that Regulation. For persons whose entry is subject to a registration in the EES, a verification of their identity in the EES shall be carried out according to the procedure described in Section 4.4.

3. Where the checks against the databases referred to in points (1) and (2) would have a disproportionate impact on the flow of traffic, a Member State may decide to carry out those checks on a targeted basis at specified border crossing points, following an assessment of the risks related to the public policy, internal security, public health or international relations of any of the Member States. The scope and duration of the temporary reduction to targeted checks against the databases shall not exceed what is strictly necessary and shall be defined in accordance with a risk assessment carried out by the Member State concerned.[76] The risk assessment shall state the reasons for the temporary reduction to targeted checks against the databases, take into account, inter alia, the disproportionate impact on the flow of traffic and provide statistics on passengers and incidents related to cross-border crime. It shall be updated regularly.[77]

4. Persons who, in principle, are not subject to targeted checks against the databases, shall, as a minimum, be subject to a check with a view to establishing their identity on the basis of the production or presentation of travel documents. Such a check shall consist of a rapid and straightforward verification of the validity of the travel document for crossing the border, and of the presence of signs of falsification or counterfeiting, where appropriate by using technical devices, and, in cases where there are doubts about the travel document or where there are indications that such

[75] Regulation (EU) 2017/2225 of the European Parliament and of the Council of 30 November 2017 amending Regulation (EU) 2016/399 as regards the use of the Entry/Exit System.

[76] The Member State concerned shall transmit its risk assessment and updates thereto to the European Border and Coast Guard Agency ("the Agency"), established by Regulation (EU) 2016/1624 of the European Parliament and of the Council, without delay and shall report every six months to the Commission and to the Agency on the application of the checks against the databases carried out on a targeted basis. The Member State concerned may decide to classify the risk assessment or parts thereof.

[77] Where a Member State intends to carry out targeted checks against the databases, it shall notify the other Member States, the Agency and the Commission accordingly without delay. The Member State concerned may decide to classify the notification or parts thereof. Where the Member States, the Agency or the Commission have concerns about the intention to carry out targeted checks against the databases, they shall notify the Member State in question of those concerns without delay. The Member State in question shall take those concerns into account.

a person could represent a threat to the public policy, internal security, public health or international relations of the Member States, the border guard shall consult the databases referred to in points (1) and (2).

The major requirements of this systematic check are presented in the figure below[78].

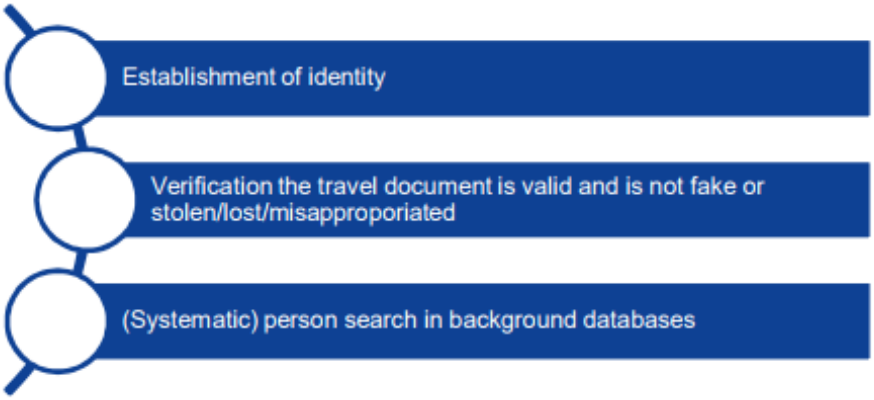

Figure 5 – Checks on persons enjoying the right of free movement under Union law

3.1.2 Legal constraints for PROTECT scenarios

In the context of the PROTECT project, the following constraints derived from current EU rules in the Schengen Border Code should be taken into account in relation with the checks on persons enjoying the right of free movement under Union law:

1) Recital 3 of Regulation (EU) 2017/458 explicitly states that *"the travel documents of persons enjoying the right of free movement under Union law should therefore be checked systematically, on entry into and on exit from the territory of Member States, against relevant databases for stolen, misappropriated, lost and invalidated travel documents in order to ensure that such persons do not hide their real identity".* Concretely, this means that the travel document must be presented for verification at each entry/exit of the Schengen area. As a reminder, a smartphone cannot be considered as a travel document under current EU rules.

2) In the same way, Article 8(2b) of the SBC states that *"persons who, in principle, are not subject to targeted checks against SIS and SLTD, shall, as a minimum, be subject to a check with a view to establishing their identity on the basis of the production or presentation of travel documents"*. As a reminder, a smartphone cannot be considered as a travel document under current EU rules.

3) An interesting novelty provided by Regulation (EU) 2017/458 is the fact that the new article 2e of the SBC specifies that checks against SIS and SLTD may be carried out in advance on the basis of API data received in accordance with Council Directive 2004/82/EC. Where those checks are carried out in advance on the basis of such data, the data received in advance shall be checked at the border crossing point against the data in the travel document. As a reminder, a smartphone cannot be considered as a travel document under current EU rules.

The main conclusion derived from these constraints are twofold:

[78] This figure was published by Diana Dimitrova and Els Kindt in "Recommendations for future ABC installations – Best practices", edited by Sirra Toivonen & Heta Kojo, VTT technology 303, p. 32, available at http://www.vtt.fi/inf/pdf/technology/2017/T303.pdf

- It is very doubtful that the mobile scenarios described in D3.1 which seek to replace travel document verification by a smartphone application verification could be considered as legal under current EU border control regulation;
- It is also very doubtful that the passport scenario at land border crossing points described in D3.1 which envisages to transmit passport data via a mobile application could be considered as legal under current EU border control regulation since that that travel documents must be presented at each entry/exit of the Schengen area.

3.2 Thorough checks on third country nationals (TCNs)

3.2.1 Description

As a general rule, TCNs have the right to enter the Schengen area for a short stay of up to 90 days within any 180-day period either with or without the need for the prior granting of a visa.[79] Visas for visits exceeding that period remain subject to national procedures.[80] It is important to note that regulation (EU) 2017/2226 of 30 November 2017[81] has introduced an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Schengen Area. The regulation applies to TCNs, both visa required and visa exempt, travelling for short stays of 90 days within a 180 days period in the Schengen area. The EES will replace the current system of manual stamping of passports and will electronically register identity data, the date and place of entry and exit as well as entry refusals of TCNs. The purpose of the EES is to improve the quality of border checks through the automatic calculation of those who overstay the permitted duration (the EES is examined in Section 4.4).

The current Article 8, (3)[82]of the SBC sets out the list of entry-exit steps governing border control for TCNs. Thorough checks on entry shall comprise verification of the conditions governing entry laid down in Article 6(1) (including the verification that they are in possession of a valid travel document entitling the holder to cross the border) and, where applicable, of documents authorizing residence and the pursuit of a professional activity. This shall include a detailed examination covering the following aspects:

1. Verification of the identity and the nationality of the third-country national and of the authenticity and validity of the travel document for crossing the border, including by consulting the relevant databases, in particular: the SIS, Interpol's SLTD database, national databases containing information on stolen, misappropriated, lost and invalidated travel documents. For passports and travel documents containing an electronic storage medium (chip), the authenticity and integrity of the chip data shall be checked, subject to the availability of valid certificates. With the exception of third-country nationals for whom an individual file is already registered in the EES, where the travel document contains a facial image recorded in the electronic storage medium (chip) and that facial image can be technically accessed, this verification shall include the verification of that facial image, by comparing electronically that facial image with the live facial image of the third-country national concerned. If technically and legally possible, this

[79] Article 6.1 pf the SBC.

[80] The procedures and conditions for issuing national long-stay visas (for intended stays of more than 3 months) are covered by national legislation, although holders of a national long-stay visa have the right to circulate within the territory of the Member States in accordance with the SBC.

[81] Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011

[82] Article 8(3), g) of the SBC.

verification may be done by verifying the live fingerprints against the fingerprints recorded in the electronic storage medium (chip).

2. Verification that the travel document is accompanied, where applicable, by the requisite visa or residence permit.

3. For persons whose entry or whose refusal of entry is subject to a registration in the EES, a verification of their identity by accessing the EES for TCNVEs or by accessing the VIS via the EES for TCNVHs (potentially using facial image or fingerprints). For persons whose entry or whose refusal of entry is subject to a registration in the EES, verification that the third-country national has not reached or exceeded the maximum duration of authorized stay on the territory of the Member States and, for third-country nationals holding a visa issued for one or two entries, verification that they have respected the number of the maximum authorized entries, by consulting the EES;

4. Verification regarding the point of departure and the destination of the third-country national concerned and the purpose of the intended stay, checking, if necessary, the corresponding supporting documents;

5. Verification that the third-country national concerned has sufficient means of subsistence for the duration and purpose of the intended stay, for his or her return to the country of origin or transit to a third country into which he or she is certain to be admitted, or that he or she is in a position to acquire such means lawfully;

6. Verification that the third-country national concerned, his or her means of transport and the objects he or she is transporting are not likely to jeopardize the public policy, internal security, public health or international relations of any of the Member States. Such verification shall include direct consultation of the data and alerts on persons and, where necessary, objects included in the SIS and other relevant Union databases, and the action to be performed, if any, as a result of an alert. This is without prejudice to the consultation of national and Interpol databases.

Figure 6 illustrates the current TCNs border checks process on entry and exit [83]

[83] This figure was published by the Research and Development Unit (RDU) of Frontex in n close cooperation with experts from a number of European Union Member States in "Guidelines for Processing of Third-Country Nationals through Automated Border Control", 2016, p.18 available at http://frontex.europa.eu/assets/Publications/Research/Guidelines_for_Processing_of_Third_Country_Nationals_through_ABC.pdf

Figure 6 - TCNs border checks process on entry and exit

3.2.2 Legal constraints for PROTECT scenarios

In the context of the PROTECT project, the following constraints derived from current EU rules in the Schengen Border Code should be taken into account in relation with the checks on TCNs:

1) For passports and travel documents containing an electronic storage medium (chip), the authenticity and integrity of the chip data shall be checked, subject to the availability of valid certificates. With the exception of third-country nationals for whom an individual file is already registered in the EES, where the travel document contains a facial image recorded in the electronic storage medium (chip) and that facial image can be technically accessed, this verification shall include the verification of that facial image, by comparing electronically that facial image with the live facial image of the third-country national concerned. If technically and legally possible, this verification may be done by verifying the live fingerprints against the fingerprints recorded in the electronic storage medium (chip). Concretely, this means that it seems the travel document must be presented for verification at each entry/exit of the Schengen area. As a reminder, a smartphone cannot be considered as a travel document under current EU rules.

2) Thorough checks on entry of TCNs shall comprise verification of the conditions laid down in Article 6(1) of the SBC, including the verification that they are in possession of a valid travel document entitling the holder to cross the border and, where applicable, of documents authorizing residence and the pursuit of a professional activity. Concretely, this means that that the travel document must be presented for verification at each entry/exit of the Schengen area. As a reminder, a smartphone cannot be considered as a travel document under current EU rules.

3) An interesting novelty provided by Regulation (EU) 2017/458 is the fact that t checks against SIS and SLTD may be carried out in advance on the basis of API data received in accordance with Council Directive 2004/82/EC. Where those checks are carried out in advance on the basis of such data, the data received in advance shall be checked at the border crossing point against the data in the travel document. As a reminder, a smartphone cannot be considered as a travel document under current EU rules.

The main conclusion derived from these constraints are twofold:

- It is very doubtful that the mobile scenarios described in D3.1 which seek to replace travel document verification by a smartphone application verification could be considered as legal under current EU border control regulation;
- It is also very doubtful that the passport scenario at land border crossing points described in D3.1 which envisages to transmit passport data via a mobile application could be considered as legal under current EU border control regulation since that travel documents must be presented at each entry/exit of the Schengen area.

3.3 Overview of the border control checks entry/exit

In order to summarize the "background checks" which should be taken into account by the PROTECT scenarios, the following table illustrates the current border checks processes of all persons crossing the external borders on entry and/or exit.

	Entry/ Exit	EU/EEA/CH TCNVEs TCNVHs	Description
Document check	Entry Exit	All	Verification of valid travel documents or other document authorising a traveller to cross the border and where applicable the requisite visa or residence permit. The documents are also checked to detect falsifications.
Bearer verification	Entry Exit	All	Checks made to secure that the bearer of the travel document is the lawful owner of the document
Visa check (VIS)	Entry	Only TCNVHs	Schengen visas are issued at consular posts around the world. The VIS is checked, using fingerprints (or facial image in the future) and the visa number
Entry Exit System (EES)	Entry Exit	TCNVEs TCNVHs	EES is checked on the basis of facial image (or fingerprints) and the stay is calculated automatically.

