The Framework Programme for Research & Innovation
Innovation actions (IA)

Project Title:

SMart mobILity at the European land borders

SMILE

Grant Agreement No: 740931

[H2020-DS-2016-2017] SEC-14-BES-2016 Towards reducing the cost of technologies in land border security applications

Deliverable

D7.1. BCPs of the future Interoperability Requirements including Compliance to International Standards. First Version

Deliverable No.		**D7.1**	
Workpackage No.	**WP7**	Workpackage Title and task type	**SMILE Ecosystem , Technology, Test Implementation and Evaluation. Interoperability Issues on BCPs**
Task No.	**T7.1**	Task Title	**Interoperability Requirements for compliance to international standards**
Lead beneficiary		**CERTH**	
Dissemination level		**Public**	
Nature of Deliverable		**Report**	
Delivery date		**30 June 2019**	
Status		**DRAFT**	
File Name:		**[SMILE] D7.1_ v1.0.pdf**	
Project start date, duration		**01 June 2017, 36 Months**	

This project has received funding from the European Union's Horizon 2020 Research and innovation programme under Grant Agreement n°740931

Authors List

Leading Author (Editor)				
Name		*Initials*	*Beneficiary Name*	*Contact email*
Georgios Stavropoulos		GS	CERTH	_
Co-authors (in alphabetic order)				
#	*Name*	*Initials*	*Beneficiary Name*	*Contact email*
1	Kim Tsun Chiu	KTC	EGOVCD	
2	Jean-Loup Depinay	JLD	IDEMIA	
3	Anargyros Sideris	AS	FINT	
4	Vladuta Alexandru Valentin	VAV	SPP	
5	Manolis Vasileiadis	MV	CERTH	
6	Nikos Zotos	NZ	FINT	

Reviewers List[1]

List of Reviewers (in alphabetic order)				
#	*Name*	*Initials*	*Beneficiary Name*	*Contact email*
1	Iacob Cru-cianou	*IC*	*SIVECO*	
2	*Lenard Zsakai*	*LZ*	*HNP*	

[1] The minutes and the Action Items produced at each consortium meeting have been composed by the Coordinator of the Project and have been reviewed and accepted by all Consortium members before they were considered finalized.

Document history			
Version	Date	Status	Modifications made by
0.1	13/05/2019	Document creation	CERTH
0.2	24/05/2019	Sections 3 & 5	FINT, EGOVCD
0.3	29/05/2019	Section 2	SPP
0.4	30/05/2019	Section 4	CERTH
0.5	03/06/2019	Sections 1 & 6	CERTH
0.6	04/06/2019	Section 3	IDEMIA
0.7	07/06/2019	Internal Review	CERTH
0.8	10/06/2019	Post-Internal Review	CERTH
1.0	12/06/2019	Final Draft for submission	CERTH

List of definitions & abbreviations

Abbreviation	Definition
LAN	Local Area Network
WLAN	Wireless Local Area Network
MIMO	Multiple Input Multiple Output
USB	Universal Serial Bus
TCP/IP	Transmission Control Protocol/Internet Protocol
LPR	License Plate Recognition
ISDN	Integrated services digital network
AES	Advanced Encryption Standard
IPSec	Internet Protocol Security
VPN	Virtual Private Networks
HTTPS	Hypertext Transfer Protocol Secure
HTTP	Hypertext Transfer Protocol
UHD	Ultra High Definition
PC	Personal Computer
HTML	Hypertext Markup Language
RDBMS	Relational Database Management System
OLTP	Online Transaction Processing
DW	Data Warehousing
MSSQL	Microsoft Structured Query Language

IEEE	Institute of Electrical and Electronics Engineers
LAN	Local Area Networks
MAN	Metropolitan Area Networks
WAN	Wide Area Networks
EDR	Endpoint Detection and Response
CCTV	Closed-circuit television
DBMS	Database Management System
URL	Uniform Resource Locator
IPS	Intrusion Prevention Systems
IDS	Intrusion Detections Systems
NGFW	Next Generation Firewall
ANPR	Automatic number-plate recognition
SIP	Session Initiation Protocol
TETRA	Terrestrial Trunked Radio
M2M	Machine-to-Machine
LTE	Long-Term Evolution
HEVC	High Efficiency Video Coding
IETF	Internet Engineering Task Force
ONVIF	Open Network Video Interface Forum
PTZ	Pan–tilt–zoom
DBMS	Database Management System
URL	Uniform Resource Locator

Executive Summary

The current document provides an in-depth analysis of existing standards and technologies that are used in BCPs, defining the requirements of the SMILE system towards its seamless integration and cooperation with these established systems. In order to increase efficiency and flow at BCPs, SMILE complies with a series of industry standards and technologies, in the form of technical specifications, within the scope of biometric and auxiliary data capture for verification, communications security and data compatibility to current and future EU and National systems and databases. Moreover, in addition to fulfilling existing standards, SMILE also contributes to these standards, by following up any standardization activities and initiatives that address its technological domains.

