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

D5.1 – Analysis of technology enablers for the SMILE interoperability and communications framework

Deliverable No.		**D5.1**	
Workpackage No.	**WP5**	Workpackage Title and task type	**Interoperable communication fabric and uniform data exchanges**
Task No.	**T5.1**	Task Title	**Analysis of technology enablers for the SMILE interoperability and communications framework**
Lead beneficiary		**SIVECO**	
Dissemination level		**Public**	
Nature of Deliverable		**Report**	
Delivery date		**31/08/2018**	
Status		**Final**	
File Name:		**[SMILE] D5.1. Analysis of technology enablers for the SMILE interoperability and communications framework.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*
Iacob Crucianu		IC	SIVECO	
Co-authors (in alphabetic order)				
#	*Name*	*Initials*	*Beneficiary Name*	*Contact email*
1	Paul Montague	PM	eGovCD	
2	Kin Tsun Chiu	KTC	eGovCD	
3	Anargyros Sideris	AS	FINT	
4	Nikolaos Zotos	NZ	FINT	
5	Mihai Simionescu	MS	SPP	

Reviewers List

List of Reviewers (in alphabetic order)				
#	*Name*	*Initials*	*Beneficiary Name*	*Contact email*
1	Yannis Nikoloudakis	YN	TEIC	
2	Andrei Baltatu	AB	RBP	

Document history			
Version	Date	Status	Modifications made by
0.1	8/06/2018	Initial version. Table of content and structure	Diana Codi
0.2	15/06/2018	General aspects of interoperability	Iacob Crucianu
0.3	14/08/2018	Contributions of partners consolidated	Iacob Crucianu
0.4	17/08/2018	Ready for review	Iacob Crucianu
0.5	29/08/2018	Corrections after review	Iacob Crucianu
1.0	31/08/2018	Final Version after Quality Control	Georgios Stavropoulos

List of definitions & abbreviations

Abbreviation	Definition
6LoWPAN	IPv6 over Low Power Wireless Personal Area Networks
CoAP	Constrained Application Protocol
CIR	Common identity Repository
DDS	Data Distribution Service
DTLS	Datagram Transport Layer Security
EIF	European Interoperability Framework
ECRIS-TCN	European Criminal Record Information System for third-country nation (ECRIS-TCN system).
EES	Entry/Exit System
ESP	European Search Portal
ETIAS	European Travel Information and Authorization System
JSON	JavaScript Object Notation.
MID	multiple-identity detector
MQTT	MQ Telemetry Transport
SBMS	Shared biometric matching service
SIS	Schengen Information System
SOA	Service Oriented Architecture
SSL	Secure Sockets Layer
TLS	Transport Layer Security
VIS	Visa Information System
XMPP	Extensible Messaging and Presence Protocol
XML	Extensible Markup Language
MID	Multiple-Identity Detector

Executive Summary

The present document contains a description of how SMILE project is considering the interoperability between its own components and in relation to other projects or systems.

First, the general context of interoperability subject is considered, by referring to the **European Interoperability Framework (EIF).**

Then, a more specific context is considered, by presenting existing status of the technology regarding the communications of the centralized IT systems at **EU level on border and visa**

Furthermore, existing status of the technology regarding the communications of the centralized IT systems at EU level on border and visa is described.

The standards on which the development will be based on, are a distinct part of the current document. From the general aspects **of ISO/IEC 19794 and ISO/IEC 19784** to the more detailed **MQTT**, the current document is presenting the aspects to be considered by the next phases of SMILE.

Finally, the technical aspects of SMILE interoperability are considered. The technical aspects are grouped by technology enablers like Operating Systems, Programming Languages, data structures, Frameworks and libraries, Databases, Containers and processing systems.

The content of the present deliverable will be an important input for the other parts of WP5 (D5.2 SMILE Gateway, D5.3 SMILE Backend, D5.4 Smile Frontend, D5.5 SMILE services)

Table of Contents

1. Introduction

The aim of this task, as described in "Description of action part A", is to analyse novel technology enablers for integration and available standards that are ensuring the SMILE project communication means for achieving the uniform, versatile, scalable and robust operation of the proposed wide-area system. In order to define the appropriate integration and communication infrastructure we need to analyse if available standards or other information exchange technology enablers are suitable for the SMILE project

The result of this work comes after an extensive research for available technologies and standards necessary to implement a solution with the architecture described in the deliverable **D2.4 SMILE Conceptual Architecture, architectural elements description and technical specifications**

The presentation of technologies and standards will follow the main conceptual elements of the architecture.

In the document we'll just refer to technologies and standards we intend to use. Alternatives which are considered to be less appropriate for our solution will not be mentioned, even though they were studied, and compared with the proposed ones.

2. Interoperability and communication framework of the IT systems on border and visa

2.1 General aspects, definitions and advantages

For the purpose of the SMILE project, interoperability is the ability of SMILE system to interact towards mutually beneficial goals, involving the sharing of information and knowledge between different components of the system, and external systems, through the business processes they support, by means of the exchange of data between their ICT systems and SMILE.

2.2 Interoperability – a priority for the Commission and European Parliament

2.2.1 European Interoperability Framework (EIF) [1]

As stipulated in the Treaties of the European Union (EU), the EU's internal market guarantees four 'freedoms' - the **free movement of goods, capital, services and people** between the 28 Member States. These freedoms are assured by common policies supported by interconnected, interoperable networks and systems. People are free to work and relocate, and businesses are free to trade and operate in all EU Member States. In doing so, they inevitably have to electronically interact with Member State public administrations. To make these interactions efficient, effective, timely and of high quality, and to help cut red-tape and reduce the cost and effort involved, Member States are modernising their public administrations by introducing digital public services. However, in doing so, they risk creating isolated digital environments and consequently electronic barriers that may prevent public administrations from connecting with each other, and citizens and businesses from identifying and using available digital public services in countries other than their own. For this reason, efforts to digitise

the public sector should be well coordinated at European and national levels to avoid digital fragmentation of services and data and help the EU's digital single market to work smoothly.