Questions	Entry Exit (means of subsistence)	TCNVEs TCNVHs	Questions are asked as regards: the purpose of the stay; sufficient means of subsistence for the duration of the stay and the return to the country of origin; other supporting documents (e.g. tickets, hotel reservations or invitations to meetings).
SIS II and SLTD check (and other databases)	Entry Exit	All	SIS II, SLTD and other relevant systems are checked to verify that the person is not a threat to public policy, internal security, public health, or international relations of any of the Member States or not allowed in the Schengen area.
Authorization to enter/exit	Entry Exit	All	When the result of all checks can be approved, the person can be granted access to the Schengen area.
Second line checks and actions	Entry Exit	All	Depending on the results of all the checks and on the questions and observations included at the border crossing, there could be alternative actions taken related to law enforcement, migration and asylum or to verify certain requirements (e.g. checking that the document is valid or that it is not a forgery).
Internal checks		All	After going through the border checks and gaining entry, a person can still be checked in the national territory (either as part of a police check or an identity check by authorities responsible for immigration).

Table 2 - Current border checks of all persons crossing the external borders

3.4 Self-service systems, eGates and automated border control systems

3.4.1 Introduction

Regulation (EU) 2017/2225[84] provides the possibility for Member States to decide whether and to what extent to make use of technologies such as self-service systems, eGates and automated border control systems for entry and exit checks at the external borders. This regulation also specifies the tasks and roles of the border guards when making use of such technologies. In this regard, it should be ensured that the results of border checks carried out by automated means are available to border guards so as to enable them to take the appropriate decisions. In addition, the Regulation takes into account the need to supervise the use of self-service systems, eGates and automated border control systems by travellers so as to prevent fraudulent behaviour and usage.

Article 1 of Regulation (EU) 2017/2225 provides for the following definitions to be included in article 2 of the SBC:

[84] Regulation (EU) 2017/2225 of the European Parliament and of the Council of 30 November 2017 amending Regulation (EU) 2016/399 as regards the use of the Entry/Exit System.

- "self-service system" means an automated system which performs all or some of the border checks that are applicable to a person and which may be used for pre-enrolling data in the EES;
- "eGate" means an infrastructure operated by electronic means where an external border or an internal border where controls have not yet been lifted is actually crossed;
- "automated border control system" means a system which allows for an automated border crossing, and which is composed of a self-service system and an eGate.
- "confirmation of the authenticity and integrity of the chip data" means the process by which it is verified, through the use of certificates, that the data on the electronic storage medium (chip) originate from the issuing authority and that they have not been changed.

Automated border control systems shall, to the extent possible, be designed in such a way that they can be used by all persons, with the exception of children under 12 years of age. They shall also be designed in a way that fully respects human dignity, in particular in cases involving vulnerable persons. Where Member States decide to use automated border control systems, they shall ensure the presence of a sufficient number of staff to assist persons with the use of such systems.[85]

3.4.2 Use of automated border control systems for EU/EEA/CH citizens and for third country nationals who hold a residence card

3.4.2.1 Description

In its proposal for a Regulation amending Regulation (EU) 2016/399[86], The EU Commission proposed the introduction of a new Article 8a on the "Use of automated border control systems for EU/EEA/CH citizens and for third country nationals who hold a residence card". This proposed article listed the cumulative conditions that must be met by EU/EEA/CH citizens and for third country nationals who hold a residence card in order to use automated border control systems: *"In particular, the person concerned must be in possession of an electronic travel document whose chip data shall be authenticated. In addition, the facial image stored in the chip shall be accessed in order to verify the identity of the holder by comparing the facial image recorded in the chip and the live facial image of the holder of the travel document. For third countries enjoying the right of free movement under Union law who hold a residence card, the residence card hold must be an electronic card whose chip data shall be authenticated. In addition, the facial image stored in the chip shall be accessed so as to verify the identity of the holder of the residence card, by comparing the facial image recorded in the chip and his/her live facial image".*

However, this article was not included in the final version of Regulation (EU) 2017/2225. By consequence, neither in the final version of Regulation (EU) 2017/2225 nor in no other EU legal instrument, NO explicit references are made to the possible use of self-service systems, eGates and automated border control systems by persons enjoying the right to free-movement whom are not subject to registration in the EES.

3.4.2.2 Legal constraints for PROTECT scenarios

In the context of the PROTECT project, the following constraints derived from current EU on the use of automated border checks by persons enjoying the right of free movement under Union law should be taken into account:

1) Neither in the final version of Regulation (EU) 2017/2225 nor in any other EU legal instrument, NO explicit references are made to the use of self-service systems, eGates or automated border control systems by persons enjoying the right to free-movement whom are not subject to registration in the

[85] Article 8c of the SBC.

[86] 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, Brussels, 6.4.2016, COM(2016) 196 final, 2016/0105 (COD).

EES. This being said, no provision explicitly opposes the checks mentioned in article 8(2) of the SBC (see Section 3.1) to be operated by eGates and automated border control systems.

2) Even though no provision explicitly opposes the checks mentioned in article 8(2) of the SBC to be operated by eGates and automated border control systems, it seems very doubtful that such automated border checks could be operated on the basis of "additional biometrics" (other than fingerprints or facial image). Indeed, article 8(2) of the SBC explicitly states that "*where there are doubts as to the authenticity of the travel document or the identity of its holder, at least one of the biometric identifiers integrated into the passports and travel documents issued in accordance with Regulation (EC) No 2252/2004 shall be verified".*

3.4.3 Use of self-service systems and eGates for the border crossing by persons whose border crossing is subject to a registration in the EES

3.4.3.1 Description

Regulation (EU) 2017/2225[87] introduces a new article 8b in the SBC. According to this provision, persons whose border crossing is subject to a registration in the EES may be permitted to use self-service systems and eGates for the carrying out of their border checks, where all of the following conditions are fulfilled:

- the travel document contains an electronic storage medium (chip) and the authenticity and integrity of the chip data are confirmed using the complete valid certificate chain;
- the travel document contains a facial image recorded in the electronic storage medium (chip) which can be technically accessed by the self-service system so as to verify the identity of the holder of the travel document, by comparing that facial image with his or her live facial image; and
- the person is already enrolled or pre-enrolled in the EES.

For TCNs, where the above conditions are met, all checks described in section 3.2 may be carried out through a self-service system on entry and exit except:

- "Verification regarding the point of departure and the destination of the third-country national concerned and the purpose of the intended stay, checking, if necessary, the corresponding supporting documents".
- "Verification that the third-country national concerned has sufficient means of subsistence for the duration and purpose of the intended stay, for his or her return to the country of origin or transit to a third country into which he or she is certain to be admitted, or that he or she is in a position to acquire such means lawfully".[88]

On entry and exit, the results of the border checks carried out through the self-service system shall be made available to a border guard. That border guard shall monitor the results of border checks and, taking into account those results, authorise the entry or exit or, otherwise, refer the person to a border guard who shall proceed with further checks.

Finally, where an eGate is used, the corresponding registration of the entry/exit record and the linking of that record to the EES[89] (the EES system is analysed in Section 4.4) shall be carried out when crossing the border

[87] Regulation (EU) 2017/2225 of the European Parliament and of the Council of 30 November 2017 amending Regulation (EU) 2016/399 as regards the use of the Entry/Exit System.

[88] Please note that the verification "that the third-country national concerned, his or her means of transport and the objects he or she is transporting are not likely to jeopardise the public policy, internal security, public health or international relations of any of the Member States" also cannot be thoroughly checked only by consulting databases. However, the PROTECT consortium decided to leave customs checks out of the scope of the project.

[89] Pursuant to Article 14 of Regulation (EU) 2017/2226.

through the eGate. Where the eGate and the self-service system are physically separated, a verification of the identity of the user shall take place at the eGate in order to verify that the person using the eGate corresponds to the person who used the self-service system. The verification shall be carried out by using at least one biometric identifier. It should be underlined that the biometrics features that can be used for that linking process seem to be exclusively fingerprint data and facial image.[90]

3.4.3.2 Legal constraints for PROTECT scenarios

In the context of the PROTECT project, the following constraints derived from current EU rules on self-service systems, eGates and automated border control systems by TCNs should be taken into account:

1) According to article 8b of the SBC one of the conditions for persons whose border crossing is subject to a registration in the EES to be permitted to use automated border control systems is that *"the travel document contains a facial image recorded in the electronic storage medium (chip) which can be technically accessed by the self-service system so as to verify the identity of the holder of the travel document, by comparing that facial image with his or her live facial image"*. For this reason, it seems legally doubtful to use additional biometrics (other than facial image – and in certain cases fingerprints) for the aforementioned purpose.

2) Where the eGate and the self-service system are physically separated, a verification of the identity of the user shall take place at the eGate in order to verify that the person using the eGate corresponds to the person who used the self-service system. The verification shall be carried out by using at least one biometric identifier. However, it seems that the only biometrics features that can be used for that linking process (between the self-service system and the eGate) are exclusively fingerprint data and facial image (not additional emerging biometrics features). Indeed, article 3(18) of Regulation (EU) 2017/2226 defines "biometric data" as "fingerprint data and facial image".

3) It should be underlined that not all "background checks" on TCNs can be performed by using a self-service system without being pre-vetted in a National Facilitation Program (NFP), in particular, the following:

   - "Verification regarding the point of departure and the destination of the third-country national concerned and the purpose of the intended stay, checking, if necessary, the corresponding supporting documents";
   - "Verification that the third-country national concerned has sufficient means of subsistence for the duration and purpose of the intended stay, for his or her return to the country of origin or transit to a third country into which he or she is certain to be admitted, or that he or she is in a position to acquire such means lawfully".[91]

   The legal basis and conditions of NFPs which can potentially be established by national legislation are analysed in the next section.

[90] Indeed, article 3(18) of Regulation (EU) 2017/2226 defines "biometric data" as "fingerprint data and facial image".

[91] Please note that the verification "that the third-country national concerned, his or her means of transport and the objects he or she is transporting are not likely to jeopardise the public policy, internal security, public health or international relations of any of the Member States" also cannot be thoroughly checked only by consulting databases. However, the PROTECT consortium decided to leave customs checks out of the scope of the project.

3.4.4 National facilitation programs

3.4.4.1 Description

Article 8d of Regulation (EU) 2017/2225 provides that each Member State may establish a voluntary national facilitation programme (NFP). For TCNs who are granted access to these NFPs, the thorough checks do not have to include the following:

- "Verification regarding the point of departure and the destination of the third-country national concerned and the purpose of the intended stay, checking, if necessary, the corresponding supporting documents";

- "Verification that the third-country national concerned has sufficient means of subsistence for the duration and purpose of the intended stay, for his or her return to the country of origin or transit to a third country into which he or she is certain to be admitted, or that he or she is in a position to acquire such means lawfully".[92]

The Member States shall pre-vet TCNs applying to the NFPs in order to verify in particular that the following conditions are fulfilled:

- the applicant fulfils the entry conditions set out in Article 6(1) of the SBC;
- the applicant's travel document and, where applicable, visa, long-stay visa or residence permit are valid and not false, counterfeit or forged;
- the applicant proves the need for frequent or regular travel or justifies his or her intention to travel frequently or regularly;
- the applicant proves his or her integrity and reliability, in particular, where applicable, the lawful use of previous visas or visas with limited territorial validity, his or her economic situation in the country of origin and his or her genuine intention to leave the territory of the Member States before the end of the authorised period of stay. Authorities (listed hereunder) shall have access to the EES to verify that the applicant has not previously exceeded the maximum duration of authorised stay on the territory of the Member States;
- the applicant justifies the purpose and conditions of the intended stays;
- the applicant possesses sufficient means of subsistence both for the duration of the intended stays and for the return to the country of origin or residence, or that the applicant is in a position to acquire such means lawfully;
- the SIS is consulted.

