E-CORRIDOR
Edge Enabled Privacy & Security Platform For Multi Modal Transport

D8.2

Advanced Security Services Requirements and Architecture

WP8 – Advanced Security Services

E-CORRIDOR
Edge enabled Privacy and Security Platform for Multi Modal Transport

Due date of deliverable: 31/05/2022
Actual submission date: 07/06/2022

07/06/2022
Version 1.5

Responsible partner: CEA
Editor: Jean-Paul Bultel
E-mail address: jean-paul.bultel@cea.fr

Project co-funded by the European Union within the Horizon 2020 Framework Programme		
Dissemination Level		
PU	Public	**X**
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

The E-Corridor Project is supported by funding under the Horizon 2020 Framework Program of the European Union DS-2018-2019-2020, GA #883135

Authors: Jean-Paul Bultel, Hoang-Gia Nguyen (CEA), Shane Daly, Stefano Sebastio, Piotr Sobonski (UTRC), Christian Plappert (FhG), Gianpiero Costantino (CNR).

Approved by: Thanh-Hai Nguyen (CEA), James O'Rourke (WIT), Thomas Walsh (WIT).

Revision History

Version	Date	Name	Partner	Sections Affected / Comments
0.1	11-Mar-2022	J.-P. Bultel	CEA	Table of Contents
0.2	21-Mar-2022	J.-P. Bultel	CEA	Introduction
0.3	19-Apr-2022	S. Daly, S. Sebastio	UTRC	Sec on T8.2
0.4	21-April-2022	C. Plappert	FHG	Sec on T8.5
0.5	25-Apr-2022	P. Sobonski, S. Sebastio	UTRC	Sec on T8.1
0.6	25-Apr-2022	J.-P. Bultel	CEA	Sec on T8.4
0.7	28-Apr-2022	G. Costantino	CNR	Sec on T8.3 (MPC-based component only)
0.8	05-May-2022	H.-G. Nguyen, J.-P. Bultel	CEA	Sec on T8.3 (FHE-based component and merge with CNR's contribution)
1.0	17-May-2022	J.-P. Bultel	CEA	Merge, executive summary, conclusion, and final update.
1.1	25-May-2022	J.-P.Bultel	CEA	Comments from internal review taken in account in all the document except §2, §3 and §6.
1.2	26-May-2022	S. Sebastio	UTRC	Comments from internal review taken in account in §2 and §3.
1.3	31-May-2022	C. Plappert	FHG	Comments from internal review taken in account in §6.
1.4	31-May-2022	J.-P. Bultel	CEA	Checking and merging.
1.5	07-June-2022	J.-P. Bultel	CEA	Final checking and taking in account remarks from the lead of the project.

Executive Summary

This document, along with the available software components, constitutes the second deliverable of Work Package 8 “Advanced Security Services”. After having fixed the corresponding requirements and architecture in D8.1, this document (due to M24) reports on the first maturation cycle of all the advanced security services available in the E-CORRIDOR framework at the moment it is written. More precisely, this document contains information about the status of the development of each component involved in these services, including its maturation and its integration in the ASI infrastructure and in the global E-CORRIDOR framework.

This first maturation of the ASI is due to an effort from different partners to implement components that provide distinct services. A global effort has also started to integrate them in the ASI, and more generally in the E-CORRIDOR infrastructure. This collective work has been realized thanks to regular intra-workpackage and inter-workpackages one-to-one meetings.

For each of these ASI services (each of them associated with a specific task of WP8), we give here a description of the components implemented to provide it, together with the workflow exchanged when they run in the E-CORRIDOR framework and pilots’ contexts, that is, the interaction between them, other E-CORRIDOR components, and the outside.

We also give the current status of maturation and integration of these components, matrices of compliance with the requirements given in D8.1 (with solutions to fulfil each of them), and work plans per component for final maturation and testing, the main goal of this document being to give the global status for this first maturation step.