The document is organized as follows: Section 1 discusses the purpose of the document. Section 2 presents the standards and technologies currently in use in BCPs, while Section 3 describes the corresponding standards employed in SMILE technologies. Section 4 introduces the interoperability requirements, Section 5 outlines SMILE's contribution to the standards, and finally, Section 6 concludes the document.

Table of Contents

List of definitions & abbreviations **3**
Executive Summary **5**
List of figures **7**
1. Introduction (CERTH) **8**
1.1 Scope of the deliverable 8
1.2 Deliverable Structure 8
2. Existing standards and technologies used in BCPs (SPP) **9**
3. Standards used by SMILE technologies (IDEMIA & FINT) **22**
3.1 Biometrics (IDEMIA) 22
3.2 Passport verification (IDEMIA) 23
3.3 Secure communications (FINT) 24
4. Interoperability requirements (CERTH) **27**
5. Contribution to standards (eGovCD) **28**
6. Conclusions (CERTH) **29**
References **30**

List of figures

Figure 1 Documents for electronic control 23
Figure 2 Communication channels in SMILE needing protection 25

1. Introduction

1.1 Scope of the deliverable

The purpose of T7.1 is the detailed analysis of standards and technologies currently used in BCPs, in order to define the requirements for the SMILE recognition/authentication platform. Hence, this document is aimed at describing in-depth these standards, outlining their adoption in SMILE within the scope of biometrics authentication, document verification and communications security. Additionally, the interoperability requirements are defined, based on the analysis of EU and National BCP systems and databases in deliverable D4.1 and user & system requirements in deliverables D2.2, D2.3. Finally, SMILE's contribution to existing standards is explored, by following up standardization activities and initiatives that fall within its technology domains.

1.2 Deliverable Structure

The rest of the document is structured as follows:

Section 2 presents all the standards and technologies that are currently used in the BCPs, which the SMILE system must be compliant with. The standards and technologies are grouped into four respective categories: communication, application, video and security.

Section 3 describes how SMILE complies with the standards used at BCPs, by introducing the standards that SMILE employs for biometrics collection and authentication, document verification and communication security.

Section 4 introduces the SMILE interoperability requirements. These requirements allow the SMILE system to efficiently exchange data with other information systems, including current and future EU and National systems and databases.

Section 5 analyses how SMILE will contribute to existing standards, in terms of securing template signatures in ISO/IEC 24745 for biometrics information, and following up standardization activities that address its technological domains, such as activities of the European Telecommunications Standards Institute (ETSI)

Section 6 provides the concluding remarks for the deliverable.

2. Existing standards and technologies used in BCPs

A **Standard** can be defined as a measure, norm or model that is used in comparative evaluations and is accepted by all entities as base of knowledge.

Crt. No.	Standard Name and Version	Standard Description	Type of equipment where standard is used (PC / Mobile Device / Server / Router etc.)	Estimated number of equipment that use the standard	Importance (Low/Medium/High)
Communication standards					
1.	802.11n [1]	Developed by the IEEE for wireless LAN (WLAN) technology. 802.11n builds upon previous 802.11 standards by adding multiple-input multiple-output (MIMO).	Router	2 per BCP	High (without connectivity the solution will not have any results)
			Laptop	3 - 5 per BCP	
2.	USB [2]	USB is an industry standard that establishes specifications for cables and connectors and protocols for connection, communication and power supply between computers, peripheral devices and other computers	Finger print scanners	2 - 3 per BCP	Medium
			Document readers	5 - 20 per BCP	
3.	TCP/IP [3]	TCP/IP or the Transmission Control Protocol/Internet Protocol, is a suite of commu-	Router	2 per BCP	High (without connectivity the solu-
			Laptop	3 - 5 per BCP	

		nication protocols used to interconnect network devices on the internet. TCP/IP can also be used as a communications protocol in a private network (an intranet or an extranet).	Router	2 per BCP	tion will not have any results)
			Switch	2 - 3 per BCP	
			Server	1 per BCP	
			LPR camera	1 for SMILE	
4.	ISDN [4]	Integrated services digital network is an international communications standard for sending voice, video, and data over digital telephone lines or normal telephone wires.	Router	1 - 5 per BPC	High (without connectivity the solution will not have any results)
5.	SIP [5]	The Session Initiation Protocol (SIP) is a signaling protocol used for initiating, maintaining, and terminating real-time sessions that include voice, video and messaging applications. Unlike the ISDN compatible the standard IP v4/ IPv6 standard network systems.	Phone / Voice communication	1 - 50 per BPC	High (without connectivity the solution will not have any results)
6.	TETRA / EDRA [6]	TETRA (Terrestrial Trunked Radio)	hand/mobil/fix/DWS	1 - 50 per BPC	High (without connectivity the solution will not have any results)