Such TCNs must be pre-vetted by border guards, by visa authorities as defined in point 3 of Article 4 of Regulation (EC) No 767/2008 or by immigration authorities as defined in point (4) of Article 3(1) of Regulation (EU) 2017/2226. When verifying in accordance whether the applicant fulfils the conditions, particular consideration shall be given to assessing whether the applicant presents a risk of illegal immigration or a risk to the security of any of the Member States and whether the applicant intends to leave the territory of the Member States during the authorised stay. The means of subsistence for the intended stays shall be assessed according to the duration and the purpose of the envisaged stay or stays and by reference to average prices in the Member States concerned for board and lodging in budget accommodation, on the basis of the reference amounts set by the Member States. Proof of sponsorship, private accommodation, or both, may

[92] Please note that the verification "that the third-country national concerned, his or her means of transport and the objects he or she is transporting are not likely to jeopardise the public policy, internal security, public health or international relations of any of the Member States" also cannot be thoroughly checked only by consulting databases. However, the PROTECT consortium decided to leave customs checks out of the scope of the project.

also constitute evidence of sufficient means of subsistence. The examination of an application shall be based, in particular, on the authenticity and reliability of the documents submitted and, on the veracity, and reliability of the statements made by the applicant. If a Member State responsible for examining an application has any doubts about the applicant, the applicant's statements or supporting documents that have been provided, it may consult other Member States before any decision on the application is taken.

First access to the NFP shall be granted for a maximum of one year. Access may be extended for a maximum of a further five years or until the end of the validity period of the travel document or any issued multiple-entry visas, long-stay visas and residence permits, whichever is shorter. In the case of an extension, the Member State shall reassess every year the situation of each TCN who is granted access to the NFP in order to ensure that, based on updated information, that third-country national still meets the abovementioned conditions. This reassessment may be performed when border checks are carried out.

Border guards may carry out the verification of the TCN benefiting from the NFP by comparing the facial image taken from the electronic storage medium (chip) and the facial image in the third-country national's individual EES file with that third-country national's face. Full verification shall be carried out at random and on the basis of a risk analysis.

3.4.4.2 Legal constraints for PROTECT scenarios

In both the mobile and the passport scenarios being described in D3.1, a passenger which would like to use the "PROTECT" solution for the first time would need to register via an enrolment kiosk. At this kiosk, they would undergo a background check in relevant European and national databases. Once this pre-verification is concluded with a positive result, the system would verify the electronic passport and passenger's biometric features with the templates stored on the chip. The entire enrolment process would be supervised by a border guard who provides assistance and monitors whether the process goes as planned. The positive results of the prior step would then allow passengers for the registration of additional biometric features that are applied in the PROTECT solution.

Given that the scenarios described in D3.1 do not foresee the verification at the kiosk of the two following elements:

- "Verification regarding the point of departure and the destination of the third-country national concerned and the purpose of the intended stay, checking, if necessary, the corresponding supporting documents";
- "Verification that the third-country national concerned has sufficient means of subsistence for the duration and purpose of the intended stay, for his or her return to the country of origin or transit to a third country into which he or she is certain to be admitted, or that he or she is in a position to acquire such means lawfully";

In this deliverable, it assumed that the envisaged purpose of D3.1 scenarios is NOT to develop a potential technical solution for NFPs. Furthermore, even it was the case, the processing of additional biometrics for NFP purposes would *a priori* seem to be disproportionate as article 8d of the SBC refers to the sole comparison of "*the facial image taken from the electronic storage medium (chip) and the facial image in the third-country national's individual EES file with that third-country national's face".*

4 Biometrics in EU information systems for border control management

4.1 Introduction

Having recalled the border checks processes of all persons crossing the external borders which should be taken into account by the PROTECT scenarios described in D3.1, this section provides for an overview of the EU databases for border control management, the purposes of these databases and the information contained therein. Indeed, border control management increasingly relies on information provided to border guards through the consultation of a number of centralized databases. For what concerns these information systems, each have their own objectives, purposes, legal bases, user groups and institutional context. Given that the main objective of the PROTECT project is to develop a contactless multimodal biometric solution for identity confirmation of travellers to help border guards to facilitate and fasten the border crossings of travellers, the PROTECT consortium decided to focus its analysis on the information systems being used for border management and exclude from its scope the information systems used for law enforcement purposes.[93] The figure below illustrates this distinction.[94]

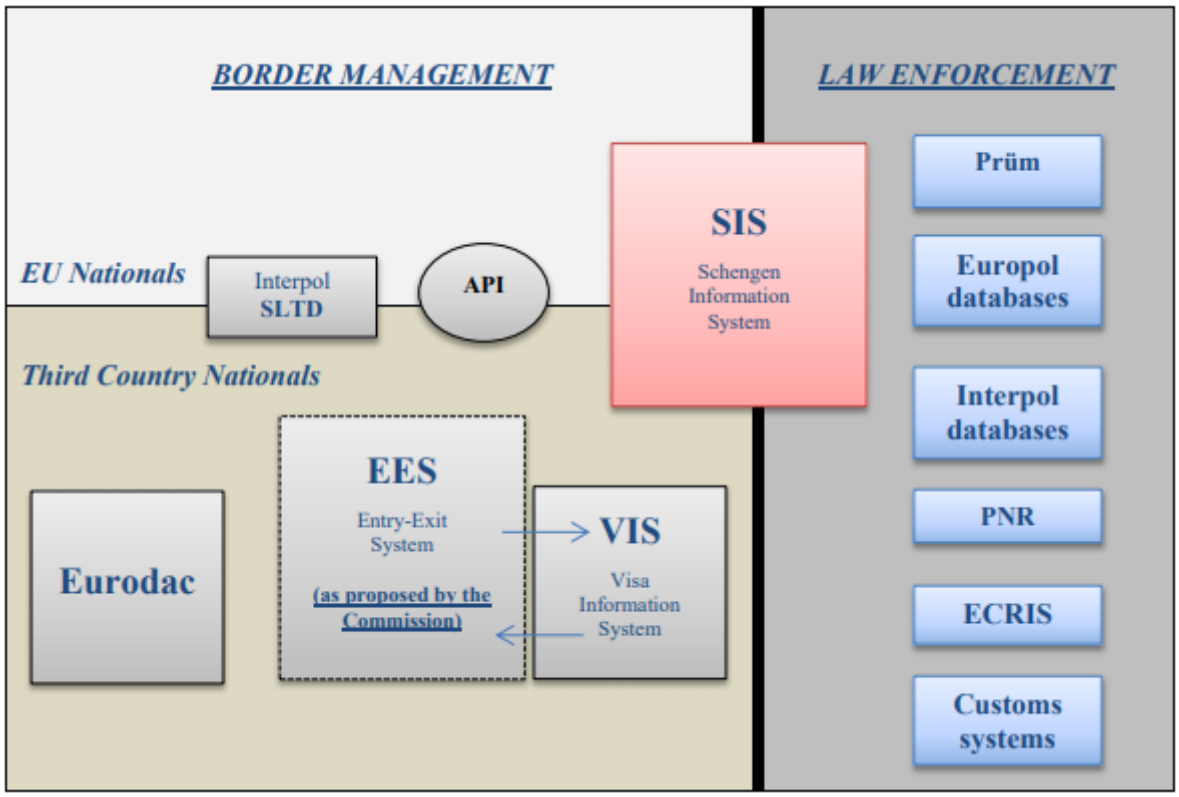

Figure 7 - Schematic overview of the main information systems for border management

The four main centralized information systems developed by the EU for border control management are (i) the Schengen Information System (SIS) with a broad spectrum of alerts on persons and objects, (ii) the Visa Information System (VIS) with data on short-stay visas, (iii) the Entry-Exit System (EES), which expected to be implemented by 2020 to replace manual stamping of passports and (iv) the EURODAC system with fingerprint

[93] In the same way, for SIS, this deliverable only analyses the system from the border control management purpose, excluding the law enforcement purposes and accesses by law enforcement authorities.

[94] This illustration was issued in Communication from the Commission to the European Parliament and the Council, "Stronger and Smarter Information Systems for Borders and Security", Brussels, 6.4.2016, COM(2016) 205 final, p.6.

data of asylum applicants and third-country nationals who have crossed the external borders irregularly. These four systems are complementary, and – with the exception of SIS – primarily targeted at third-country nationals. Additional existing instruments for border management are Interpol's Stolen and Lost Travel Documents (SLTD) database and the Advance Passenger Information (API) that collects information on passengers ahead of inbound flights to the EU. Finally, the EU Commission is proposing a EU Travel Information and Authorisation System (ETIAS), where visa-exempt travellers would register relevant information regarding their intended journey.

As a preliminary remark, it should be emphasised that the four EU centralized databases using biometrics for border control management (SIS, VIS, EES, EURODAC) are (or are in the process) to rely on:

- Fingerprints
- Facial image

The table below illustrates the biometric data stored in in existing and planned IT-systems for border control management purposes. Proposed systems and proposed changes in italics. It is worth mentioning that the ETIAS proposal, SLTD and API systems do not contain any biometrics.

	SIS (immigration control)	VIS	EES	EURODAC	ETIAS proposal
Biometrics included	*Fingerprints and facial image, according to SIS II proposals on borders and return*	Fingerprints and facial image as of the age of 12 years	Fingerprints and facial image as of the age of 12 years	Fingerprints as of the age of 14 years, and fingerprints and *facial image as of the age of 6 years, according to Eurodac proposal (2016)*	No

Table 3 - Overview of biometrics contained in Schengen databases

4.2 The Schengen Information System (SIS)

4.2.1 Purpose of SIS

SIS is currently the largest and most widely used information exchange platform on immigration.[95] It is a centralised system used by 25 EU Member States[96] and four Schengen associated countries[97], currently containing 63 million alerts. The second generation of the Schengen Information System (hereinafter "SIS II") entered into operation on the basis of Regulation (EC) No 1987/2006[98] and contains records on third-country nationals prohibited to enter or stay in the Schengen area as well as on EU and third country nationals who are wanted or missing (including children) and on wanted objects (firearms, vehicles, identity documents,

[95] This deliverable only analyses SIS from the border management perspective excluding the law enforcement purposes of the system.

[96] All, except Ireland, Cyprus, Croatia

[97] Switzerland, Liechtenstein, Norway, Iceland

[98] Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second-generation Schengen Information System (SIS II), (OJ L 381, 28.12.2006, p. 4).

industrial equipment, etc.). For border control management purposes, the SIS enables border guards to consult alerts on third-country nationals for the purpose of refusing their entry into or stay in the Schengen Area.

Furthermore, it is worth mentioning that on 21 December 2016 the Commission issued a "SIS Proposal on return".[99] The aim of this proposal is to:

- oblige Member States to enter an alert in the SIS in all cases where an entry ban has been issued to an illegally staying third country national in accordance with Directive 2008/115/EC15 (hereinafter "Return directive")[100];
- harmonise national procedures by introducing a new obligatory consultation procedure to avoid that a third-country national who is subject to an entry ban in one Member State, holds a valid residence permit issued by another Member State.

4.2.2 Current use of biometrics in SIS for border control management

For alerts on persons, articles 20 of Regulation 1987/2006 state that the information on persons in relation to whom an alert has been issued **shall be no more** than the following:

- surname(s) and forename(s), name(s) at birth and previously used names and any aliases which may be entered separately;
- any specific, objective, physical characteristics not subject to change;
- place and date of birth;
- sex;
- photographs;
- fingerprints;
- nationality(ies);
- whether the person concerned is armed, violent or has escaped;
- reason for the alert
- authority issuing the alert;
- a reference to the decision giving rise to the alert;
- action to be taken;
- link(s) to other alerts issued in SIS II;

In the context of the PROTECT project, it should be emphasized that photographs (not facial image) and fingerprints are currently the only biometric modalities which may currently be processed within the SIS II database for border control management purposes. Furthermore, fingerprints can only be used to verify and confirm the identity of a person who has already been identified on the basis of an alphanumeric **search.**[101] This being said, it is worth mentioning that the new article 2e of the SBC Regulation as amended by Regulation (EU) 2017/458 specifies that checks against SIS may be carried out in advance on the basis of API data

[99] Proposal for a Regulation of the European Parliament and of the Council on the use of the Schengen Information System for the return of illegally staying third country nationals (hereinafter "the SIS Proposal on return"), COM(2016) 881 final.
[100] Directive 2008/115/EC of the European Parliament and of the Council of 16 December 2008 on common standards and procedures in Member States for returning illegally staying third-country nationals (OJ L 348, 24.12.2008, p. 98).
[101] Article 22, b) of Regulation 1987/2006.

received in accordance with Council Directive 2004/82/EC. Where those checks are carried out in advance on the basis of such data, the data received in advance shall be checked at the border crossing point against the data in the travel document.