2.2.2 Current context [2]

In recent decades, European public administrations have invested in ICT to modernise their internal operations, reduce costs and improve the services they offer to citizens and businesses. Despite the significant progress made and benefits already obtained, administrations still face considerable barriers towards exchanging information and collaborating electronically. These include legislative barriers, incompatible business processes and information models, and the diversity of technologies used. This is because, historically, information systems were set up in the public sector independently of each other and not in a coordinated way. The diversity of institutional configurations across Europe adds another layer of complexity at EU level. Interoperability is a prerequisite for enabling electronic communication and exchange of information between public administrations. This also makes it a prerequisite for achieving a digital single market. Interoperability programmes in the EU have evolved over time. At first, they were concerned with achieving interoperability in particular domains, then with putting in place common infrastructure. More recently, they have started to address interoperability at the semantic level. Governance, compatibility of legal regimes, alignment of business processes and secure access to data sources are some of the issues to be addressed next, to provide fully fledged public services. The EIF promotes electronic communication among European public administrations by providing a set of common models, principles and recommendations. It acknowledges and stresses the fact that interoperability is not only an ICT matter, as it has layers of implications ranging from the legal to the technical. Addressing issues in a holistic approach in all these layers and at different administrative levels from local to EU remains a challenge. The EIF identifies four layers of interoperability challenges (legal, organisational, semantic and technical) at the same time pointing out the essential role of governance to ensure coordination of relevant activities across all levels and sectors of administration.

2.2.3 Regulations and standards regarding information system for border management in operation across EU

At the current time there are several regulations in operation that establish the status of the various information systems that store and provide information for border management and security.

The information systems that are in use at the present time are the following:

- **Schengen Information System (SIS).** The SIS is used by twenty-six European countries to find information about individuals and entities for the purposes of national security, border control and law enforcement. Information in SIS is shared among the institutions of countries participating in the Schengen Agreement Application Convention (SAAC). The status and operational extend of the SIS system are regulated by the fallowing regulations:

- REGULATION (EC) No 562/2006 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 15 March 2006 establishing a Community Code on the rules governing the movement of persons across borders (Schengen Borders Code);
- REGULATION (EC) No 1931/2006 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 20 December 2006 laying down rules on local border traffic at the external land borders of the Member States and amending the provisions of the Schengen Convention.
- 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)
- 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)

- **Eurodac** was the first biometrically-enabled system commissioned by the European Union, and the first multinational biometric system in the world. The EU's asylum fingerprint database contains the fingerprints of all asylum applicants from each Member State, as well as fingerprints from persons apprehended in an irregular border crossing. Its primary role is to assist in determining the Member State responsible for examining an asylum application made in the EU and to thereby implement the "Dublin Regulation". The status and operational extend of the Eurodac system are regulated by the following regulation:
  - Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 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 the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice
- **Visa Information System.** 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. The system can perform biometric matching, primarily of fingerprints, for identification and verification purposes. The status and operational extend of the VIS system is regulated by the following regulations:
  - COUNCIL DECISION of 8 June 2004 establishing the Visa Information System (VIS);
  - Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and other serious criminal offences;

- 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);
- 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).

Some of the regulations establish the functionalities of future systems proposed in 2016-2017, which, at the present time, are under development, such as:

- **Entry/Exit System (EES).** The system that will be operational by 2020 and will be responsible for the recording and storage of the date, time and place of entry and exit of third-country nationals crossing the border of the Member States at which the EES operates, calculation of the duration and generation of alerts regarding the authorised stay time. A record of date, time and place of refusals of entry of third-country nationals and the authority of the Member state which refused the entry will be stored as well. The status and proposed operational extend of the EES system are regulated by the following regulation:
  - 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
- **European Travel Information and Authorization System (ETIAS).** The legal procedures to work with the ETIAS have started in 2016, and the system is expected to be in place by 2021. ETIAS will be mandatory for all countries who are Schengen visa-free and will keep track of visitors from countries who do not need a visa to enter the Schengen Zone. The ETIAS will undergo a detailed security check of each applicant to determine whether they can be allowed to enter any Schengen Zone country. The status and proposed operational extend of the EES system is regulated by the following regulation:
  - 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
- **European Criminal Record Information System for third-country nationals (ECRIS-TCN system).** Will augment the already existing European Criminal Records Information System (ECRIS) that was established in April 2012 in order to improve the exchange of information on criminal records throughout the EU. The improved decentralised system will enable authorities to identify EU countries' convictions of a non-EU national. In this way any EU country can then request this information through ECRIS. The status and proposed operational extend of the ECRIS-TCN system are regulated by the following regulation:
  - Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL establishing a centralised system for the identification of Member States holding conviction information on third country nationals and stateless

persons (TCN) to supplement and support the European Criminal Records Information System (ECRIS-TCN system) and amending Regulation (EU) No 1077/2011

Except this existing and proposed systems that have a major role in the preservation of border security for the EU member states, there are a series of adjacent databases that also contain vital information:

- National information systems and decentralized EU information systems;
- Interpol's Stolen and Lost Travel Documents (SLTD) database;
- Interpol's Travel Documents Associated with Notices (TDAWN) database.

The operational management of the existing systems is ensured by European Agency for the Operational Management of large-scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA). The eu-LISA agency that was founded in 2012 to ensure the uninterrupted operation of large-scale IT systems within the area of freedom, security and justice (AFSJ) is responsible for the operational management of IT-systems EURODAC, SIS II and VIS, while ensuring information security and data protection.[3] Thereby, it allows for immediate data exchange among member states. Furthermore, eu-Lisa evolves and develops new IT systems alongside building up a Centre of Excellence and conducting training, monitoring, and reporting. The agency describes itself as "one of the enablers of an integrated response to existing and emerging threats to European security". As such, it facilitates the practical implementation of political priorities and legal instruments. The status and proposed operational extend for eu-LISA is regulated by the following regulation:

- Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, and amending Regulation (EC) 1987/2006 and Council Decision 2007/533/JHA and repealing Regulation (EU) 1077/2011

2.2.4 Proposal regulation on establishing framework for interoperability between EU information systems (border and visa) from 12.12.2017

In the context of the already existing or under development information systems responsible for the augmentation of the border management procedures and for border protection, the necessity to increase the efficiency of these systems is constant.
Other innovative initiatives aim towards filling the gaps between these systems in order to create a truly interoperable infrastructure to better manage the Schengen borders and enhance EU internal security.
Following this idea, European Commission issued a proposal for a regulation that will set the ground rules for a unified infrastructure for border management.
The status and proposed operational extend of the framework is laid out in the following proposal:

- Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on establishing a framework for interoperability between EU information systems (borders and visa) and amending Council Decision 2004/512/EC, Regulation