7.	LTE-450 [7]	High speed data transmission services on network for governmental and business clients and low speed data transmission services for M2M applications are available in Hungary.	hand terminal and modem	1 - 50 per BPC	High (without connectivity the solution will not have any results)
Security standards					
1.	AES [8]	AES is based on a design principle known as a substitution–permutation network, and is efficient in both software and hardware. It does not use a Feistel network. AES is a variant of Rijndael which has a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits.	Dedicated encryption devices	1 - 3 per BPC	High (without encryption the solution will not be able to store personal data)
2.	IPSec [9]	Internet Protocol Security (IPsec) is a secure network protocol suite that authenticates and encrypts the packets of data sent over an Internet Protocol network. It is used in virtual private networks (VPNs).	Router	1 per BPC	Medium (a solution can work standalone on a BPC without communicating with other sites)
			Mobile devices	1 - 2 per BCP	
3.	HTTPS [10]	Hypertext Transfer Protocol Secure (HTTPS) is an extension of the Hypertext Transfer Protocol (HTTP). It is used for secure communication over a computer network, and is widely used on the Internet.	Server	3 for all BCP's	High (Privacy and integrity of the exchanged data is very important)
			PC	5 - 20 per BCP	
			Laptop	3 - 5 per BCP	

4.	IPS / IDS / NGFW [11]	Intrusion Prevention Systems, Intrusion Detections Systems, Next Generation Firewall, with separated (min 5 local + 1 wan/other side) physical zone. Improved detection of encrypted applications and intrusion prevention service. Modern threats like web-based malware attacks, targeted attacks, application-layer attacks, and more have had a significantly negative effect on the threat landscape.	Firewall	1 per BC	High (a solution can work communicating beetwen inside local specialized zones, and with other sites)
Video standards					
1.	H.264 / MPEG-4 AVC [12]	H.264 or MPEG-4 Part 10, Advanced Video Coding (MPEG-4 AVC) is a block-oriented motion-compensation-based video compression standard. As of 2014, it is one of the most commonly used formats for the recording, compression, and distribution of video content. It supports resolutions up to 8192×4320, including 8K UHD.	Surveillance cameras	5 - 15 per BPC	Medium (a solution can work standalone on a BPC without communicating with other sites)

2.	H.265 [13]	H.265 / High Efficiency Video Coding (HEVC), MPEG-H Part 2, is a video compression standard. In comparison to H.264/MPEG-4 AVC, HEVC offers from 25% to 50% better data compression at the same level of video quality, and . And unlike the primarily 8-bit AVC, HEVC's higher fidelity Main10 profile has been incorporated into nearly all supporting hardware. HEVC is competing with the AV1 coding format for standardization by the video standard working group NetVC of the Internet Engineering Task Force (IETF).	Surveillance cameras, videostreaming, video analyse, centralized recording and video servicing	5 - 150 per BPC	High (solution can work on a BPC and communicating with other sites and central sites)
3.	ONVIF Profile S and G [14]	ONVIF (Open Network Video Interface Forum) is a global and open industry forum with the goal of facilitating the development and use of a global open standard for the interface of physical IP-based security products. ONVIF creates a standard for how IP products within video surveillance and other physical security areas can communicate with each other. Profile S Addresses common functionalities of IP video systems, such as video and audio streaming, PTZ controls, and re-	Surveillance cameras, videostreaming, video analyse, centralized recording and video servicing	5 - 150 per BPC	High (In Hungary solution can work on a BPC and communicating with other sites and central sites)

		lay activation. Profile G Addresses video storage, recording, search, and retrieval.			
Application standards					
1.	HTML5 [15]	HTML is the World Wide Web's core markup language. Originally, HTML was primarily designed as a language for semantically describing scientific documents. Its general design, however, has enabled it to be adapted, over the subsequent years, to describe a number of other types of documents and even applications.	Server	1 to 2 per end-user	High (a solution cannot work without an front-end solution)
2.	Oracle [16]	Oracle Database (commonly referred to as Oracle RDBMS or simply as Oracle) is a proprietary multi-model database management system produced and marketed by Oracle Corporation. It is a database commonly used for running online transaction processing (OLTP), data warehousing (DW) and mixed (OLTP & DW) database workloads.	Server	1 - 2 per end-user	High (a solution cannot work without an front-end solution)
3.	MSSQL [17]	Microsoft SQL Server is a relational database management system developed	Server	1 - 2 per end-user	High (a solution cannot work with-

		by Microsoft. As a database server, it is a software product with the primary function of storing and retrieving data as requested by other software applications—which may run either on the same computer or on another computer across a network (including the Internet). Microsoft markets at least a dozen different editions of Microsoft SQL Server, aimed at different audiences and for workloads ranging from small single-machine applications to large Internet-facing applications with many concurrent users.			out an front-end solution)
4.	.NET [18]	The .NET Standard is a formal specification of .NET APIs that are intended to be available on all .NET implementations. The motivation behind the .NET Standard is establishing greater uniformity in the .NET ecosystem. ECMA 335 continues to establish uniformity for .NET implementation behavior, but there's no similar spec for the .NET Base Class Libraries (BCL) for .NET library implementations.	Software	5 - 80 per BPC	High (a solution cannot work without an front-end solution)
5.	XML [19]	The Extensible Markup Language (XML) is a subset of SGML that is completely described in this document. Its goal is to enable generic SGML to be served, received,	Software	5 - 80 per BPC	High (a solution cannot work without an front-end solution)

		and processed on the Web in the way that is now possible with HTML. XML has been designed for ease of implementation and for interoperability with both SGML and HTML.			