Article 22 (a)of Regulation 1987/2006 contains specific rules for photographs and fingerprints in SIS. This article reads as follows:

"The use of photographs and fingerprints […] shall be subject to the following provisions:

(a) photographs and fingerprints shall only be entered following a special quality check to ascertain the fulfilment of a minimum data quality standard. [specifications of the special quality check shall be established in accordance to the procedure referred to in article 67 of Decision 2007/533/JHA and 51 of Regulation 1987/2006]"

In this context, on 4 August 2016, the EC adopted implementing Decision (EU) 2016/1345 on minimum data quality standards for fingerprint records within SIS II.[102] The annex of this Decision sets forth the minimum requirements relating to standards and input formats which are to be met when capturing and transmitting fingerprint data to SIS II.

4.2.3 Future use of biometrics in SIS for border control management

4.2.3.1 Automatic Fingerprint Identification System (AFIS)

Article 22(c) of Regulation 1987/2006 foresees that SIS may also be used to identify a person on the basis of his/her fingerprints, a functionality which requires the implementation of an Automatic Fingerprint Identification System (AFIS) "*once it becomes technically possible"* and when the Commission has presented *"a report on the availability and readiness of the required technology on which the European Parliament is consulted"*. In 2015, the Joint Research Centre (JRC) published a study, carried out for DG HOME, on the readiness and availability of AFIS technologies for their introduction in SIS-II. [103] The study summarises a review of the scientific literature, visits to authorities managing AFIS in nine Member States and in the United States of America and consultations with eu-LISA and with AFIS vendors. The study concludes that AFIS technology has reached a satisfactory level of readiness and availability and proposes a series of recommendations in order to accomplish a successful implementation of a SIS-II AFIS. On the basis of this study, in 2016, the Commission issued a report on "The availability and readiness of technology to identify a person on the basis of fingerprints held in the second-generation Schengen Information System (SIS II)".[104] The conclusion of this report is that the Commission considers that the implementation of 19 recommendations should be considered to support the successful deployment and use of an AFIS in SIS.

It is worth mentioning that the Commission envisages the use of AFIS, in case of doubts on the identity of a traveller, in its Proposal for a Regulation on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks[105] (hereinafter "the SIS Proposal on border checks"). Indeed, article 28 of the Proposal states that "*If the identity of the person cannot be ascertained by other*

[102] Commission Implementing Decision (EU) 2016/1345 of 4 August 2016 on minimum data quality standards for fingerprint records within the second generation Schengen Information System (SIS II) (notified under document C(2016) 4988).

[103] This study is available at http://publications.jrc.ec.europa.eu/repository/bitstream/JRC97779/lbna27473enn.pdf

[104] Report from the Commission to the European Parliament and the Council, "The availability and readiness of technology to identify a person on the basis of fingerprints held in the second generation Schengen Information System (SIS II)", Brussels, 29.2.2016, COM(2016) 93 final.

[105] Proposal for a Regulation of the European Parliament and of the Council on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, amending Regulation (EU) No 515/2014 and repealing Regulation (EC) No 1987/2006 (hereinafter "the SIS Proposal on border checks"), COM(2016) 882 final. Current version is available at
http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_14115_2017_INIT&from=EN

means, dactyloscopic data shall be searched for identification purposes. Dactyloscopic data may be searched in all cases to identify a person".[106]

4.2.3.2 Facial image

In its SIS Proposal on border checks, the Commission also envisages the inclusion of facial image in the SIS in order to ensure consistency in border control procedures where the identification and the verification of identity are required by the use of facial images.[107] *Article 28(4) specifies that "As soon as this becomes technically possible, and while ensuring a high degree of reliability of identification, photographs and facial images may be used to identify a person. Before this functionality is implemented in SIS, the Commission shall present a report on the availability and readiness of the required technology, on which the European Parliament shall be consulted. Identification based on photographs or facial images shall only be used subject to national law".*

4.2.4 Legal constraints for PROTECT scenarios

In the context of the PROTECT project, the following major constraint derived from current EU rules on SIS II should be taken into account:

1) First, it should be recalled that Regulation (EU) 2017/458 imposes the travel documents of both all third-country nationals and persons enjoying the right of free movement to be verified against SIS II on entry and exit of the Schengen Area.
2) Secondly, Article 22 of Regulation 1987/2006 specify that the only biometric modalities which may currently be processed within the SIS II database are photographs (facial image in the future) and fingerprints. Furthermore, currently, fingerprints can only be used to verify and confirm the identity of a person who has already been identified on the basis of an alphanumeric search.

4.3 The Visa Information System (VIS)

4.3.1 Purpose of VIS

The VIS is a centralised system for the exchange of data on short-stay visas between Member States. It processes data and decisions relating to applications for short-stay visas to visit, or to transit through, the Schengen area. All the consulates of the Schengen States (around 2000) and all their external border crossing points (in total some 1800) have been connected to the system. The VIS contains data on visa applications and decisions, as well as whether issued visas are revoked, annulled, or extended. It currently contains data on 20 million visa applications and, at peak-times, it handles over 50.000 transactions per hour.

Article 2 of Regulation (EC) No 767/2008[108] defines the purpose of VIS as to improve the implementation of the common visa policy, consular cooperation and consultations between the central visa authorities by:

---

[106] In the same way, recital 18A of the SIS Proposal on border checks states that *"It should be possible in all cases to identify a person by using dactyloscopic data. Wherever the identity of the person cannot be ascertained by any other means, dactyloscopic data should be used to attempt to ascertain the identity".*

[107] Article 20 (w) of the SIS Proposal on border checks.

[108] Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation) as amended by Regulation (EC) No 810/2009 of the European Parliament and of the Council of 13 July 2009 establishing a Community Code on Visas (Visa Code). A consolidated version is available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2008R0767:20100405:EN:PDF

- facilitating the visa application procedure;
- preventing visa shopping;
- facilitating the fight against fraud;
- facilitating checks at external border crossing points and in the national territories;
- assisting in the identification of persons that do not meet the requirements for entering, staying or residing in the national territories;
- facilitating the application of the Dublin III Regulation[109] for determining the EU country that is responsible for the examination of a non-EU country national's asylum application and for examining said application;
- contributing to the prevention of threats to EU countries' internal security.

4.3.2 Current use of biometrics in VIS

Article 5 of Regulation (EC) No 767/2008 specifies that only the following categories of data are recorded in the VIS:

- alphanumeric data on the applicant and on the visas requested, issued, refused, annulled, revoked or extended;
- photographs;
- fingerprint data;
- links to previous visa applications and to the application files of persons travelling together.

As noted in Section 2.4, 10 fingerprints and a digital photograph (not facial image) are collected from persons applying for a visa. These biometric data, along with data provided in the visa application form, are recorded in the Visa Information System (VIS).[110]

At the entry of Schengen Area's external borders, border guards "*have access to search [the VIS] with the number of the visa sticker in combination with verification of fingerprints of the visa holder, or the number of the visa sticker"*.[111] By consequence, when arriving at the external border of the Schengen area, visa holders have to provide their fingerprints for comparison with those registered in the VIS, if requested by Schengen States' border control authorities. This process is meant to guarantee that the person that applied for the visa is the same person as the one crossing the border.

Commission Decision of 9 October 2009 lays down specifications for the resolution and use of fingerprints for biometric identification and verification in the VIS.

4.3.3 Future use of biometrics in VIS

In 2016, an overall evaluation of the VIS stated that *"to address reported hindrances in collecting biometrics, in particular those affecting the quality of facial images, and to allow in the future combined searches using*

[109] Regulation (EU) No 604/2013 (Dublin III Regulation), replacing Council Regulation (EC) No 343/2003 (Dublin II Regulation), lays down the criteria and mechanisms for determining which EU country is responsible for examining an asylum application.

[110] 10-digit finger scans are not required from children under the age of 12 or from people who physically cannot provide finger scans. Frequent travellers to the Schengen Area do not have to give new finger scans every time they apply for a new visa. Once finger scans are stored in VIS, they can be re-used for further visa applications over a 5-year period.

[111] Article 20 of the Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation).

facial image, alternative standards could be put in place, such as taking photographs directly when applying for a visa".[112]

The Commission confirmed its intention to use the facial image for biometric matching against the VIS in in article 15.5 of Regulation (EU) 2017/2226 which reads as follows*: "Within a period of two years following the start of operations of the EES, the Commission shall produce a report on the quality standards of facial images stored in the VIS and on whether they are such that they enable biometric matching with a view to using facial images stored in the VIS at borders and within the territory of the Member States for the verification of the identity of third-country nationals subject to a visa requirement, without storing such facial images in the EES. The Commission shall transmit that report to the European Parliament and to the Council. That report shall be accompanied, where considered appropriate by the Commission, by legislative proposals, including proposals to amend this Regulation, Regulation (EC) No 767/2008, or both, as regards the use of the facial images of third-country nationals stored in the VIS for the purposes referred to in this paragraph".*

4.3.4 Legal constraints for PROTECT scenarios

In the context of the PROTECT project, the following major constraint derived from current EU rules on VIS should be taken into account:

Currently, at border crossing points, the VIS is used to verify the identity of visa holders by comparing his/her fingerprints with the fingerprints stored in the VIS on request of the border guards. This process guarantees that the person that applied for the visa is the same person as the one crossing the border. The fact that TCNVHs could be required to provide their fingerprint at the entry of the Schengen Area should be taken into account when developing a complete contactless biometric-based cross-border control solution. The use the facial image for biometric matching against the VIS has not yet been implemented. This issue could be resolved once the EES will become functional and that TCNVHs would be able to pre-enrol their facial image into that system.

4.4 The Entry-exit system (EES)

4.4.1 Background

In February 2013, the Commission adopted a "Smart Borders package" consisting of three proposals: (1) a Regulation for an Entry/Exit System (EES)[113] for the recording of information on the time and place of entry and exit of third country nationals travelling to the Schengen area, (2) a Regulation for a Registered Traveller Programme (RTP)[114] to allow third country nationals who have been pre-vetted to benefit from facilitation of border checks at the Union external border, (3) a Regulation amending the Schengen Borders Code[115] in order to take into account the existence of the EES and RTP.

[112] Report from the Commission to the European Parliament and the Council on the implementation of Regulation (EC) No 767/2008 of the European Parliament and of the Council establishing the Visa Information System (VIS), the use of fingerprints at external borders and the use of biometrics in the visa application procedure/REFIT Evaluation, Brussels, 14.10.2016, COM(2016) 655 final, p.13.

[113] Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data of third country nationals crossing the external borders of the Member States of the European Union Brussels, 28.2.2013, COM(2013) 95 final.

[114] Proposal for a Regulation of the European Parliament and of the Council establishing a Registered Traveller Programme, Brussels, 28.2.2013, COM(2013) 97 final.

[115] Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No 562/2006 as regards the use of the Entry/Exit System (EES) and the Registered Traveller Programme (RTP), COM (2013) 96.

This 2013 SBP package was poorly received. The European Parliament and the Council expressed strong reservations over its cost, technical feasibility, and scope.[116] The European Data Protection Supervisor (EDPS), the Article 29 Working Party (WP29), and civil society groups such as the Meijers Committee voiced major concerns regarding necessity and proportionality, particularly in light of the volume of personal data processing the measures would entail. The European Commission's own Impact Assessment Board twice asked DG Home to provide evidence supporting the need for EU action in relation to the objectives set by the Smart Borders package.[117]

In the context of the preparation of a revised proposal and in order to assess the technical, organisational and financial impact of possible solutions to the contentious issues, the Commission initiated with the support of both co-legislators a so-called "proof of concept" exercise consisting of two stages:

- A Commission-led Technical Study on Smart Borders[118], and
- A testing phase led by eu-LISA (European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice) on the impact of the use of various biometric identifiers on the border control processes.[119]

The Commission also conducted a public consultation on the Smart Borders Package, inviting citizens (both EU nationals and non-EU nationals) and organisations to contribute. The results of the consultation were published in December 2015.[120]

After having carried out this long process, on April 2016, the EC adopted a revised legislative proposal for Smart Borders in which she decided to:

- revise its 2013 proposal for a Regulation for the establishment of an Entry/Exit System (hereafter "EES proposal")[121];
- revise its 2013 proposal for Regulation amending the Schengen Borders Code to integrate the technical changes that result from the new proposal for a Regulation establishing an Entry/Exit System (hereafter "SBC-EES proposal")[122].

[116] European Parliament IMPA (2013), Initial appraisal of a European Commission impact assessment: Smart Borders Package, PE 514.062.

[117] European Commission Impact Assessment Board (2013), Opinion – DG Home – Impact assessment on a proposal establishing the entry/exit system, Brussels, 2010/HOME/004; European Commission Impact Assessment Board (2013), Opinion – DG Home – Impact assessment on a proposal establishing the entry/exit system, Brussels, 2010/HOME/006.