(EC) No 767/2008, Council Decision 2008/633/JHA, Regulation (EU) 2016/399 and Regulation (EU) 2017/2226

According to the proposal the main objectives of the system are:

- **Fast, seamless**, systematic and controlled access to the desired information for law enforcement and immigration officers, border guards and other interested authorities;
- **Identity check of third-country nationals;**
- **Streamline access to lay enforcement authorities** to specific information for prevention, detection or prosecution and investigation of crimes and terrorism;

In order to achieve these objectives, the following components will be put in place:

- **A European Search Portal (ESP)** that will enable the simultaneous query of multiple systems using both biographical and biometric data. The databases that will queried, will be part of the following existing systems: Eurodac, VIS, SIS, Interpol and Europol, and of the under-development systems, eTIAS, EES and ECRIS-TCN; The stated role of the portal will be as one of a message brokers that will only retrieve the messages from the associated databases.
- **Shared biometric matching service (shared BMS)** will have the main role of detecting connections between data sets (fingerprints and facial images) and different identities assumed by the same person in different central systems.
- **Common identity repository (CIR)** will be the common storing environment for biographical and biometric identity data of third-country national. Except SIS data, that will not be contained in the common repository due to the complex technical architecture of the system, the rest of the existing and future systems will be covered by CIR.As a functional principle, the data will be stored in CIR, but would continue to belong to the native system that recorded them.
- **A multiple-identity detector (MID)** will crosscheck the data between systems. The target databases will be the ones covered by CIR or SIS)

3. Existing situation of the technology regarding the communications of the centralized IT systems at EU level on border and visa

This section will cover the following aspects regarding the communication infrastructure:

- Description of the communication channels used to exchange information between the existing systems at border control points (technologies used, hardware and software infrastructure, communication standards/protocols, availability and redundancy of the network, response-time, other relevant aspects regarding the communication channels)
- Communication channels used at the border control points for local devices to transmit or exchange data with the system. (Cameras, scanners, tablets, biometric terminals, other mobile devices)
- Other suitable standards regarding communication infrastructure that were taken into account for existing projects or future expansion projects of the communication platform at the border control point. With strong emphasis on the communication for biometric check point.

- Other available communication technologies suited for SMILE solution.
- Description of the condition/regulations/standards that regulate operation, integration and availability.

The aim of this chapter is to provide a comprehensible study regarding the existing and novel technologies that could be used as a communication platform for the SMILE project.

The interconnection of the Border Crossing Points with the available IT applications is realised through private communication channels. Depending on the available infrastructure, the Border Crossing Points are connected via radio channels (radio relay, WiMAX) standard IEEE 802.16.

In the Border Crossing Points there are computer networks consisting of hardware equipment and IT applications that connect the workstations from which the IT applications are accessed. The interconnection is realised using active network equipment. The connection between the workstations and the technical room, from where the access to the radio networks is ensured, is made by UTP / STP or fibre optic cable.

The connection between the Border Crossing Points technical rooms and the existing communication node at the county level is created using the private infrastructure (communication through radio relay, WiMAX).

In the Border Crossing Points, optical document readers that are connected via USB to the workstations are used, as well as cameras that can be connected via UTP/STP cable or Coaxial Cable.

EMYNOS project, which was targeting at emergency communications, proposed using satellite communication channels to conduct emergency communications and release public warnings. Satellite communications are costly and slow compared to other means like ethernet and WLAN, nevertheless, they remain a suitable solution as backup or failover channels.

Wi-Fi (IEEE 802.11) is a set of networks layer 1 and 2 specifications for creating wireless local area network (WLAN). Due to its popularity, most of the smartphones and tablets that were selling within 5- 10 years support Wi-Fi. Wi-Fi can be used for biometric-enabled tablets and other sensors with higher bandwidth requirements (Up to 600 Mbit/s for 802.11n) to communicate with the SMILE gateway.

Zigbee, based on IEEE 802.15.4, is a communication protocol to create wireless personal area networks (WPANs). This is often used with IoT devices as it targets low-power and low-bandwidth (Up to 250 Kbit/s) usage. In SMILE, Zigbee can be used for biometric sensors with lower bandwidth requirements to transmit data to centralized receivers or sending data between sensors in a mesh network.

Currently, two types of automated biometric identifications are in use in European airports:

1. Fingerprint recognition
2. Face recognition

Both work by using specific passages, with either:

- The first door opens upon passport-verification and the second one upon verification that the right individual has entered the passage: either by showing the right face to the camera, or by putting the right fingerprint on the fingerprint scanner.
- The first door opens upon detection of an entering individual, and then a biometric scan is performed while the person approaches the second door, then the traveller's passport is checked for authenticity, and crosschecked with the saved biometrics.

Some border polices created their own Automatic Border Control (ABC) systems, including:

- The Italian eGates at Naples, Rome Fiumicino, Rome Ciampino, Bologna, Venice, Milan, Treviso airports
- The Hungarian Budapest Airport ABC
- The Luxembourg airport ABC gates
- The French PARAFE ABC system, found in Paris CDG, Paris ORY
- The Czech Republic, with their Easy Go ABC system
- The German EasyPass ABC solution, deployed in the:
  - Germany: Hamburg, Berlin-Schönefeld, Berlin-Tegel, Düsseldorf, Cologne, Frankfurt, Munich airports
  - Norway: Oslo airport

Other border polices also use systems conceived by specialized private companies and their solutions, as:

- The Lisbon-based Vision Box, and their ABC solution, found in Copenhagen Dublin airport

Therefore, passport readers, fingerprint scanners, cameras, computers to store, send, receive and process information, and a wired internet connection are used to accomplish this process.

4. Available SOA technologies and standards regarding communication infrastructure

This section will describe the fallowing aspects regarding the communication infrastructure:

- Description of the existing SOA communication technologies and standards. General study regarding the current state of technology.
- Suitable standards regarding communication infrastructure that were taken into account for research projects or future expansion projects for the communication infrastructure in general.
- SOA Communication channels for biometric check point.
- Other available communication technologies suited for SMILE solution.

The aim of this chapter is to provide a comprehensible study regarding the SOA technologies that could be used (even if theoretical) as a communication platform for the SMILE project

4.1 eIDAS [3]

To be able to provide identification verifications throughout the EU, the European commission implemented a global system called the eIDAS-network.