Technology can be defined as an application of scientific knowledge for practical purposes.

Crt. No.	Technology Name and Version	Technology Description	Type of equipment where technology is used (PC/Mobile Device/Server/Router etc.)	Estimated number of equipment that use the technology	Importance (Low/Medium/High)
Communication technologies					
1.	Wi-fi [20]	Wi-Fi is a family of radio technologies that is commonly used for the wireless local area networking (WLAN) of devices which is based around the IEEE 802.11 family of standards.	Router	2 per BCP	High (without connectivity between devices, the solution will not work)
			Laptop	3 - 5 per BCP	
2.	10/100/1000 Ethernet [21]	Ethernet is a family of computer networking technologies commonly used in local area networks (LAN), metropolitan area networks (MAN) and wide area networks (WAN).	PC	5 - 20 per BCP	High (without connectivity between devices, the solution will not work)
			Laptop	3 - 5 per BCP	
			Router	2 per BCP	
			Switch	2 - 3 per BCP	
			Server	1 per BCP	
3.	4G [22]	4G is the fourth generation of broadband cellular network technology, succeeding 3G.	Mobile devices	1 - 2 per BCP	High (without connectivity between devices, the solution will not

					work)
4.	VPN [23]	A virtual private network (VPN) extends a private network across a public network, and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.	Router	1 per BPC	High (without connectivity between devices, the solution will not work)
			Mobile devices	1 - 2 per BCP	
5.	Microwave radio relay [24]	Microwave radio relay is a technology widely used for transmitting signals, such as long-distance telephone calls and television programs between two terrestrial points on a narrow beam of microwaves. In microwave radio relay, microwaves are transmitted on a line of sight path between relay stations using directional antennas, forming a fixed radio connection between the two points.	Radio equipment	1 - 3 per BCP	Low (if it is not the only communication technology available in the BCP)
Security technologies					

1.	EDR [25]	Endpoint Detection and Response (EDR) is a cybersecurity technology that addresses the need for continuous monitoring and response to advanced threats. It is a subset of endpoint security technology and a critical piece of an optimal security posture.	Server	1 per end user	High (security is very important for solutions to protect personal data)
Video technologies					
1.	LPR	License plate recognition is a technology that uses optical character recognition on images to read vehicle registration plates.	LPR IP camera	1 per BCP	High (License plate recognition very important functionality)
2.	ANPR [26]	Automatic number-plate recognition (ANPR; see also other names below) is a technology that uses optical character recognition on images to read vehicle registration plates to create vehicle location data. It can use existing closed-circuit television, road-rule enforcement cameras, or cameras specifically designed for the task. ANPR is used by police forces around the world for law enforcement purposes, including to check if a vehicle is registered or licensed. It is also used for electronic toll collection on pay-per-use roads and as a method of cataloguing the movements of traffic, for example by highways agencies. Automatic number-plate recognition can be used to store the images captured by the cameras as well as the text from the	ANPR cameras	1 per BCP lane	Medium

		license plate, with some configurable to store a photograph of the driver. Systems commonly use infrared lighting to allow the camera to take the picture at any time of day or night. ANPR technology must take into account plate variations from place to place. Concerns about these systems have centered on privacy fears of government tracking citizens' movements, misidentification, high error rates, and increased government spending. Critics have described it as a form of mass surveillance.			
3.	CCTV [27]	Video surveillance is the use of video cameras to transmit a signal to a specific place, on a limited set of monitors.	IP camera	5 - 20 per BCP	High
4.	Thermal imaging [28]	Cameras with thermal imaging capture images based solely on the heat radiating from people and objects, they're unaffected by darkness or poor visibility. So they're as accurate in pitch black, fog, and camouflage as they are on a bright sunny day.	Surveillance cameras	1 - 5 per BCP	Medium (detection in bad light conditions is a benefit that can help the final solution)
Application technologies					
1.	Database Management System [29]	The database management system (DBMS) is the software that interacts with end users, applications, and the database itself to capture and analyze the data. The DBMS software additionally encompasses the core facilities provided to administer the data-	Server	1 per end user	High

		base. The sum total of the database, the DBMS and the associated applications can be referred to as a "database system". Often the term "database" is also used to loosely refer to any of the DBMS, the database system or an application associated with the database.			
2.	Web Technology [30]	Is an information system where documents and other web resources are identified by Uniform Resource Locators (URLs), which may be interlinked by hypertext, and are accessible over the network.	Server and client	2 - 10 per end user	High

3. Standards used by SMILE technologies

3.1 Biometrics

ISO and IEC created in 2002 a common working group to handle the standardization process regarding biometrics requirements. This group includes in its scope: common file frameworks, biometric application programming interfaces, biometric data interchange formats, related biometric profiles, application of evaluation criteria to biometric technologies, methodologies for performance testing and reporting and cross jurisdictional and societal aspects. Some key technologies related to biometrics are excluded from this domain, in particular personal verification.