[118] Technical Study on Smart Borders, European Commission, DG HOME, 2014. http://ec.europa.eu/dgs/home-affairs/what-wedo/policies/borders-and-visas/smart-borders/index_en.htm

[119] The aim of the Pilot was to verify the feasibility of the options proposed in the Technical Study in operational environments with real travellers across the EU. Twelve different test cases were performed in 18 Border Crossing Points spread over eleven Member States, covering air, sea and land borders in different climatological situations, with different operational requirements. In total 78 tests were carried out. The pilot not only collected quantitative test case results but also sought feedback from travellers as well as border guards. See Final Report of the Smart Borders Pilot Project, eu-LISA, December 2015. http://ec.europa.eu/dgs/home-affairs/what-wedo/policies/borders-and-visas/smart-borders/index_en.htm

[120] Results of the consultations are available at https://ec.europa.eu/home-affairs/what-is-new/public-consultation/2015/consulting_0030

[121] Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third country nationals crossing the external borders of the Member States of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No 767/2008 and Regulation (EU) No 1077/2011, Brussels, 6.4.2016, COM(2016) 194 final.

[122] 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, Brussels, 6.4.2016, COM (2016) 196 final

- withdraw its 2013 proposal for a Regulation for a Registered Traveller Programme (RTP). Nonetheless, the SBC-EES proposal introduces a legal provision for national facilitation programmes that can be established by Member States on a voluntary basis (Article 8e).

On 25 October 2017, the European Parliament plenary session voted to adopt the Entry/Exit System. Members also approved the amendments needed to integrate the new Entry/Exit System into the Schengen Borders Code. The Council adopted both Regulation (EU) 2017/2225[123] and Regulation (EU) 2017/2226[124] in November 2017. The Entry/Exit System is due to become fully functional by 2020 at the latest.

4.4.2 Purpose of the EES

As already mentioned, the general rule is that TCNs have the right to enter the Schengen area for a short stay of up to 90 days within any 180-day period either with or without the need for the prior granting of a visa. Third country nationals who are in possession of a valid residence permit or long stay visa issued by a Member State ('residence permit holders') are not bound by this limitation. Currently the stamping of the travel documents indicating the dates of entry and exit is the sole method available to border guards and immigration authorities to calculate the duration of stay of "short stay TCNs" and to verify if someone is overstaying. These stamps can be difficult to interpret: they may be unreadable or the result of counterfeiting.

For that reason, the aims of Regulation (EU) 2017/2226 establishing the EES is to ensure:

« (a) the recording and storage of the date, time and place of entry and exit of third–country nationals crossing the borders of the Member States at which the EES is operated;

(b) the calculation of the duration of the authorized stay of such third-country nationals;

(c) the generation of alerts to Member States when the authorized stay has expired; and

(d) the recording and storage of the date, time and place of refusal of entry of third-country nationals whose entry for a short stay has been refused, as well as the authority of the Member State which refused the entry and the reasons therefor".[125]

The Regulation establishing the EES addresses TCNs entering the Schengen area for a short stay with or without visa (both TCNVHs and TCNVEs). Third-country nationals who enjoy the right of free movement or the rights of free movement equivalent to those of EU citizens (family members of EU citizens or permanent residents) but who do not yet have a residence card are also included. On the other hand, the proposed EES Regulation excludes from its scope persons enjoying the right of free movement, TCNs holding a residence permit, TCNs holding a long-stay visa as well as other TCNs under Article 2(3) of the proposed EES Regulation.

An automated calculator is included in the EES to inform border guards:

« (a) on entry, of the maximum duration of authorized stay of third-country nationals and whether the number of authorized entries of a short-stay visa issued for one or two entries has been exhausted;

[123] Regulation (EU) 2017/2225 of the European Parliament and of the Council of 30 November 2017 amending Regulation (EU) 2016/399 as regards the use of the Entry/Exit System.

[124] Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011.

[125] Article 1 of Regulation (EU) 2017/2226.

(b) during checks or verifications carried out within the territory of the Member States, of the remaining authorized stay or duration of overstay of the third-country nationals;

(c) on exit, of any overstay of third-country nationals;

(d) when examining and deciding on short-stay visa applications, of the maximum remaining duration of authorized stay based on intended entry dates".[126]

4.4.3 Storage of biometrics in the EES

The data registered in the revised EES includes 26 elements, down from 36 in the 2013 proposal:

- Identity of third-country national: first name, surname, date of birth, nationality, gender;
- Biometrics: four fingerprints and a facial image for TCNVEs. The EES does not store the biometric data of TCNVHs, which remain stored in VIS;
- Information on travel document: document number, document type, document country code and expiry date;
- Information on the TCHVHs: visa sticker number, visa expiry date, number of authorised entries, authorised period of stay;
- Information on cross-border movements of the person: date and time of entry, authority allowing entry, entry border crossing point, date and time of exit, exit border crossing point;
- Information on changes of authorisation of stay: revised expiry date of the authorisation of stay, date of change of limit of stay, place of change of limit of stay, ground for change or revocation.

The EES system would process biometric data of both TCNVHs and TCNVEs in two ways:

- Firstly, by recording/enrolling biometric identifiers from TCNVEs (four fingerprints in combination with a facial image). The four fingerprints are used at enrolment to check if the third country national was already registered in the system while the facial image allows for a quick and reliable (automatic) verification at subsequent entry that the individual subject to the border control is the one already registered in the EES;
- Secondly, by pulling biometric identifiers for TCNVHs from VIS.

This statement is written down in Recital 21 of Regulation (EU) 2017/2226 which reads as follows: *"Four fingerprints per visa-exempt third–country national should be registered in the EES, if physically possible, to allow for accurate verification and identification, thus ensuring that the third–country national is not already registered under another identity or with another travel document, and to guarantee that sufficient data are available in order to ensure that the objectives of the EES are achieved in every circumstance. The fingerprints of visa-holding third-country nationals should be checked against the VIS. The facial image of both visa-exempt and visa holding third-country nationals should be registered in the EES. Fingerprints or facial images should be used as a biometric identifier for verifying the identity of third–country nationals who have been previously registered in the EES, for as long as their individual files have not been deleted".*

[126] Article 11(2) of Regulation (EU) 2017/2226.

4.4.4 Use of self-service systems for pre-enrolling data in the EES

Regulation (EU) 2017/2225 introduces a new article 8a in the SBC. According to this provision, persons whose border crossing is subject to a registration in the EES may use self-service systems for the purpose of pre-enrolling in the EES if the following conditions are fulfilled:

- the travel document contains an electronic storage medium (chip) and the authenticity and integrity of the chip data are confirmed using the complete valid certificate chain;
- the travel document contains a facial image recorded in the electronic storage medium (chip) which can be technically accessed by the self-service system so as to verify the identity of the holder of the travel document by comparing the facial image recorded in the electronic storage medium (chip) with his or her live facial image; if technically and legally possible, this verification may be done by verifying the live fingerprints against the fingerprints recorded in the electronic storage medium (chip) of the travel document.

If the two above conditions are fulfilled, persons whose border crossing is subject to a registration in the EES may use self-service systems to pre-enrol in the EES the following data:

- surname (family name), first name or names (given names), date of birth, nationality or nationalities, sex;
- the type and number of the travel document or documents and the three-letter code of the issuing country of the travel document or documents;
- the date of expiry of the validity of the travel document or documents;
- the facial image;
- where applicable, the status of that third-country national indicating that he or she is a third-country national who: a) is a member of the family of a Union citizen to whom Directive 2004/38/EC applies or of a national of a third country enjoying the right of free movement equivalent to that of Union citizens under an agreement between the Union and its Member States, on the one hand, and a third country, on the other; and b) does not hold a residence card pursuant to Directive 2004/38/EC or a residence permit pursuant to Regulation (EC) No 1030/2002;
- the short-stay visa sticker number, including the three-letter code of the issuing Member State, the type of short-stay visa, the end date of the maximum duration of the stay as authorized by the short-stay visa, which shall be updated at each entry, and the date of expiry of the validity of the short-stay visa, where applicable;
- on the first entry on the basis of a short-stay visa, the number of entries and the duration of stay authorized by the short-stay visa as indicated on the short-stay visa sticker;
- where applicable, the information indicating that the short-stay visa has been issued with limited territorial validity.

After the above-mentioned data are pre-enrolled, the self-service system shall verify whether the person has a previous registration in the EES and shall verify the identity of the third-country national in accordance with the following procedure:

1) In the event that data concerning the person are not recorded in the EES, third-country nationals who are subject to a visa requirement to cross the external borders shall pre-enrol in the EES through the self-service system the abovementioned data. Subsequently, the person shall be referred to a border guard who shall:
    - pre-enrol the data concerned, where it was not possible to collect all the required data through the self-service system;
    - verify that the travel document used at the self-service system corresponds to the one held by the person in front of the border guard, that the live facial image of the person concerned

corresponds to the facial image that was collected though the self-service system, and for persons who do not hold a visa required, that the live fingerprints of the person concerned correspond to the fingerprints that were collected though the self-service system;

- when the decision to authorise or refuse entry has been taken, confirm the data.

2) Where the pre-enrolment operations indicate that data on the person are recorded in the EES, the self-service system shall assess whether any of the data need to be updated. Where this assessment reveals that the person referred has an individual file registered in the EES but that his or her data need to be updated, the person shall:

- update the data in the EES by pre-enrolling them through the self-service system;
- be referred to a border guard who shall verify the correctness of the update under point (a) of this paragraph and, when the decision to authorise or refuse entry has been taken, update the individual file.

Self-service systems shall be operated under the supervision of a border guard who shall be in charge of detecting any inappropriate, fraudulent or abnormal use of the self-service system.

4.4.5 Use of biometrics in the EES by border guards

Article 23 of Regulation (EU) 2017/2226 contains the rules of access of border guards to the EES. Border authorities have access to the EES for verifying the identity and previous registration of the third-country national, for updating the EES data where necessary and for consulting the data to the extent required for the carrying out of border checks. While performing these tasks, the border authorities have access to search with the following data:

(a) surname (family name); first name or names (given names); date of birth; nationality or nationalities; sex;

(b) the type and number of the travel document or documents and the three-letter code of the issuing country of the travel document or documents;

(c) the date of expiry of the validity of the travel document or documents.

In addition, for the purposes of consulting the VIS for verification of third-country nationals who are subject to a visa requirement, the border authorities shall launch a search in the VIS directly from the EES using the same alphanumeric data.

If the search in the EES with the above-mentioned data indicates that data on the third-country national are recorded in the EES, the border authorities shall compare the live facial image of the third-country national with the facial image in the EES or the border authorities shall, in the case of visa-exempt third-country nationals, proceed to a verification of fingerprints against the EES and, in the case of third-country nationals subject to a visa requirement, proceed to a verification of fingerprints directly against the VIS. For the verification of fingerprints against the VIS for visa holders, the border authorities may launch the search in the VIS directly from the EES. If the verification of the facial image fails, the verification shall be carried out using fingerprints and vice versa. It has to be emphasized that the main biometric identifier (facial image or fingerprint) to be used for verification at border crossing points depends on a choice of national authorities. Indeed, recital 21 states that: *"In order to take into account the specificities of each border crossing point and the different kinds of borders, the national authorities should establish for each border crossing point whether the fingerprints or the facial image are to be used as the main biometric identifier for carrying out the required verification".*

4.4.6 Legal constraints for PROTECT scenarios

In the context of the PROTECT project, the following major constraint derived from current EU rules on EES should be taken into account:

1) According to Regulation (EU) 2017/2226, in order to take into account the specificities of each border crossing point and the different kinds of borders, the national authorities should establish for each border crossing point whether the fingerprints or the facial image are to be used as the main biometric identifier for carrying out the required verification. To be pragmatic, this means that a complete contactless solution could not yet be implemented at borders where the main chosen biometric feature for verification against the EES is fingerprints.

2) It should be emphasized that for TCNVHs, the border guards must launch a search from the EES to the VIS for biometric verification. As a reminder, currently, the VIS is used to verify the identity of visa holders by comparing his/her fingerprints with the fingerprints stored in the VIS on request of the border guards. The fact that TCNVHs could be required to provide their fingerprint at the entry of the Schengen Area should be taken into account when developing a complete contactless biometric-based cross-border control solution. The use the facial image for biometric matching against the VIS has not yet been implemented. This issue could be resolved once the EES will become functional and that TCNVHs would be able to pre-enrol their facial image into that system.