Table of contents

1 Advanced Security Services

E-CORRIDOR Framework leverages the concept of Advanced Security Infrastructure (ASI) to evaluate privacy-aware authorization and authentication mechanisms. ASI is responsible for managing security mechanisms to determine access levels or Prosumer privileges related to system resources including customer profiles, transport services, data and application features. This is the process of granting or denying access to a network resource that allows the Prosumers access to various resources based on identity features.

Figure 1 (imported from WP5 deliverables) recalls the general E-CORRIDOR architecture. It shows how the ASI component interacts with other components in the generic framework.

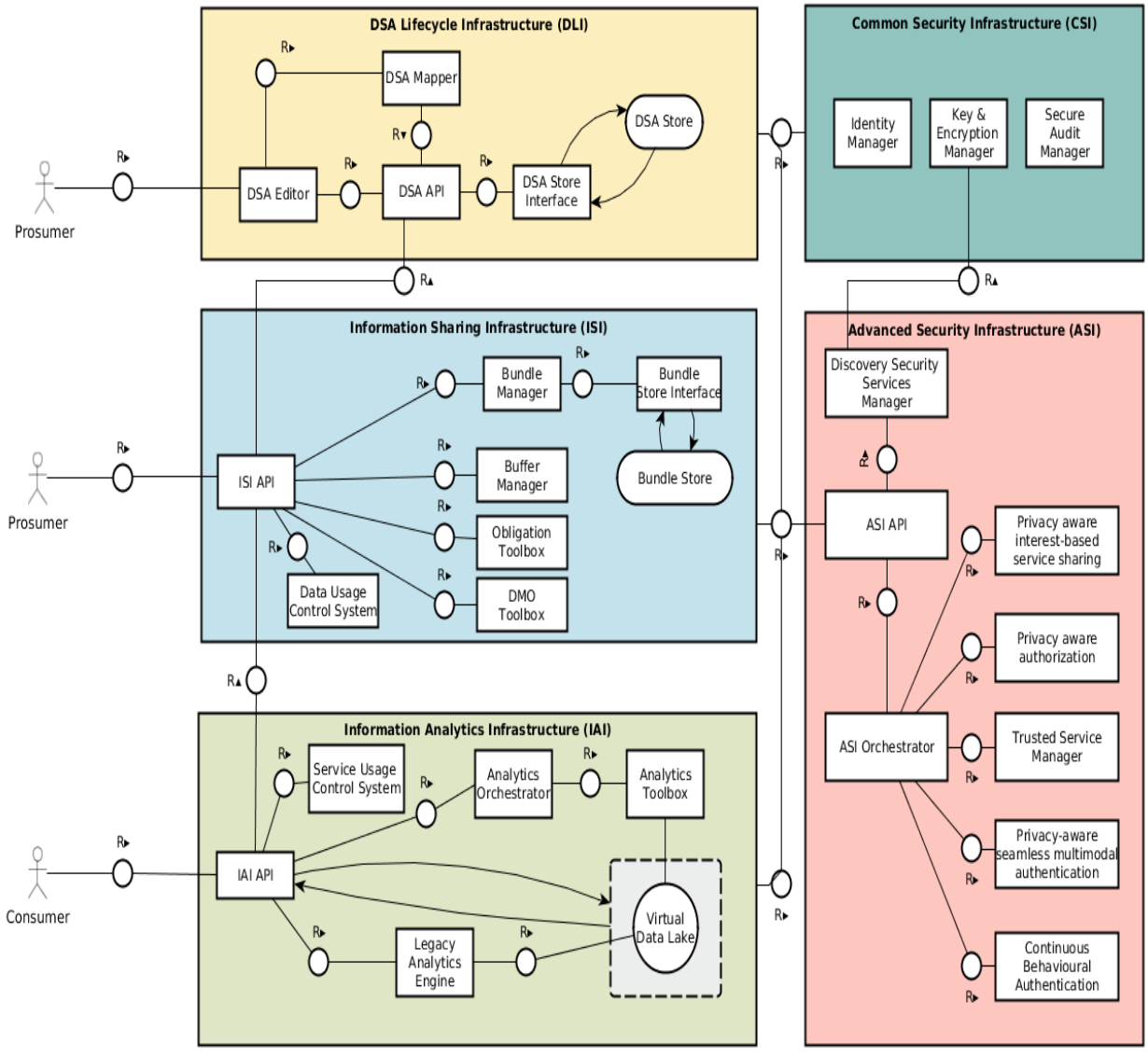

Figure 1: E-CORRIDOR architecture overview.