This system operates using the electronic identifications (eID) of the European citizen, stored in a network of nodes, called eIDAS-Nodes. Each country should have one of these nodes, and have the responsibility to implement it, and to support the connection of national Identity Providers and Attribute Providers to the eIDAS-Node, thus making their national eID schemes accessible to cross-border online services.

eIDAS-Nodes are composed of two main parts:

- A Proxy-Service
- A Connector

It may also contain member state specific middleware services.

The role of the proxy service is to provide an interface to access a citizen's National eID information, in correlation with the national eID databases. It is the main interface between the connectors of other eIDAS nodes, and the eID information of a member citizen.

The role of the connector is to connect from one eIDAS-Node to the proxy of another one.

According to the eIDAS interoperability architecture, communication between eIDAS-Nodes is performed using the Security Assertion Markup Language (SAML) for-mat. All request messages must be signed, and the eIDAS Crypto must be enforced. The usage of eIDAS crypto and Transport Layer Security (TLS) is checked on each request.

4.2 MQTT

MQTT (MQ Telemetry Transport) [4] [4] s a simple and lightweight messaging protocol which follows the publish/subscribe paradigm and is designed for devices operating in low-bandwidth, high-latency or unreliable networks. As far as security is concerned, MQTT relies on external protocols such as SSL and/or to the applications' data encryption capabilities (if any). An extension of this protocol, named MQTT-SN (MQTT for Sensor Networks), is optimized for being utilized in wireless sensor networks (WSN) where there are enough constraints in terms of power, storage and processing.

4.3 CoAP

Constrained Application Protocol (CoAP) [5] is a UDP based messaging protocol suited for environments where wireless sensor nodes are deployed. The protocol is well suited for Machine-to-Machine (M2M) applications and supports a number of features including a web protocol, asynchronous messages exchange, URI and content type support, simple proxy/caching capabilities, stateless HTTP mapping and security

bindings to the Datagram Transport Layer security (DTLS). Regarding the latter, CoAP supports four different modes, namely the no-security (NoSec), pre-shared key (PresharedKey), asymmetric key (RawPublicKey) and X.509 certificate (Certificate).

4.4 DDS

Data Distribution Service (DDS) [6] is a middleware protocol and API standard for data-centric connectivity (from the Object Management Group®) which uses a publish/sub-scribe model towards enabling consumers (e.g. IoT devices, services) to subscribe to topics of interest. DDS supports anonymized and automated communications, since no relationship between endpoints is required. Additionally, the protocol inherently supports Quality of Service (QoS) mechanisms, including reliability, system health (liveliness), and security which are built into the protocol. Regarding the latter, DDS controls access, enforces data flow paths, and encrypts data on-the-fly.

4.5 XMPP

Extensible Messaging and Presence Protocol (XMPP) [7] [8]is an XML-based set of open technologies suited for communication services, such as instant messaging, pres-ence, multi-party chat and voice/video calls. XMPP supports the transmission of XML messages over TCP transport, allowing IoT developers to implement service discovery and service advertisements. XMPP-IoT is a tailored version of XMPP focusing in the IoT environments. XMPP follows a decentralized architecture and as far as security is con-cerned, the protocol has SASL and TLS built to its core. The XMPP developer commu-nity is actively working on end-to-end encryption towards further enhancing the secu-rity level.

4.6 6LoWPAN

IPv6 over Low Power Wireless Personal Area Networks (6LoWPAN) [9]enables for the use of IPv6 within network-constrained environments. 6LoWPan supports wireless In-ternet connectivity at low data rates to accommodate highly constrained devices (e.g. IoT sensors). 6LoWPAN builds upon the 802.15.4 -Low Rate Wireless Personal Area Networks (LRWPAN) specification **Error! Reference source not found.**, towards creating an IPV6 adaptation layer. The adaptation layer provides several features that include IPv6 with UDP header compression, support for fragmentation, and security. Regarding the latter, 6LoWPAN, designers can take advantage of link encryption offered within IEEE 802.15.4 but can also apply transport layer encryption such as DTLS.

4.7 SOAP

SOAP (originally Simple Object Access Protocol) [10]is a messaging protocol specifica-tion for exchanging structured information in the implementation of web ser-vices in computer networks. Its purpose is to induce extensibility, neutrality and inde-pendence. It uses XML Information Set for its message format, and relies on applica-tion layer protocols, most often Hypertext Transfer Protocol (HTTP) or Simple Mail Transfer Protocol (SMTP), for message negotiation and transmission.

SOAP allows processes running on disparate operating systems (such as Windows and Linux) to communicate using Extensible Markup Language (XML). Since Web protocols like HTTP are installed and running on all operating systems, SOAP allows clients to invoke web services and receive responses independent of programming languages and platforms.

4.8 RESTful web services

RESTful web services are built to work best on the Web. Representational State Transfer (REST) is an architectural style that specifies constraints, such as the uniform interface, that if applied to a web service induce desirable properties, such as performance, scalability, and modifiability, that allow services to work best on the Web. In the REST architectural style, data and functionality are considered resources and are accessed using Uniform Resource Identifiers (URIs), typically links on the Web. The resources are acted upon by using a set of simple, well-defined operations. The REST architectural style constrains an architecture to a client/server architecture and is designed to use a stateless communication protocol, typically HTTP. In the REST architecture style, clients and servers exchange representations of resources by using a standardized interface and protocol.

4.9 gRPC

gRPC [11] is the TLS-compatible server application technology Google has been using for the past years for most of their software components.

Being an alternative technology to REST, gRPC uses HTTP/2.0, which supports multiplexing of requests, to allow faster communication between asynchronous controllers. It uses protocol buffers (protobuf) for binary serialization of the messages, and allows dual-sided streaming of the data, whilst needing a server only to run the lightweight application without having another webhosting server behind.

The protobuf format used by gRPC before serialization allows a strongly typed format for the building of the application server component, with most of the code being generated automatically according to the "*.proto" file in which the input/ output of each API route is declared.

This route declaration format allows full transparency between members of different teams working on the same project, without taking too much effort to adapt to it.

With the stated advantages, gRPC can considerably improve computation time and message transfer time. When combined with Docker containers, gRPC can provide lightweight and easily scalable services, that can have a great impact on cost reductions over a large deployment.