3) Furthermore, both in the passport and the mobile scenarios (both types A and B), D3.1 envisages the enrolment of additional biometrics (other than fingerprints or facial image) at "a kiosk". It is not clear whether a self-service system (referred to as "kiosk" in D3.1) as defined by article 1 of Regulation (EU) 2017/2225 could be used to enrol additional biometrics other than facial image as this is the only biometric feature explicitly listed by for possible enrolment in Article 8a of said Regulation.

4.5 EURODAC

EURODAC is an EU-wide biometric database containing fingerprints of asylum applicants and non-EU/EEA nationals for comparison between EU countries. The EURODAC fingerprint database has been established by Council Regulation (EC) 2725/2000.[127] The first aim of EURODAC is to help to apply the Dublin III Regulation[128], which lays down rules for determining which EU country is responsible for examining an asylum application.[129] Each EU country must take the fingerprints of all fingers of asylum applicants and those apprehended while trying to cross a border irregularly (e.g. non-EU/EEA nationals or stateless persons entering without valid documents) over the age of 14 and, within 72 hours, transmit the data to EURODAC. When an asylum-seeker or non-EU/EEA national has been found to be present illegally in an EU country, then that EU country can consult EURODAC to determine whether the individual has previously applied for asylum in an EU country or has previously been apprehended when trying to unlawfully enter the EU. Fingerprint data should be erased once asylum applicants, non-EU/EEA nationals or stateless persons obtain citizenship of an EU country.

Due to the large scale arrivals since the start of the migration and refugee crisis in 2015, some Member States became overwhelmed with fingerprinting all those arriving irregularly to the EU at the external borders, and who further transited through the EU *en route* to their preferred destination. As a consequence, thousands of migrants have remained invisible in Europe, a situation that facilitates unauthorised secondary and subsequent movements and irregular stay within the EU. As part of the first reform package of May 2016,

[127] Council Regulation (EC) 2725/2000 of 11 December 2000 concerning the establishment of "Eurodac" for the comparison of fingerprints for the effective application of the Dublin Convention.

[128] Regulation (EU) No 604/2013 (Dublin III Regulation), replacing Council Regulation (EC) No 343/2003 (Dublin II Regulation), lays down the criteria and mechanisms for determining which EU country is responsible for examining an asylum application.

[129] The second aim of EURODAC is to allow national police forces and Europol to compare fingerprints linked to criminal investigations with those contained in EURODAC. However, due to the fundamental right to privacy, law enforcement agencies are only allowed to use EURODAC for comparisons: (1) if there are reasonable grounds that doing so will substantially assist them in preventing, detecting or investigating a terrorist offence or other serious criminal offence; and (2) only as a last resort after several other checks have been carried out first.

the Commission presented a proposal to reinforce EURODAC[130] to make sure that it continues to provide the fingerprint comparison evidence it needs to function. The extension of the scope of EURODAC as proposed in the recast 2016 extends its scope for the purposes of identifying illegally staying third country nationals and those who have entered the European Union irregularly at the external borders, with a view to use this information to assist Member States to re-document a third country national for return purposes. This new purpose of EURODAC has been described in Article 1 (b) of the Recast proposal as follows: *"assist with the control of illegal immigration to and secondary movements within the Union and with the identification of illegally staying third-country nationals for determining the appropriate measures to be taken by Member States, including removal and repatriation of persons residing without authorisation".*

EURODAC is available at border crossing points, but unlike SIS, VIS and EES, it is not a border management system. For this reason, the EURODAC system will not be extensively analysed in this deliverable.

4.6 INTERPOL's Stolen and Lost Travel Documents (SLTD)

4.6.1 Purpose

INTERPOL's Stolen and Lost Travel Documents (SLTD) database is a central database on passports and other travel documents that have been reported stolen or lost by the issuing authorities to INTERPOL. SLTD enables INTERPOL National Central Bureaus (NCBs) and other authorized law enforcement entities – such as immigration and border control officers – to ascertain the validity of a travel document (passports, identity documents, visas).

SLTD includes information about stolen blank passports. Travel documents reported lost or stolen to the authorities of countries participating in SIS are entered both in SLTD and SIS. The SLTD also holds data on travel documents entered by countries not participating in SIS (Ireland, Croatia, Cyprus and third countries). Details of stolen and lost passports are submitted directly to the STLD database by INTERPOL NCBs and law enforcement agencies via INTERPOL's 24/7 secure global police communication system. Only the country which issued a document can add it to the database. Law enforcement officials at INTERPOL NCBs and other locations with access to INTERPOL's databases through the I-24/7 system – such as airports and border crossings – can query the passports of individuals travelling internationally against the SLTD, and immediately determine if the document has been reported as lost or stolen so they can take the necessary actions.

As stated in the Council Conclusions of 9 and 20 November 2015[131] and in Regulation (EU) 2017/458[132], the travel documents of all third-country nationals and persons enjoying the right of free movement should be verified against SLTD. All border control posts have to be connected to SLTD.

4.6.2 Legal constraints for PROTECT scenarios

In the context of the PROTECT project, the following aspects of the SLTD should be taken into account:

[130] Proposal for a Regulation of the European Parliament and of the Council on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of [Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person] , for identifying an illegally staying third-country national or stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes (recast), Brussels, 4.5.2016, COM(2016) 272 final 2016/0132 (COD).

[131] Conclusions of the Council of the EU and of the Member States meeting within the Council on Counter-Terrorism, 20 November 2015

[132] Regulation (EU) 2017/458 of the European Parliament and of the Council of 15 March 2017 amending Regulation (EU) 2016/399 as regards the reinforcement of checks against relevant databases at external borders.

1) It should be recalled that Regulation (EU) 2017/458 imposes the travel documents of both all third-country nationals and persons enjoying the right of free movement to be verified against SLTD on entry and exit of the Schengen Area.

2) To our knowledge, the SLTD database contains no biometric features.

4.7 Advance passenger information (API)

4.7.1 Purpose

Council Directive 2004/82/EC[133] regulates the transfer of advance passenger information (API) data by air carriers to the competent national authorities for the purpose of improving border controls and combating illegal immigration. This Directive was adopted following a request by the European Council of 25 and 26 March 2004, which met following the terrorist attacks in Madrid. The obligations provided for in this Directive are complementary to those laid down by Article 26 of the Convention implementing the Schengen Agreement, as supplemented by Council Directive 2001/51/EC, concerning the obligation of carriers to return third-country nationals who are refused entry by the Member State of destination.

According to this Directive, air carriers are required to communicate information concerning their passengers travelling to a European Union (EU) border crossing. This information is supplied, at the request of the authorities responsible for carrying out checks on persons at the external borders of the EU, to improve border control and to combat illegal immigration more effectively.

These data are forwarded to these authorities for passenger registration purposes. In principle they are transmitted electronically to these authorities.

Carriers are required to transmit the following information:

- the number and type of travel document used,
- nationality,
- full names,
- the date of birth,
- the border crossing point of entry into the territory of the Member States,
- code of transport,
- departure and arrival time of the transportation,
- total number of passengers carried on that transport,
- the initial point of embarkation.

In principle, these data are deleted by these authorities within 24 hours of transmission, provided that the passengers have arrived within the territory of the Member States. The personal data are deleted by the carrier within 24 hours of arrival of the means of transport.

No biometric data are collected or processed in the context of the API framework. However, it should be noted that Regulation (EU) 2017/458 (which will be discussed below in section 12) provides for the possibility to carry out checks in advance against SIS II and SLTD on the basis of passenger data received in accordance with Council Directive 2004/82/EC.

[133] Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data.

4.7.2 Legal constraints for PROTECT scenarios

In the context of the PROTECT project, the following aspects of API should be taken into account:

1) It should be reminded that API data is currently only regulated at European level in the context of air transport. This means that, currently, under EU law, API data could not be used in PROTECT's scenario related to land borders. However, as emphasized by a 2012 study[134], it has to be noted that the scope of implementation of API systems varies in the different Member States: all Member States collected API from air carriers, only three[135] also collect API from sea carriers. Some Member States[136] often collected API only from selected flights which had been assessed as 'at risk' of carrying irregular migrants and others implement API systems that collect API from all non-EU flights[137].

2) It should be recalled that no biometric features for ID verification are processed in the context of Council Directive 2004/82/EC.

3) An interesting novelty provided by Regulation (EU) 2017/458 is the fact that the new article 2e of the SBC specifies that checks against SIS and SLTD may be carried out in advance on the basis of API data received in accordance with Council Directive 2004/82/EC. Where those checks are carried out in advance on the basis of such data, the data received in advance shall be checked at the border crossing point against the data in the travel document.

4.8 The ETIAS proposal

4.8.1 Background

The European Commission's initiative of establishing a European Travel Information and Authorisation System (hereinafter referred to as 'ETIAS') dates back to a Communication of 2008 entitled "Preparing the next steps in border management in the European Union".[138] In the Communication "Stronger and Smarter Information Systems for Borders and Security" of 6 April 2016, the Commission announced that it will assess the necessity, technical feasibility and the proportionality of establishing a future European Travel Information and Authorisation System.[139] The same year, the Commission carried out a Feasibility Study, which used as a benchmark three other existing travel authorisation systems in the world: the ESTA in the USA, the eTA in Canada and the eVisitor in Australia.[140] Finally, on 16 November 2016, the Commission introduced a proposal to establish ETIAS to strengthen security checks on visa-free travellers (hereafter the

[134] Evaluation on the implementation and functioning of the obligation of carriers to communicate passenger data set up by Directive 2004/82, Final Report for Directorate-General for Home Affairs, available at http://ec.europa.eu/smart-regulation/evaluation/search/download.do?documentId=6412251

[135] DK, ES, UK

[136] AT, CH, CZ, DE, HU, IT, NL, LV – DK and MT also only collect API from selected flights, but it is not clear whether this is based on risk assessment or not.

[137] CY, EE, IE, RO, ES, UK

[138] Communication of 13 February 2008 from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "Preparing the next steps in border management in the European Union", COM(2008) 69 final.

[139] Communication of 6 April 2016 from the Commission to the European Parliament and the Council "Stronger and Smarter Information Systems for Borders and Security", COM(2016) 205 final.

[140] Feasibility Study of 16 November 2016 for a European Travel Information and Authorisation System (ETIAS) - Final Report available at: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/legislative-documents/docs/20161116/etias_feasability_study_en.pdf

ETIAS proposal). [141]On 6 March 2017, the EDPS issued its opinion.[142] In the European Parliament, the proposal has been assigned to the Civil Liberties, Justice and Home Affairs Committee (LIBE). The rapporteur Kinga Gál finalised her draft report on 8 June 2017. By the deadline of 11 July, almost 1 000 amendments were tabled to the draft report. On 19 October 2017, the LIBE committee adopted both draft reports, regarding ETIAS and amendments to the Europol Regulation (following a decision by the Council to split the proposal into two distinct legal acts), as well as a decision to enter into inter-institutional negotiations.[143] The Commission expects the development of ETIAS to start not long after the Entry/Exit System, in view of also having this new system in place in 2020.

4.8.2 Purpose

Currently, TCNVHs and TCNVEs travellers are subject to border controls when entering the Schengen area. According to the SBC, both categories of travellers need to comply with the conditions for short-term stay, which include not being a threat to public order and security, holding valid travel documents (including by checking SLTD), justifying the purpose and conditions of the intended stay, not being the subject of any alert in SIS for the purpose of refusing entry, and having sufficient means of subsistence. However, unlike the advance transfer of detailed information required for the visa application procedure of TCNVHs, no such advance information is required about TCNVEs arriving at the Schengen external borders. This means that border guards need to make a decision on allowing or refusing access to the Schengen area without prior knowledge regarding any security, migration or public-health risks associated with persons not requiring a visa. This is particularly true for TCNVHs travellers arriving by land, as the only source of information about them is their travel document presented at the external border. As regards passengers arriving by air (and in some Member States by sea), Council Directive 2004/82/EC obliges carriers to communicate all passenger data, known as 'advance passenger information' (API), ahead of inbound flights to the EU, including name, date of birth, passport number and nationality.

Hence, the aim of the ETIAS proposal of November 2016 is to verify if TCNVEs have a valid travel authorisation, prior to arriving in the Schengen area. A valid ETIAS travel authorisation, obtained in advance of arrival at a Schengen border crossing point, will be a precondition for entering the Schengen area. However, border guards at the external Schengen borders will still take the final decision to grant or refuse entry according to the Schengen Borders Code. The proposed ETIAS will be a largely automated system that will gather information on all visa-free travellers that intend to travel to the Schengen area. The proposed ETIAS will verify the information submitted via an online application ahead of their travel to the EU's external borders, to assess if they pose a risk for irregular migration, security or public health.