1.1 Advanced Security Services Architecture Overview

Figure 2 recalls the internal architecture of the ASI, including its different sub-components and the interactions between them.

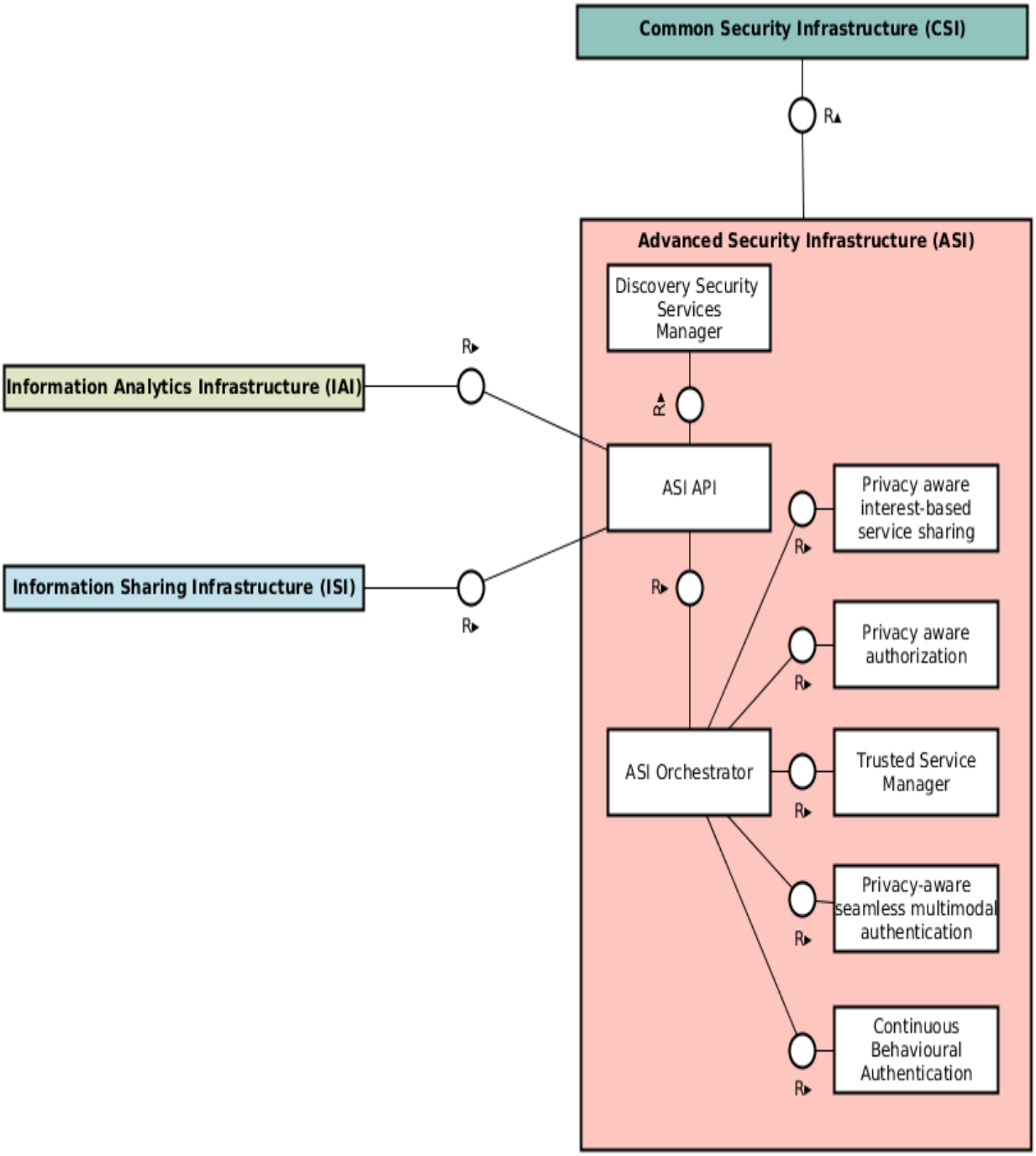

Figure 2: Security infrastructure architecture overview.