Working Group Reference	Scope
ISO/IEC JTC 1/SC 37/WG 3	Biometric data interchange formats
ISO/IEC JTC 1/SC 37/WG 2	Biometric technical interfaces
ISO/IEC JTC 1/SC 37/WG 5	Biometric testing and reporting
ISO/IEC JTC 1/SC 37/WG 6	Cross-Jurisdictional and Societal Aspects of Biometrics
ISO/IEC JTC 1/SC 37/WG 1	Harmonized biometric vocabulary
ISO/IEC JTC 1/SC 37/WG 4	Technical Implementation of Biometric Systems

The group delivered and published the first standards set between 2005 and 2007, and a second rollout since 2011 each time under the reference ISO/IEC 19794. Some new useful data items (e.g. elements linked to biometric sample quality) have been added. Important effort has also been put towards harmonizing header data structures. Moreover, XML encoding has been added in addition the binary encoding

The following standards are especially significant in the context of SMILE:

- ISO/IEC 19794-2, Information Technology – Biometric Data Interchange Format – Part 2: Finger Minutiae Data
- ISO/IEC 19794-4, Information Technology – Biometric Data Interchange Format – Part 4: Finger Image Data
- ISO/IEC 19794-5, Information Technology – Biometric Data Interchange Format – Part 5: Face Image Data
- ISO/IEC 19794-6, Information Technology – Biometric Data Interchange Format – Part 6: Iris Image Data
- ISO/IEC 7816-11:2004, Identification cards – Integrated circuit cards – Part 11: Personal verification through biometric methods

SMILE also complies with the quality standards of imprint (29794-4) and iris (29794-6).

At testing and reporting level, when requested, SMILE ensures that it will evaluate different algos according to the recommendations of the test standards (19795 for biometrics, 30107 for anti-fraud).

The standards below are also mentioned, however they are outside of the scope of SMILE as the Biometric templates are restricted for usage of the SMILE system through the security mechanism.:

- ISO/IEC 19785 Common Biometric Exchange Formats Framework (CBEFF)
- Biometric Application Programming Interface (BioAPI) series of standards ISO/IEC 19784
- biometric profile series of standards ISO/IEC 24713

3.2 Passport verification

According to FRONTEX, document authentication is the process by which an electronically machine readable travel document (eMRTD) (most of the time this document is an ePassport) presented by the border crosser is inspected in order to determine whether it is genuine and valid. It means that the document has a physical support and that a "smart engine" (e.g. Automatic Border Control Gate in some international airports) should be available in order to verify all the controls done by a human agent like optical document checks, accessing and reading ePassport data and verification of these data. Usually an automatic engine implies that this engine is specialized.

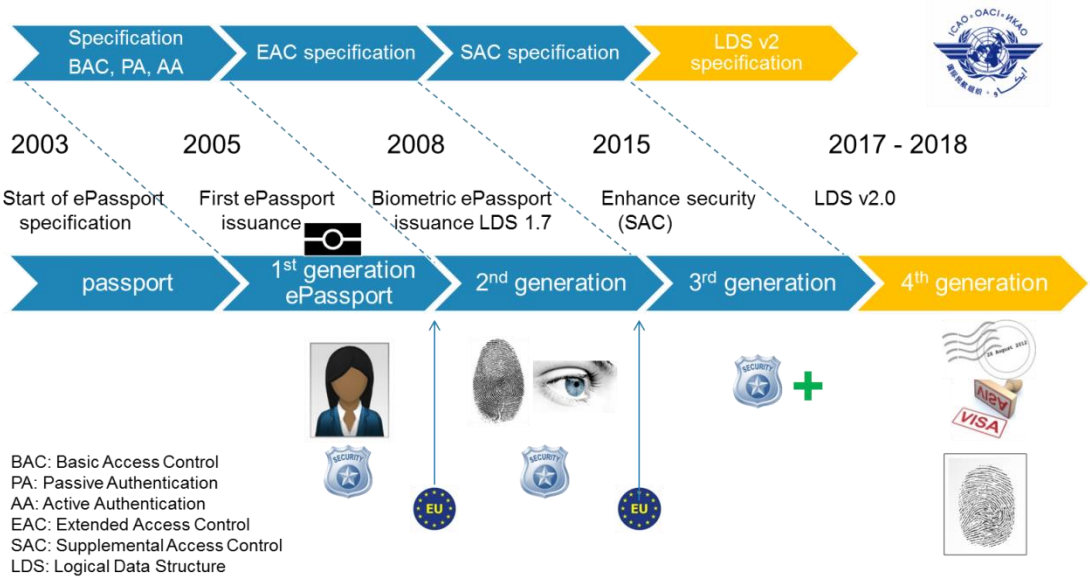

Figure 1 Documents for electronic control

1st Generation Basic Access Control

The Basic Access Control (BAC) protocol enables access to the data registered on the microchip through the numbering of the communications between that chip and the reader. The BAC protocol relies on an access key derived from the Machine Readable Zone (MRZ), which contains data that can be read on the passport itself or are partially known (i.e. date of birth).