4.10 BioAPI

BioAPI (Biometric Application Programming Interface) [12] [12]is a key part of the International Standards that support systems that perform biometric enrolment and verification (or identification). It defines interfaces between modules that enable soft-

ware from multiple vendors to be integrated together to provide a biometrics application within a system, or between one or more systems using a defined Biometric Interworking Protocol (BIP) – see below.

ISO/IEC 19784, the BioAPI specification, provides a high-level generic biometric authentication model suited for most forms of biometric technology. No explicit support for multimodal biometrics is currently provided. An architectural model is described which enables components of a biometric system to be provided by different vendors, and to interwork through fully-defined Application Programming Interfaces (APIs). A key feature of the architecture is the BioAPI Framework, which supports calls by one or more application components (provided by different vendors, and potentially running concurrently) using the BioAPI API specification. The BioAPI Framework provides this support by invoking (through a Service Provider Interface, SPI) one or more biometric service provider (BSP) components (provided by different vendors, and potentially running concurrently) which can be dynamically loaded and invoked as required by an application component. At the lowest level there is hardware or software that performs biometric functions such as capture, matching, or archiving. These parts of the architecture are called BioAPI Units and can be integral to a BSP or can be supplied as part of a separate BioAPI Function Provider (BFP) component. Interactions (through the BioAPI Framework) can occur between BSPs from different vendors provided data structures used to record information from the BioAPI Units they access conform to other International Standards, and in particular to ISO/IEC 19794

4.11 ISO/IEC 19794

ISO/IEC 19794-1:2011 [13]describes the general aspects and requirements for defining biometric data interchange formats. The notation and transfer formats provide platform independence and separation of transfer syntax from content definition. ISO/IEC 19794-1:2011 defines what is commonly applied for biometric data formats, i.e. the standardization of the common content, meaning, and representation of biometric data formats of biometric types considered in the specific parts of ISO/IEC 19794.

ISO/IEC 19794 is defining several components, from which we are using:

BS ISO/IEC 19794-1:2006: Information technology. Biometric data interchange formats. Framework

BS ISO/IEC 19794-2:2005: Information technology. Biometric data interchange formats. Finger minutiae data

BS ISO/IEC 19794-3:2005: Information technology. Biometric data interchange formats. Finger pattern spectral data

BS ISO/IEC 19794-4:2005: Information technology. Biometric data interchange formats. Finger image data

BS ISO/IEC 19794-5:2005+A2:2009: Information technology. Biometric data interchange formats. Face image data

BS ISO/IEC 19794-6:2005: Information technology. Biometric data interchange formats. Iris image data

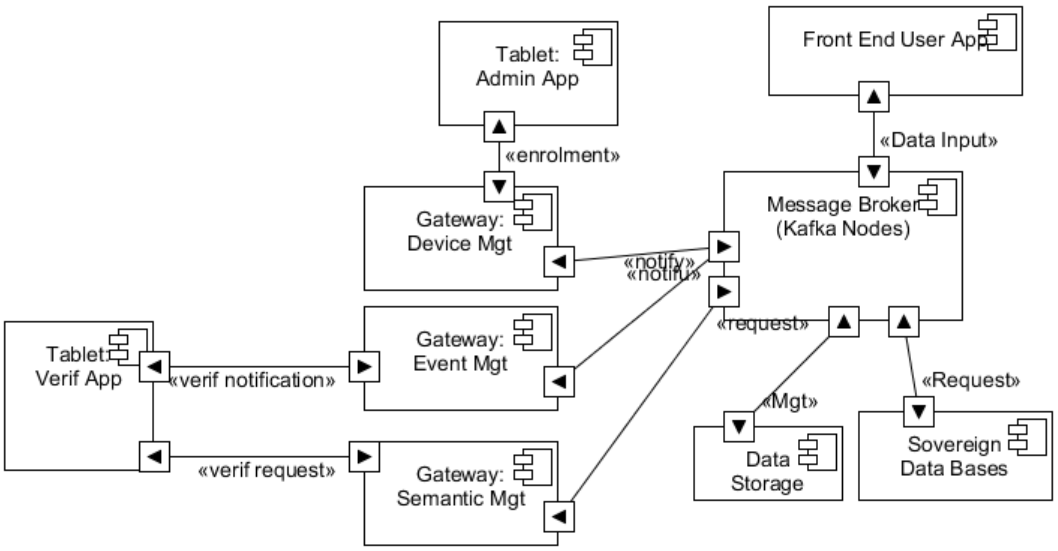
5. Perspectives on the use of SOA communication infrastructure for SMILE

This section will present the following aspects regarding the communication infrastructure perspective use for SMILE project.

- Perspectives upon the use of the existing SOA communication technologies and standards for SMILE project.
- Description of the SOA communication channels used to exchange information between systems similar with the ones used for border management and security (See the documentation provided in section 2.2.2 of the present document). Relevant existing test cases regarding SoA communication architecture.

The aim of this document is to select relevant SOA communication infrastructure that best serves the needs of the SMILE project.

The SoA communication infrastructure will be applied on a logical architecture like that presented in D2.4 and included bellow:



5.1 Operating Systems

5.1.1 Microsoft Windows

Microsoft Windows [14] is a group of several graphical operating system families, all of which are developed, marketed, and sold by Microsoft. Each family caters to a certain sector of the computing industry. Active Windows families include Windows NT and Windows Embedded; these may encompass subfamilies, e.g. Windows Embedded Compact (Windows CE) or Windows Server. The most recent version of Windows for PCs, tablets, smartphones and embedded devices is Windows 10

5.1.2 Ubuntu

Ubuntu [15]is a free and open source operating system and Linux distribution based on Debian. Ubuntu is offered in three official editions: Ubuntu Desktop for personal

computers, Ubuntu Server for servers and the cloud, and Ubuntu Core for Internet of things devices. New releases of Ubuntu occur every six months, while long-term support (LTS) releases occur every two years. The most recent version is Ubuntu 18.04 (LTS)

5.1.3 Android

Android [16]is a mobile operating system developed by Google, based on a modified version of the Linux kernel and other open source software and designed primarily for touchscreen mobile devices such as smartphones and tablets. In addition, Google has further developed Android TV for televisions, Android Auto for cars, and Wear OS for wrist watches, each with a specialized user interface. Variants of Android are also used on game consoles, digital cameras, PCs and other electronics. The operating system has since gone through multiple major releases, with the current version being 8.1 "Oreo", released in December 2017. The core Android source code is known as Android Open Source Project (AOSP) and is primarily licensed under the Apache License.