Applications will be automatically processed against other EU information systems (such as SIS, VIS, EES, SLTD and ECRIS), a dedicated ETIAS watch list (established by Europol) and targeted screening rules to determine if there are factual indications or reasonable grounds to issue or refuse a travel authorisation. In cases where no hits or elements requiring further analysis are identified, travel authorisations will be issued automatically within minutes after the application has been submitted.

[141] European Commission, Proposal for a Regulation of the European Parliament and the Council establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/794 and (EU) 2016/1624, COM(2016) 731.

[142] EDPS, Opinion 3/2017 EDPS Opinion on the Proposal for a European Travel Information and Authorisation System (ETIAS), 6 March 2017.

[143] This report is available at http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A8-2017-0322&language=EN

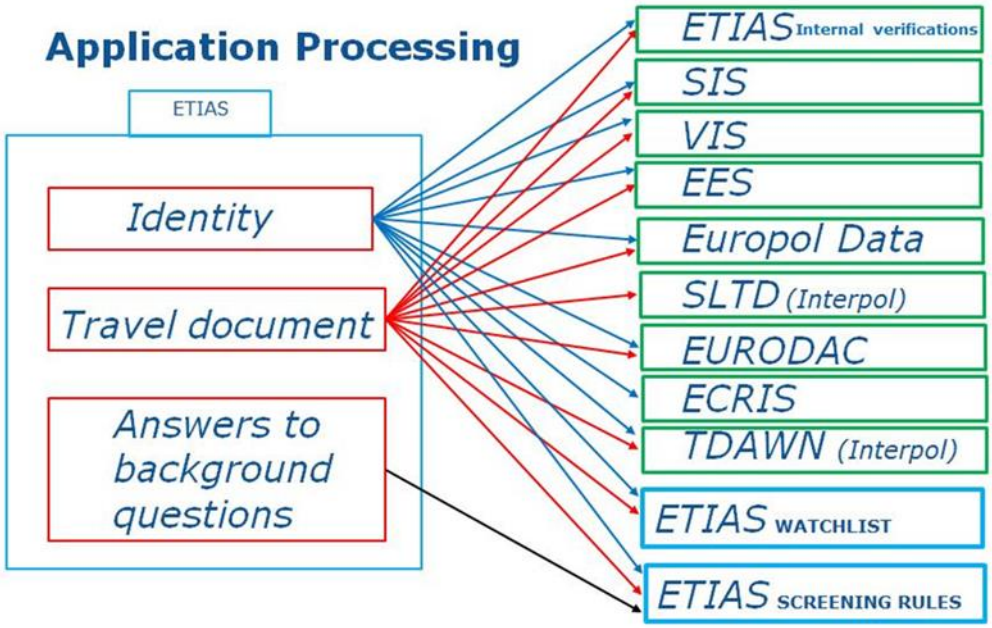

Figure 8 - ETIAS Automated Application Processing

The objective of this automated process is to ensure that:

- no other valid travel authorisation already exists, the data provided in the application concerning the travel document do not correspond to another application for travel authorisation associated with different identity data, and the applicant or the associated travel document do not correspond to a refused, revoked or annulled application for travel authorisation (ETIAS);
- the applicant is not subject to a refusal of entry alert (SIS) and/or the travel document used for the application does not correspond to a travel document reported lost, stolen or invalidated (SIS and Interpol's SLTD);
- whether the applicant is not subject to an alert on the basis of a European Arrest Warrant or wanted for arrest for extradition purposes (SIS)
- the applicant has not been reported as an overstayer, at present or in the past, or has was refused entry (EES);
- the applicant had no visa application refused in Visa Information System (VIS – this would be valid for nationals of countries which were granted visa waiver status within five years or less and for applicants having more than one nationality);
- the applicant and the data provided in the application corresponds to information recorded in the Europol data;
- a risk assessment is conducted for irregular migration risks, particularly as to whether the applicant was subject to a return decision or a removal order issued following the withdrawal or rejection of the application for international protection;
- no criminal record is recorded (ECRIS);
- the applicant and/or his/her travel document are not subject to an Interpol alert (TDAWN).

This automated process would also ensure that the applicant is not in the ETIAS watchlist and would verify if the applicant has replied affirmatively to any of the ETIAS background questions.

4.8.3 ETIAS Application and Issuance Process

The legislative proposal sets out in detail the practical steps and the process for issuing or refusing the travel authorisation. The figure below presents an overview of the process from the visa exempt third country national's perspective.

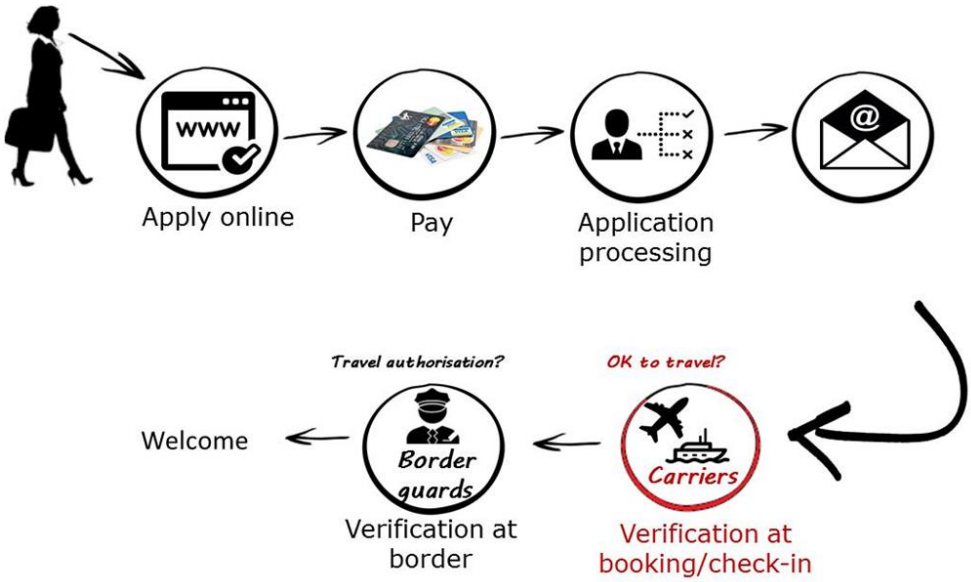

Figure 9 - Traveller's journey with ETIAS

Prior to the intended travel, the applicant completes an online application, via a dedicated website or the mobile application.

To fill in the application, each applicant will be requested to provide the following data:

- Surname (family name), first name(s), surname at birth, usual name(s); date of birth, place of birth, country of birth, sex, current nationality, first names of the parents of the applicant; home address;
- Travel document;
- If applicable, any other nationality;
- Permanent residence information;
- Email address and phone number;
- Member State of intended first entry;
- Education and current occupation details;
- Answers to a set of ETIAS background questions (as regards conditions with epidemic potential or other infectious or contagious parasitic diseases; criminal records; presence in war zones; and any previous decision to return to borders or orders to leave the territory of an EU Member State),
- If the applicant is a minor, the identity of the person responsible for the minor,
- If the application is submitted by a person different of the applicant, the identity of the person and company that he or she represents (if applicable).
- For family members to EU citizens/third country nationals benefitting from free movement without residence cards: their status as family member; the identity details of the family member with whom the applicant has ties; their family ties.

Filling the application form online would in principle not take more than 10 minutes. Apart from having a valid passport, no further documentation would be required to reply to the questions asked. ETIAS would accept applications introduced on behalf of the applicant in situations where visa exempt third country nationals cannot themselves create an application (for example, because of age, literacy- level, access to and inability to use information technology). In such cases, the application may be submitted by a third person provided this person's identity is included in the application.

The process of assessing and deciding on an application would start immediately after the payment of a fee is confirmed. The application would be automatically processed. Where applicable, the application would undergo manual processing by the ETIAS Central Unit and ETIAS National Unit(s). This automated step will process data related to identity data, travel document, and the answers to the background questions. The central system will, within minutes, proceed to a fully automated cross-checking of the information provided by the applicant against other information systems, a watchlist established in ETIAS and against ETIAS' defined screening rules.

4.8.4 Legal constraints for PROTECT scenarios

The ETIAS proposal does not foresee the processing of biometric data.

5 Interoperability based on fingerprints and facial image

5.1 Description

5.1.1 Background

In its Communication of 6 April 2016 *"Stronger and Smarter Information Systems for Borders and Security"*[144], the Commission emphasized the need to improve the interoperability of information systems. According to the EC, the existing information systems in the EU for border management cover a wide range of functionalities. Nevertheless, there are still shortcomings in the functionalities of existing systems and gaps in the EU's architecture of data management which have as consequence that border guards face a complex landscape of differently governed information systems at EU level.

For these reasons, the Commission set up a high-level expert group on information systems and interoperability ("HLEG"). The HLEG was tasked to address "the legal, technical and operational aspects of the different options to achieve the interoperability of the information systems, including the necessity, technical feasibility and proportionality of available options and their data protection implications". The HLEG presented recommendations on strengthening and developing the EU's information systems and interoperability first in its interim report of December 2016[145] , and later in its final report of May 2017[146].

In its seventh Progress report towards an effective and genuine security union[147], the Commission set out a new approach to the management of data for borders and security in line with the Communication of 2016

[144] Communication from the Commission to the European Parliament and the Council on Stronger and Smarter Information Systems for Borders and Security, 6.4.2017, COM (2016) 205 final.

[145] Interim report by the chair of the high-level expert group on information systems and interoperability set up by the European Commission, Interim report by the chair of the high-level expert group, December 2016, available at: http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3435

[146] Final report of the high-level expert group on information systems and interoperability set up by the European Commission, 11 May 2017; available at http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3435

[147] Communication of 16.05.2017 from the Commission to the European Parliament, the European Council and the Council, Seventh progress report towards an effective and genuine Security Union, COM(2017) 261 final.

and the recommendations of the HLEG. Under this approach, all centralised EU information systems for security, border and migration management should be interoperable so that:

- the systems can be searched simultaneously using a European search portal;
- the systems use one shared biometric matching service to enable searches across different information systems holding biometric data, possibly with hit/no-hit flags indicating the connection with related biometric data found in another system;
- the systems share a common identity repository with alphanumeric identity data to detect if a person is registered under multiple identities in different databases.

On 8 June 2017, the Council welcomed the Commission's view and the proposed way forward to achieve the interoperability of information systems by 2020. It invited the Commission to pursue the work on three dimensions of interoperability (i.e. the European search portal, the biometric matching service and a common identity repository).[148]

On 17 November 2017, the EDPS published a reflection paper on the interoperability of information systems in the area of Freedom, Security and Justice[149] to advise the EU institutions on the data protection implications of their policies in the field of information management for borders management.

Finally, on 12 December 2017, the EC published a proposal for a Regulation on establishing a framework for interoperability between EU information systems (hereafter interoperability proposal).[150] In order to achieve the objectives of this proposal, the EC considers that four interoperability components need to be established:

- European search portal — ESP
- Shared biometric matching service — shared BMS
- Common identity repository — CIR
- Multiple-identity detector — MID

The four components combined would lead to the following interoperability solution:

[148] Council conclusions on the way forward to improve information exchange and ensure the interoperability of EU information systems, 8 June 2017: http://data.consilium.europa.eu/doc/document/ST-10151-2017-INIT/en/pdf

[149] EDPS, Reflection paper on the interoperability of information systems in the area of Freedom, Security and Justice, 17 November 2017.

[150] Proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration), Brussels, 12.12.2017, COM(2017) 794 final.