2nd Generation Extended Access Control

This protocol complementary to BAC was suggested in 2006 regarding EU passports for Schengen area's member states, or "2nd Generation passports". The Extended Access Control (EAC) protocol relies on advanced cryptography and aims at restricting biometric data access, especially digital prints (viewed as more sensitive data by the EU). It still uses BAC for 'normal data' access.

3rd Generation Supplemental Access Control: Supplemental Access Control

The SAC protocol compared to BAC introduces new supplemental security features. This new mechanism brings superior security features when compared to BAC and guarantees a higher level of privacy for data confidentiality. The 3G ePassport implements:

- Advanced cryptography
  - AES 256b
  - Elliptic Curve Cryptography 521b
- ICAO Supplemental Access Control (SAC)
  - Protect your personal data with a PIN
- Extended Access Control v2.1

  - Secure the access to your biometric data through PKI
  - Terminal authentication before chip authentication to operate in un-trusted environments

The latest version of ICAO standards specifically focuses on the ability of the passport to store sensitive data and credentials. That's why it focuses on the Logical Data Structure and it is mainly known as LDS V2. New data areas in the document shall be updated for

- eVISA
  - Ease procedure for citizen : Apply over internet and store online or at the Embassy
  - Better security control (strong identity proof, prevent Visa thief)
  - Speed-up citizen cross border
- Electronic Entry Exit stamping
  - Faster border crossing
  - Historical travelling record for Visa appliance
- Additional benefits
  - For 3rd country using different biometrics (Iris vs Finger)
  - "Replace" existing biometry from LDS1 with an updated biometry in LDS2
- Enhance state security
  - Easier traveller profiling with electronic data background processing

Documents reference for ePassport and Secure eDocuments

- ICAO, Machine Readable Travel Documents - Part 1 & 3, ICAO Doc 9303
- Technical Guideline – BSI - TR03110 v2.10- Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC v2.10). NOTE: for 3G passport, only Part1&Part3 are relevant.
- Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC) Tests for Security Implementation – latest version (currently TR-03105 part 3.2 version 1.3)
- ICAO Technical Report - Supplemental Access Control (SAC) for Machine Readable Travel Documents –version 1.01 final2
- Advanced Security Mechanisms for Machine Readable Travel Documents - Supplemental Access Control (SAC) Test for Security Implementation
- ISO14443-2:2010, ISO14443-3:2011, and ISO14443:4:2008
- BSI-CC-PP-0056-V2-2012 - Protection Profile for Machine Readable Travel Document with "ICAO Application" Extended Access Control with PACE (EAC PP) – version 1.3.1, 22/03/2012)
- BSI-CC-PP-0055 (v1.10) - Protection Profile for Machine Readable Travel Document with ICAO Application", Basic Access Control.
- BSI-CC-PP-0068-V2-2011 - Protection Profile for Machine Readable Travel Document using standard inspection procedure with PACE (PACE PP) - SAC

3.3 Secure communications

As Figure 2 depicts, in SMILE there are five distinct types of communication channels that need to be protected, namely the channels between:

a) the SMILE cloud and the travellers
b) the SMILE cloud and the External databases/systems used in border checking (e.g. SIS II, VIS, etc)
c) the SMILE cloud and the SMILE GWs

d) the SMILE GW and the PUF
e) the SMILE GW and the SMILE verification tablets or other equipment (e.g laptops) that the BCP officers may use for accessing SMILE services via the SMILE GW.