5.1.4 iOS

iOS [17]is a mobile operating system created and developed by Apple Inc. exclusively for its hardware. It is the operating system that presently powers many of the company's mobile devices, including the iPhone, iPad, and iPod Touch. The iOS user interface is based upon direct manipulation, using multi-touch gestures. Major versions of iOS are released annually. The current version, iOS 11, was released on September 19, 2017 and is available for all iOS devices with 64-bit processors.

5.2 Programming Languages

5.2.1 C

C [18]is a general-purpose, imperative computer programming language, supporting structured programming, lexical variable scope and recursion, while a static type system prevents many unintended operations. By design, C provides constructs that map efficiently to typical machine instructions, and therefore it has found lasting use in applications that had formerly been coded in assembly language, including operating systems, as well as various application software for computers ranging from supercomputers to embedded systems. C was originally developed by Dennis Ritchie between 1969 and 1973 at Bell Labs and used to re-implement the Unix operating system. It has since become one of the most widely used programming languages of all time, with C compilers from various vendors available for the majority of existing computer architectures and operating systems. C has been standardized by the American National Standards Institute (ANSI) since 1989 (ANSI C) and subsequently by the International Organization for Standardization (ISO).

5.2.2 C++

C++ [19]is a general-purpose programming language. It has imperative, object-oriented and generic programming features, while also providing facilities for low-level memory manipulation. It was designed with a bias toward system programming and embedded, resource-constrained and large systems, with performance, efficiency and flexibility of use as its design highlights. C++ has also been found useful in many other contexts, with key strengths being software infrastructure and resource-constrained applications, including desktop applications, servers (e.g. e-commerce, Web search or SQL servers), and performance-critical applications (e.g. telephone switches or space probes). C++ is a compiled language, with implementations of it available on many platforms. Many vendors provide C++ compilers, including the Free Software Foundation, Microsoft, Intel, and IBM.

C++ is standardized by the International Organization for Standardization (ISO), with the latest standard version ratified and published by ISO in December 2017 as ISO/IEC 14882:2017 (informally known as C++17).

5.2.3 Python

Python [20]is an interpreted high-level programming language for general-purpose programming. Created by Guido van Rossum and first released in 1991, Python has a design philosophy that emphasizes code readability, notably using significant whitespace. It provides constructs that enable clear programming on both small and large scales. Python features a dynamic type system and automatic memory management. It supports multiple programming paradigms, including object-oriented, imperative, functional and procedural, and has a large and comprehensive standard library. Python interpreters are available for many operating systems. CPython, the reference implementation of Python, is open source software and has a community-based development model, as do nearly all of Python's other implementations. Python and CPython are managed by the non-profit Python Software Foundation.

5.2.4 Java

Java [21]is a general-purpose computer-programming language that is concurrent, class-based, object-oriented, and specifically designed to have as few implementation dependencies as possible. It is intended to let application developers "write once, run anywhere" (WORA), meaning that compiled Java code can run on all platforms that support Java without the need for recompilation. Java applications are typically compiled to bytecode that can run on any Java virtual machine (JVM) regardless of computer architecture. As of 2016, Java is one of the most popular programming languages in use particularly for client-server web applications, with a reported 9 million developers. The language derives much of its syntax from C and C++, but it has fewer low-level facilities than either of them. The latest version is Java 10, released on March 20, 2018

5.3 Data storage format

Data exchanged between different components of the system will be packaged in formats widely recognized by all platforms and systems considered in our architecture.

The exchange of data will be message-based, and messages will contain data in XML or JSON format.

5.3.1 XML

- XML [22]stands for eXtensible Markup Language
- XML is a markup language much like HTML
- XML was designed to store and transport data
- XML was designed to be self-descriptive
- XML is a W3C Recommendation

5.3.2 JSON

- JSON [23]stands for JavaScript Object Notation
- JSON is a lightweight data-interchange format
- JSON is "self-describing" and easy to understand
- JSON is language independent *

5.4 Frameworks & Libraries

5.4.1 Chainer

Chainer [24]is a powerful, flexible Python-based deep learning framework allowing for the fast implementation, training and evaluation of deep learning models. It is actively used for most of the current approaches for neural networks (CNN, RNN, RL, etc.), aggressively adding new approaches as they’re developed, and providing support for many kinds of hardware as well as parallelization for multiple GPUs. Chainer follows the Define-by-Run paradigm, meaning that the neural networks definitions are defined on-the-fly at run time, allowing for dynamic network changes.

5.4.2 TensorFlow Lite

TensorFlow Lite [25]is the lightweight version of the TensorFlow open source high performance numerical computation library, suitable for mobile and embedded devices. It enables on-device machine learning inference with low latency and a small binary size using various such as optimizing the kernels for mobile apps, pre-fused activations, and quantized kernels that allow smaller and faster (fixed-point math) models. It provides a C++ and Java API, and also supports hardware supports hardware acceleration with the Android Neural Networks API.

5.4.3 Android Neural Networks API

The Android Neural Networks API [26](NNAPI) is an Android C API designed for running computationally intensive operations for machine learning on mobile devices. NNAPI is designed to provide a base layer of functionality for higher-level machine learning frameworks (such as TensorFlow Lite, Caffe2, or others) that build and train neural networks. The API is available on all devices running Android 8.1 (API level 27) or higher. NNAPI supports inferencing by applying data from Android devices to previously trained, developer-defined models. Examples of inferencing include classifying images, predicting user behaviour, and selecting appropriate responses to a search query.

5.4.4 Android Native Development Kit

The Native Development Kit [27](NDK) is a set of tools that allows the use of C and C++ code with Android and provides platform libraries that can be used to manage native activities and access physical device components, such as sensors and touch input. The NDK can be useful for cases in which it is necessary to squeeze extra performance out of a device to achieve low latency or run computationally intensive applications or when trying to reuse custom C or C++ libraries. Using Android Studio 2.2 and higher, the NDK can be used to compile C and C++ code into a native library and package it into an APK using Gradle, the IDE's integrated build system. The Java code can then call functions in the native library through the Java Native Interface (JNI) framework

5.4.5 OpenCV

OpenCV [28](Open Source Computer Vision Library) is an open source computer vision and machine learning software library. OpenCV was built to provide a common infrastructure for computer vision applications and to accelerate the use of machine perception in the commercial products. Being a BSD-licensed product, OpenCV makes it easy for businesses to utilize and modify the code. The library has more than 2500 optimized algorithms, which includes a comprehensive set of both classic and state-of-the-art computer vision and machine learning algorithms.