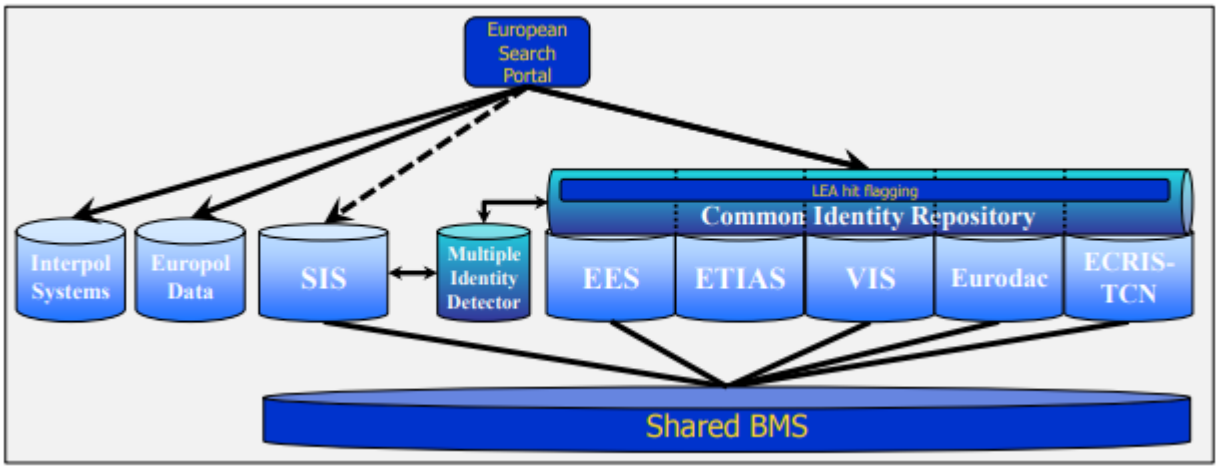

Figure 10 - EC's proposed interoperability solution

5.1.2 The shared biometric matching service (shared BMS)

The proposed shared biometric matching service (shared BMS) is of particular interest in the context of the PROTECT project. Indeed, the shared BMS would enable the querying and comparison of biometric data (fingerprints and facial images) from several central systems (in particular, SIS, VIS, EES and EURODAC)[151]. As neither the API framework nor the SLTD and the proposed ETIAS contain biometric data, these would therefore not be linked to the shared BMS.

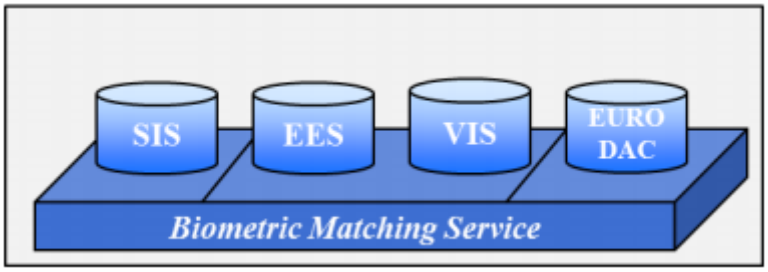

Figure 11 - EC's proposed shared BMS

The idea behind the EC's proposed shared BMS is that the legal instruments of SIS, VIS, EES and EURODAC do not prescribe the technical implementation details of the infrastructure that performs the fingerprint identification functions. Instead of a dedicated automated fingerprint identification system (AFIS) for each individual system, a shared biometric matching service could be implemented. Whereas the former is only capable of matching fingerprints, **the biometric matching service would be able to process both fingerprints and facial images**. And rather than serving just one system, the shared biometric matching service would perform identifications and verifications for all the centralised systems.

[151] As well as the proposed ECRIS-TCN system which is out of scope of this deliverable since its purpose is law enforcement and not border control management.

5.1.3 Legal constraints for PROTECT scenarios

The EC's proposed shared biometric matching service confirms the intention of the European Council of Thessaloniki to develop a coherent approach on biometric identifiers or biometric data for documents for third country nationals, European Union citizens' passports and information systems.[152]

Fingerprints and facial image are increasingly being promoted by the EU as the biometric features which should be used in both travel documents and in border control management databases to enhance the tasks of border guards. For this reason, the enrolment of additional biometric features (other than fingerprints or facial image) in travel documents for the purpose of "facilitating" border control processes as described in D3.1 should be considered as being in contradiction with the data minimization principle enshrined in article 5(c) of the GDPR which reads as follows "personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed".

Therefore, for the purposes of D3.1 scenarios, it is recommended to PROTECT technical partners to only focus on the development of "emerging" biometric features which could update current facial image standards, for example 2D face, iris, periocular and 3D face.

6 Conclusion

The aim of D2.2 is to explore the current and proposed European legal framework regulating both biometric border control and personal data protection in order to identify the legal constraints which should be taken into account by the scenarios being defined in D3.1. The main objective of the PROTECT project being to develop a contactless multimodal biometric solution for identity confirmation of travellers with the aim to facilitate and fasten their border crossings, this deliverable was dedicated to analyse the hereunder main legal questions:

1) Under current EU law, is there a possibility for electronic machine-readable documents to support an enhanced set of contactless biometrics? In other words, could emerging biometrics (other than facial image and fingerprints) be included in travel documents under current EU law?

   Answer: Under current EU Regulation, it is very unlikely that inclusion of additional multimodal biometrics features (being not facial image or fingerprints) developed within the PROTECT project could legally be integrated in ePassports (or residence permits) without a national legislation of a Member State allowing it. Furthermore, even if a national law would allow such integration of additional biometrics, it would certainly be challenged in Court for privacy reasons related to proportionality and data minimization.

2) Under current EU law, could a smartphone be considered as a travel document to support traditional biometrics (fingerprints and facial image) as well as an enhanced set of contactless biometrics?

   Answer: Under current EU law, it seems very doubtful that mobile devices such as smartphones could legally be used to replace travel documents as a result of strict rules regulating the materials of travel documents. In other words, smartphones cannot be considered as "travel documents" under current EU law and therefore cannot support traditional biometrics (fingerprints and facial image) as well as an enhanced set of contactless biometrics for the purpose of border control management.

3) Under current EU law, could consent of a traveller be the legal basis to enrol additional biometrics in a travel document for "government use of their personal data"?

[152] The Presidency conclusions of the Thessaloniki European Council of 19 and 20 June 2003 are available at http://data.consilium.europa.eu/doc/document/ST-11638-2003-INIT/en/pdf

Answer: Recital 43 of the GDPR expressly states that: *"in order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation".* This means that it seems that consent of travellers cannot be considered as a legitimate basis of lawfulness in PROTECT scenarios to allow public border control authorities to speed up their public interest missions by enrolling additional biometrics in travel documents.

4) Under current EU law, which constraints related to the entry/exit external border checks for both persons enjoying the EU right to free movement and TCNs should be taken into account by the PROTECT scenarios?

Answer: Both for persons enjoying the EU right to free movement and for TCNs, the travel document must be presented for verification at each entry/exit of the Schengen area. For this reason, it is very doubtful that the passport scenario at land border crossing points described in D3.1 which envisages to transmit passport data via a mobile application could be considered as legal under current EU border control regulation since that that travel documents must be presented at each entry/exit of the Schengen area.

5) Under current EU law, which constraints should be taken into account by the PROTECT scenarios when making use of technologies such as self-service systems, eGates and automated border control systems?

Answer: Both for persons enjoying the EU right to free movement and for TCNs, it seems very doubtful that automated border checks could be operated on the basis of "additional biometrics" (other than fingerprints or facial image). Indeed, for persons enjoying the EU right to free movement article 8(2) of the SBC explicitly states that "*where there are doubts as to the authenticity of the travel document or the identity of its holder, at least one of the biometric identifiers integrated into the passports and travel documents issued in accordance with Regulation (EC) No 2252/2004 shall be verified".* As for TCNs, According to article 8b of the SBC, one of the conditions for persons whose border crossing is subject to a registration in the EES to be permitted to use automated border control systems is that *"the travel document contains a facial image recorded in the electronic storage medium (chip) which can be technically accessed by the self-service system so as to verify the identity of the holder of the travel document, by comparing that facial image with his or her live facial image"*. For this reason, and according to the data minimization principle, it seems legally doubtful to use additional biometrics (other than facial image – and in certain cases fingerprints) for the aforementioned purpose.

6) Under current EU law, which checks against databases should be taken into account by the PROTECT scenarios and which legal constraints derive from these in relation to the development of a contactless solution?

Answer: Under current EU law, checks which should be taken into account at external border crossings are mainly the ones against the SIS, SLTD, VIS, EES, EURODAC (and the proposed ETIAS) databases as well as the API framework. An overview of the legal constraints related to this background is provided in Section 4 of this Deliverable. Currently, one of the main legal constraints to take into account when developing a "full" contactless solution is that the VIS is used to verify the identity of visa holders by comparing his/her fingerprints with the fingerprints stored in the VIS on request of the border guards. The fact that TCNVHs could be required to provide their fingerprint at the entry of the Schengen Area should be taken into account when developing a complete contactless biometric-based cross-border control solution. The use the facial image for biometric matching against the VIS has not yet been implemented. This issue could be resolved once the EES will become functional and that TCNVHs would be able to pre-enrol their facial image into that system.

7) Does the PROTECT scenarios fit in with the EU's own future border control plans, in particular the EC's proposal for a Regulation on establishing a framework for interoperability between EU information systems?

   Answer: The EC's proposed shared biometric matching service confirms the intention of the European Council of Thessaloniki to develop a coherent approach on biometric identifiers or biometric data for documents for third country nationals, European Union citizens' passports and information systems.[153] Fingerprints and facial image are increasingly being promoted by the EU as the biometric features which should be used in both travel documents and in border control management databases to enhance the tasks of border guards. For this reason, the enrolment of additional biometric features (other than fingerprints or facial image) in travel documents for the purpose of "facilitating" border control processes as described in D3.1 should be considered as being in contradiction with the data minimization principle enshrined in article 5(c) of the GDPR which reads as follows "personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed". Therefore, for the purposes of D3.1 scenarios, it is recommended to PROTECT technical partners to only focus on the development of "emerging" biometric features which could update current facial image standards, for example 2D face, iris, periocular and 3D face.

As a result of the answers to the aforementioned questions, the scenarios proposed by D3.1 should more than certainly be considered as beyond the scope of current legislation. One of the main reasons of this negative conclusion is that consent of travellers cannot be considered as a legitimate basis of lawfulness under the GDPR to allow public border control authorities to speed up their public interest missions by enrolling additional biometrics in travel documents (which currently may not be replaced by a smartphone app).

This being said, Deliverable "D2.3 - Privacy impact of next-generation biometric border" control will analyse if, as an alternative to D3.1 scenarios, emerging biometric modalities could be processed in a "passport companion" such as a smartphone for "comfort and convenience purposes" of travellers on basis of their consent. The idea would be to analyse − from a privacy and data protection point of view − the possibility and the conditions to enrol additional contactless biometrics in a smartphone app for travellers willing to join a "PROTECT programme" allowing them to be given priority in waiting areas for "traditional" security and border checks and/or allowing them to benefit of additional convenience services such as access to VIP parking zones or waiting lounges.

[153] The Presidency conclusions of the Thessaloniki European Council of 19 and 20 June 2003 are available at http://data.consilium.europa.eu/doc/document/ST-11638-2003-INIT/en/pdf

Pervasive and UseR Focused BiomeTrics BordEr ProjeCT

(PROTECT)

H2020 – 700259

Security Sensitivity Assessment

Publication number:	D2.2
Publication title:	Legal framework of biometric border control
Publication type:	Deliverable
Related WP number:	WP2
Which conference/journal, etc.	N/A
Dissemination level: (Confidentiality)	PU
Version reviewed:	V1.0
Date:	22/03/2018

Objective

This form is related to the Security Sensitivity Assessment procedure which will assure that no sensitive information will be included in the publications and deliverables of the PROTECT project.

Security sensitive information means here all information in whatever form or mode of transmission that is classified by Council Decision on the security rules for protecting EU classified information (2011/292/EU) and all relevant national laws and regulations. The information can be already classified, or such that it should be classified.

In practice the following criteria is used:

- Information is already classified
- Information may describe shortcomings of existing safety, security or operating systems
- Information is such, that it might be misused.
- Information that can cause harm to
    - European Union
    - a Member State
    - society
    - industry and companies
    - third country
    - citizen or an individual person of a country.

Document Information

Project Number	H2020 - 700259	**Acronym**	PROTECT
Full Title	Pervasive and UseR Focused BiomeTrics BordEr ProjeCT		
Project URL	http://www.projectprotect.eu/		
Document URL			
EU Project Officer	Agnieszka Marciniak		

Authors (names and affiliations)	Franck Dumortier (UNAMUR)

Assessment form for the main author

Please fill in the form below:

This is: *pre-assessment* ☐ *final assessment* X

***List the input material used in the publication/deliverable*:**

***List the results developed and presented in the publication/deliverable*:**

The draft publication

X is attached to this statement

☐ can be found in link:

This publication does not include any data or information that could be interpreted as security sensitive.

X True

☐ Not sure

If not sure, please specify what are the material / results that you are not sure if they are security sensitive? Why?

Date: 26/03/18

Signature of the Responsible Author:

Comments from the SAB member

X The publication can be published as it is.

Comments:

From the view of Security Sensitivity Assessment - OK.

X Before publication the following modifications are needed:

- please check the rapport on the view the replacement or missing letter.
-

Date	22.03.2018
Name: **On behalf of the Security Advisory Board (SAB)**	Phd. Leon Jodłowski
Signature of the member of the SAB