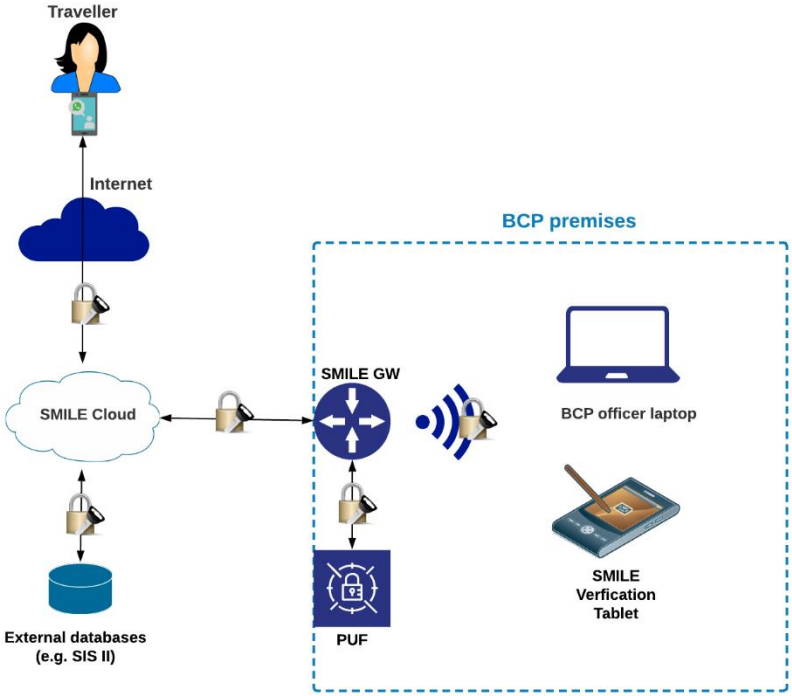

Figure 2 Communication channels in SMILE needing protection

For all the communication channels, except for the ones used for interacting with the external databases, we implement SSL/TLS [31] mechanisms. Specifically, for each end-point of the communication channel self-signed SSL certificates have been produced; for each certificate a pair of public/private keys has been derived. In this configuration, the self-signed certificates are used for authenticating the identity of the server to the clients. The respective private keys are kept at the server side whereas the public key is included in each SSL certificate and is used from the clients to perform the TLS handshake towards agreeing to a common cipher suite and deriving common session encryption keys (symmetric encryption) that will be used for encrypting the data transferred via the communication channel.

Furthermore, the wireless channel used to interconnect the verification tablets, BCP officer laptops, etc., with the SMILE GW provides an additional security layer by implementing WiFi Protected Access version 2 (WPA2) using AES-256 as the encryption algorithm. To ease deployability during the testing sessions (pilots included), we use pre-shared keys (PSK); however for deployments in real environments, if needed, the SMILE GW can be configured to support IEEE 802.1X-2010 [32] (and amendments e.g. 802.1AE™-2018 [33]) port-based access network control methods (e.g. utilising EAP TLS [34], etc).

Finally, for the communication channels with the external databases/systems, it is evident that the security mechanisms and protocols required by them need to be supported. However, in the project's context, these external DBs are emulated internally in the SMILE cloud (they have a local scope), so currently, we do not use encrypted communication channels.

It should be noted here, that in order to add an extra security layer, the data transmitted are also encrypted separately prior to transmission and/or storage; this is to be described in detail at D7.2. Additionally, we acknowledge that using self-signed certificates is not the indicated way to implement security in production environments, however they are used often

in the development and testing stages for speed purposes; in light of this, during the third year, we plan to use certificates either signed from a trusted root CA (Certification Authority) or signed from an internal CA that will be hosted in the SMILE cloud.

4. Interoperability requirements

Interoperability is defined as the ability of information systems to exchange data and enable sharing of information. The goal is to improve the efficiency and effectiveness of Europe-wide information-sharing tools, by ensuring the technical processes, standards and tools that allow EU information systems to work better together.

Towards this end, the following interoperability requirements are defined for the SMILE system:

1. SMILE must have interfaces to current EU systems and databases:
   - EURODAC
   - Schengen Information System - SIS (I, II)
   - Visa Information System – VIS
   - Europol Information System - EIS
   - European Criminal Records Information System – ECRIS
2. SMILE must have interfaces to under-development EU systems and databases:
   - Entry – Exit System -EES
   - European Travel Information and Authorisation System - ETIAS
   - Shared biometric matching service - S-BMS
3. SMILE must have interfaces to current National systems and databases used at the BCPs:
   - National Information System - NSIS (Romania)
   - National Schengen Information System – N.SIS II (Bulgaria)
   - National Visa Information System – NVIS (Bulgaria)
   - Robotszaru System (Hungary)
   - Border check and registration system - HERR (Hungary)
   - National Complex Document Registration System - NEKOR (Hungary)
4. SMILE must have interfaces with Interpol database:
   - Stolen and Lost Travel Document database - SLTD

The interface with each database must conform to the respective Interface Specification Standard. For each of the used databases, SMILE must implement the associated API end-points towards being able to access the stored information, make queries and get back results.

The databases and systems mentioned above are described in detail in deliverable D4.1 “Analysis of existing databases and Data Collection Study for SMILE use cases”

5. Contribution to standards

In addition to fulfilling existing standards, SMILE is looking forward to contributing to the standard. These are the measures that SMILE will consider:

1. SMILE will follow up activities in ongoing progress on securing template signatures in ISO/IEC 24745. ISO/IEC 24745 is standardized by International Organization for Standardization (ISO), with the latest version published in 2011. This standard provides guidance for how the biometric information should be protected under various requirements for confidentiality, integrity and renewability/ revocability during storage and transfer. In addition, the standard provides requirements and guidelines for the secure and privacy- compliant management and processing of biometric information.
2. SMILE will follow up any standardization activities and initiatives that address its technological domains, one of the examples is activities of European Telecommunications Standards Institute (ETSI) like seminars and plugtests. Similar to ISO, ETSI is a standardization organization focusing on European standard for ICT solution, including fields that relates to BCPs like cyber security, digital signature, security algorithms and smart cards.