5.5 RDBMS

RDBMS are used to store information which is well structured. The speed and the ACID principle makes them necessary to store data processed in transactions.

We consider two RDBMS as candidates for SMILE: MySQL and Postgresql. Our choice considered that they are open source, and they are proven in critical large-scale systems.

5.5.1 MySQL

MySQL [29]is the world's most popular open source database. Whether you are a small, fast growing company, a technology ISV or large enterprise, MySQL can cost-

effectively help you deliver high performance, scalable database applications with advanced features like the following:

1. Data Security
2. On-Demand Scalability
3. High Performance
4. Round-the-clock Uptime
5. Comprehensive Transactional Support
6. Complete Workflow Control
7. Reduced Total Cost of Ownership
8. The Flexibility of Open Source

Las version available is :8.0

5.5.2 Postgresql

PostgreSQL [30]is a powerful, open source object-relational database system that uses and extends the SQL language combined with many features that safely store and scale the most complicated data workloads. The origins of PostgreSQL date back to 1986 as part of the POSTGRES project at the University of California at Berkeley and has more than 30 years of active development on the core platform.

PostgreSQL has earned a strong reputation for its proven architecture, reliability, data integrity, robust feature set, extensibility, and the dedication of the open source community behind the software to consistently deliver performant and innovative solutions. PostgreSQL runs on all major operating systems, has been ACID-compliant since 2001, and has powerful add-ons such as the popular PostGIS geospatial database extender. It is no surprise that PostgreSQL has become the open source relational database of choice for many people and organisations.

Last version available is:10.5

5.6 NoSQL

We consider the usage of NoSQL databases for unstructured data, as usually biometric data is. Also, the speed for storing and retrieving data, and the horizontal scalability makes them a good candidate for SMILE project. Our choice is for Cassandra

5.6.1 Cassandra [31]

As already mentioned, different alternatives for implementing the data storage cluster have been evaluated.

Firstly, we evaluated the use of the Apache Hadoop project's file system, HDFS (Hadoop Distributed File System) and the use of Apache Spark for the work, which has demonstrated its superiority over classic alternatives such as the use of MapReduce, however, in the evaluation of the noSQL database to be used, Cassandra was chosen for different reasons.

Cassandra is one of the most used noSQL databases and stands out from the others in several aspects, as they are:

- Easily configurable.
- Easy to maintain compared to other systems.
- Automatically replicated.
- Flexible requirements in the definition of data columns.
- Scale massively better than other systems.
- Written in Java and with drivers to use it from many languages, including Java which is the language we mainly use in our platform.
- Native Hadoop support including platforms such as Hive, Pig and others, giving us flexibility to extend usage or add features in the future.

It also has some negative aspects with respect to other noSQL systems, such as a worse handling of transactional operations, but given the use to be made of the data, the remarkable aspects were more important.

In conclusion, Cassandra is the right choice, depending on the type of data and information that is stored when scalability (linear), fault tolerance and high availability are required without compromising performance. Last version is v3.11.

5.7 Stream Processing

5.7.1 Kafka

Apache Kafka® [32]is a distributed streaming platform. Kafka can be seen as a three in one system – Messaging system, Stream storage system and Stream processing system. A streaming platform has three key capabilities:

- Publish and subscribe to streams of records, similar to a message queue or enterprise messaging system.
- Store streams of records in a fault-tolerant durable way.
- Process streams of records as they occur.

Kafka is generally used for two broad classes of applications:

- Building real-time streaming data pipelines that reliably get data between systems or applications
- Building real-time streaming applications that transform or react to the streams of data

Kafka concepts:

- Kafka is run as a cluster on one or more servers that can span multiple datacentres.
- The Kafka cluster stores streams of records in categories called topics.
- Each record consists of a key, a value, and a timestamp.

Kafka has four core APIs:

- The Producer API allows an application to publish a stream of records to one or more Kafka topics.
- The Consumer API allows an application to subscribe to one or more topics and process the stream of records produced to them.
- The Streams API allows an application to act as a stream processor, consuming an input stream from one or more topics and producing an output stream to one or more output topics, effectively transforming the input streams to output streams.

- The Connector API allows building and running reusable producers or consumers that connect Kafka topics to existing applications or data systems. For example, a connector to a relational database might capture every change to a table.

In Kafka, the communication between the clients and the servers is done with a simple, high-performance, language agnostic TCP protocol. This protocol is versioned and maintains backwards compatibility. We provide a Java client for Kafka, but clients are available in many languages. Latest version available is 2.0.

5.7.2 Zookeper

ZooKeeper [33]is a centralized service for maintaining configuration information, naming, providing distributed synchronization, and providing group services. All of these kinds of services are used in some form or another by distributed applications. Latest version available is 3.4.13

5.8 Containers

Container engines [34], often referred to as operating-system-level virtualization, are operating systems in which the kernel allows the existence of multiple isolated instances. Each instance is referred as a container, virtualization engine. Developers use them to create secure, virtual hosting environments with isolated resources. Developers can also separate applications, programs, or segments of code for increased security. These tools reduce overhead for companies and simplify migration processes. Containers can also be used to store applications in a securely hosted environment to increase space, efficiency, and organization. Software solutions such as container management software, container orchestration software, container networking software, container monitoring software, and service discovery software are combined to create a microservice ecosystem.

5.8.1 Docker

Docker [35]unlocks the potential of an organization by giving developers and IT the freedom to build, manage and secure business-critical applications without the fear of technology or infrastructure lock-in.

By combining its industry-leading container engine technology, an enterprise-grade container platform and world-class services, Docker enables you to bring traditional and cloud native applications built on Windows, Linux and mainframe into an automated and secure supply chain, advancing dev to ops collaboration and reducing time to value.

5.9 Biometric Databases

The following face databases are used for training the face recognition and analysis models within the scope of the SMILE project:

DATABASE	SUBJECTS	FILES	ANNOTATIONS

CelebFaces Attributes [36]	10177	202599	gender, glasses, facial hair, hair, hat
color FERET [37]	1199	14126	id, gender, age, ethnicity
IMDB-WIKI [38]	20284	523000	id, age, gender
LFW Soft Biometrics [39]	5749	13233	id, age, gender, ethnicity, glasses, facial hair
OUI-Adience Face Image Project [40] [40]	2284	26580	id, age, gender

6. Conclusion

The study we have conducted reveals a wide range technology enabler for the SMILE interoperability and communications framework.

Current advances in technologies offer solutions for the whole area where the SMILE system will operate.

Modern operating systems, good storage systems like RDBMS or NoSQL systems, stream processing, distributed computing, biometric data processing, security mechanism, mobile devices or customs designed systems are available and will be part of SMILE architecture.

All the systems and components identified as SMILE components candidates are implementing well known and industry proven protocols.

Based on the analysis of technology enablers, considerate can be considered that there is a sound technological base for SMILE interoperability and communication framework.

7. Bibliography

[1] "EIF," [Online]. Available: https://ec.europa.eu/isa2/eif_en.

[2] "EIF brochure," [Online]. Available: https://ec.europa.eu/isa2/sites/isa/files/eif_brochure_final.pdf.

[3] "eIDAS Regulation (Regulation (EU) N°910/2014)".

[4] OASIS, "MQTT Version 3.1.1," October 2014. [Online]. Available: http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/os/mqtt-v3.1.1-os.doc.

[5] IETF, "RFC7252, The Constrained Application Protocol (CoAP)," June 2014. [Online]. Available: https://tools.ietf.org/html/rfc7252.

[6] OMG, "Data Distribution Service Specification Version 1.4," March 2015. [Online]. Available: https://www.omg.org/spec/DDS/1.4/.

[7] IETF, "RFC3920, Extensible Messaging and Presence Protocol (XMPP)-Core," October 2004. [Online]. Available: https://tools.ietf.org/html/rfc3920.

[8] IETF, "RFC3921, Extensible Messaging and Presence Protocol (XMPP): Instant Messaging and Presence," October 2004. [Online]. Available: https://tools.ietf.org/html/rfc3921.

[9] IETF, "IPv6 over Low power WPAN (6lowpan)," [Online]. Available: https://datatracker.ietf.org/wg/6lowpan/documents/.

[10] W3C, "SOAP W3C Recommendation (Second Edition)," April 2007. [Online]. Available: https://www.w3.org/TR/soap/.

[11] "gRPC Protocol," [Online]. Available: https://grpc.io/.

[12] "Biometric application programming interface -- Part 1," ISO, 2018. [Online]. Available: https://www.iso.org/standard/70866.html.

[13] "Biometric API," 2011. [Online]. Available: https://www.iso.org/standard/50862.html.

[14] "Windows 10 (version 1803)," Microsoft, July 2018. [Online]. Available: https://www.microsoft.com/en-us/windows.

[15] "Ubuntu 18.04 LTS, Canonical Ltd.," July 2018. [Online]. Available: https://www.ubuntu.com/.

[16] "Android 8.1," Google, December 2017. [Online]. Available: https://www.android.com/.

[17] "iOS11," Apple Inc, September 2017. [Online]. Available: https://www.apple.com/lae/ios/ios-11/.

[18] "C11 Standard," C11, ISO/IEC 9899:2018, June 2018. [Online]. Available: https://www.iso.org/standard/74528.html.

[19] "C++17, ISO/IEC 14882:2017," ISO, December 2017. [Online]. Available: https://www.iso.org/standard/68564.html.

[20] "Python 3.7.0," Python Software Foundation, June 2018. [Online]. Available: https://www.python.org/.

[21] "Java SE Development Kit 10.0.2," Oracle Corporation, Juky 2018. [Online]. Available: http://www.oracle.com/technetwork/java/index.html.

[22] “XML description,” w3schools, [Online]. Available: https://www.w3schools.com/xml/xml_whatis.asp.

[23] “JSON description,” w3schools, [Online]. Available: https://www.w3schools.com/js/js_json_intro.asp.

[24] “Chainer v4.3.1,” Preferred Networks, July 2018. [Online]. Available: https://chainer.org/.

[25] “TensorFlow Lite r1.10,” TensorFlow, July 2018. [Online]. Available: https://www.tensorflow.org/mobile/tflite/.

[26] “Android Neural Networks API NDK r17b,” Google, April 2018. [Online]. Available: https://developer.android.com/ndk/guides/neuralnetworks/ https://developer.android.com/ndk/.

[27] “Android Native Development Kit (NDK) r17b,” Google, July 2018. [Online]. Available: https://developer.android.com/ndk/.

[28] “OpenCV 3.4.2,” Intel Corporation, July 2018. [Online]. Available: https://opencv.org/.

[29] “MySQL,” Oracle, July 2018. [Online]. Available: https://www.mysql.com/products/.

[30] “PostgreSQL,” [Online]. Available: https://www.postgresql.org/about/.

[31] “Apache Cassandra,” Apache Software Foundation, July 2018. [Online]. Available: http://cassandra.apache.org/.

[32] “Apache Kafka,” Apache, [Online]. Available: https://kafka.apache.org/intro.

[33] “Apache Zookeper,” [Online]. Available: https://zookeeper.apache.org/.

[34] “Container engines description,” [Online]. Available: https://www.g2crowd.com/categories/container-engine.

[35] “Docker container description,” Docker, [Online]. Available: https://www.docker.com/why-docker.

[36] Z. L. P. W. X. &. T. X. Liu, “Deep learning face attributes in the wild. In Proceedings of the IEEE International Conference on Computer Vision,” 2015, pp. 3730-3738.

[37] “colour FERET database,” 2016. [Online]. Available: https://www.nist.gov/sites/default/files/documents/2016/12/15/feret3.pdf.

[38] R. T. R. &. V. G. L. Rothe, “Deep expectation of apparent age from a single image. In Proceedings of the IEEE International Conference on Computer Vision Workshops,” 2015, pp. 10-15.

[39] E. F. J. V.-R. R. &. A.-F. F. Gonzalez-Sosa, “Facial Soft Biometrics for Recognition in the Wild: Recent Works, Annotation, and COTS Evaluation. IEEE Transactions on Information Forensics and Security, 13(8)”.

[40] E. E. R. &. H. T. Eidinger, “Age and gender estimation of unfiltered faces. IEEE Trans. on Information Forensics and Security, 9(12),,” 2014, pp. 2170-2179.