6. Conclusions

This document presented the process followed by the SMILE project to identify and analyse the initial interoperability requirements that will ensure the system seamless integration and compliance to established International standards currently in use in BCPs. This process included the identification of such standards and technologies and the investigation on how they are applied in SMILE, within the scope of biometrics capture & authentication, document verification and communications security. Additionally, following the systems and databases analysis in D4.1, interoperability requirements were defined in order to allow the efficient exchange of information between SMILE and current and future EU and National systems.

This initial interoperability requirements analysis will also allow SMILE to contribute to standards that fall within its technical domain, with the final results presents in deliverable D7.7 in M36

References

[1] IEEE 802.11n-2009 - IEEE Standard for Information technology-- Local and metropolitan area networks-- Specific requirements-- Part 11, online: https://standards.ieee.org/standard/802_11n-2009.html

[2] USB - Universal Serial Bus, online: https://en.wikipedia.org/wiki/USB

[3] TCP/IP - Transmission Control Protocol/Internet Protocol, online: https://searchnetworking.techtarget.com/definition/TCP-IP

[4] ISDN - Integrated Services Digital Network, online: https://en.wikipedia.org/wiki/Integrated_Services_Digital_Network

[5] SIP - Session Initiation Protocol, online: https://en.wikipedia.org/wiki/Session_Initiation_Protocol

[6] TETRA - Terrestrial Trunked Radio, online: https://www.pro-m.hu/

[7] LTE-450 - Long Term Evolution, online: https://en.wikipedia.org/wiki/LTE_(telecommunication)

[8] AES - Advanced Encryption Standard, online: https://en.wikipedia.org/wiki/Advanced_Encryption_Standard

[9] IPSec - Internet Protocol Security, online: https://en.wikipedia.org/wiki/IPsec

[10] HTTPS - Hypertext Transfer Protocol Secure, online: https://en.wikipedia.org/wiki/HTTPS

[11] IPS/IDS/NGFW - Next-Generation Firewall, online: https://en.wikipedia.org/wiki/Next-generation_firewall

[12] H.264/MPEG-4 AVC - MPEG-4 Part 10, Advanced Video Coding, online: https://en.wikipedia.org/wiki/H.264/MPEG-4_AVC

[13] H.265 - High Efficiency Video Coding, online: https://en.wikipedia.org/wiki/High_Efficiency_Video_Coding

[14] ONVIF - Open Network Video Interface Forum, online: https://en.wikipedia.org/wiki/ONVIF

[15] HTML5 - HTML Living Standard, online: https://html.spec.whatwg.org/#is-this-html5?

[16] Oracle - Oracle Database, online: https://en.wikipedia.org/wiki/Oracle_Database

[17] MSSQL - Microsoft SQL Server, online: https://en.wikipedia.org/wiki/Microsoft_SQL_Server

[18] .NET - .NET Standard, online: https://docs.microsoft.com/en-us/dotnet/standard/net-standard

[19] XML - Extensible Markup Language (XML) 1.0 (Fifth Edition), online: https://www.w3.org/TR/2008/REC-xml-20081126/

[20] Wi-Fi, online: https://en.wikipedia.org/wiki/Wi-Fi

[21] Ethernet, online: https://en.wikipedia.org/wiki/Ethernet

[22] 4G - Fourth generation of broadband cellular network, online: https://en.wikipedia.org/wiki/4G

[23] VPN - Virtual Private Network, online: https://en.wikipedia.org/wiki/Virtual_private_network

[24] Microwave radio relay, online: https://en.wikipedia.org/wiki/Microwave_transmission

[25] EDR - Top 10 Endpoint Detection and Response (EDR) Solutions, online: https://www.esecurityplanet.com/products/top-endpoint-detection-response-solutions.html

[26] ANPR - Automatic Number Plate Recognition, online: https://en.wikipedia.org/wiki/Automatic_number-plate_recognition

[27] CCTV - Closed Circuit Television, online: https://en.wikipedia.org/wiki/Closed-circuit_television

[28] Thermal imaging - Picturing the invisible, online: https://www.axis.com/technologies/thermal-imaging
[29] Database Management System, online: https://en.wikipedia.org/wiki/Database
[30] WWW - World Wide Web, online: https://en.wikipedia.org/wiki/World_Wide_Web
[31] RFC5246, The Transport Layer Security (TLS) Protocol Version 1.2, online: https://tools.ietf.org/html/rfc5246
[32] IEEE 802.1X-2010 - IEEE Standard for Local and metropolitan area networks--Port-Based Network Access Control, online: https://standards.ieee.org/standard/802_1X-2010.html
[33] IEEE 802.1Xck-2018 - IEEE Standard for Local and metropolitan area networks - Port-Based Network Access Control Amendment 2: YANG Data Model, online: https://standards.ieee.org/standard/802_1Xck-2018.html
[34] RFC5216, EAP-TLS, online: https://tools.ietf.org/html/rfc5216