The main structural sub-components of the ASI are the following:

Discovery Security Service Manager: This component proposes a discovery service, which is responsible for detecting the status of a security service (on or off).

ASI API: This component is an exposed OpenAPI that allows other Infrastructure or components in E-CORRIDOR Framework to invoke.

ASI Orchestrator: This component receives from the discovery service manager the information about RESTfull connection endpoint. This information facilitates it to interact with available security services hosted in ASI.

Each of the five other main components depicted in Figure 2 is devoted to a specific service associated to a task. Each of them is implemented by the partners involved in its associated task. These task components are the following:

Privacy aware seamless multimodal authentication (T8.1 led by UTRC):

This component provides protocols necessary to execute a privacy aware seamless multimodal authentication (MFA) scheme. This scheme is designed to work in the multimodal transport pilot's framework by applying adaptive device and user context. Various authentication ways are leveraged to build this MFA system, such as hardware tokens, passwords, biometric data and behavioral data. From a multi-modal transport perspective, dynamic access policies associated to transport use-cases are identified, based on user-centric attributes like (e)-passport (for airport context), driving license validity (for car-sharing context), role, location, or device information. When a risky behavior is detected, these policies can be automatically enforced with step-up authorization or access denial.

In the airport pilot's use-case, the context-aware MFA mechanism provides the security and the privacy preserving of the passenger's personal data while facilitating the seamless flow of his/her journey with the help of Single Token technologies.

Concerning the cryptographic technical aspects, this component uses recent cryptographic technologies for blind computation, which are multi-party computation (MPC) and fully homomorphic encryption (FHE).

Continuous behavioral authentication (T8.2 led by UTRC):

This component provides a privacy-aware continuous behavioral authentication mechanism based on a behavioral profile, which is unique per transport entity. This profile is defined from various behavioral (spatio-temporal) fingerprints. These fingerprints include data collected from sensors for action recognition, voice and video analysis and the original ID type or information, by using technologies based on (deep) learning. The knowledge of the system is enforced over the time of the golden communication channel between transport entities.

The risk-based model is adaptive and allows a continuous authentication of a user based on a behavioral profile under different devices/ contexts.

Privacy aware interest-based service sharing (T8.3 led by CEA):

This component provides a privacy aware interest-based sharing framework, which allows users to share their data for a common interest with respect to security and privacy requirements.

These requirements are fully and clearly expressed in a Data Sharing agreement established between the stakeholders. This agreement is fully and transparently controllable in data exploitation and analysis. To meet the associated constraints, secure blinded computation services are used, based on fully homomorphic encryption and anonymization techniques.

In the context of cross-border pan-European multimodal transport, this component offers a high benefit not only for cyber threats detection and notification but also for eWallet Sharing, a privacy–aware passenger information checker.

Privacy aware authorization (T8.4 led by CEA):

This component provides a privacy-aware authorization service based on attribute-based encryption. This component has a layered modular structure, accommodating the various functional blocks and respecting privacy by design rules.

Each module should operate (in terms of intercommunication with others) in a well-defined manner, so to ensure proper isolation of each functional block. This component will identify the authorization information flows among national/regional transport systems, and local (city) transport services and on-site actors. It will also capture the required security and privacy requirements for the flows for the different partners.

Trusted Service Manager (T8.5 led by FhG):

This component provides a secure identity management mechanism for both eWallet sharing and continuous authentication token checking for both passenger and baggage. Actually, this mechanism provides an edged security layer for the whole E-CORRIDOR framework, usable for all other pilots across the whole project.

Main features of this component focus to the secure distribution of credentials to establish strong identities in participating entities. This includes the User identification with one's token authentication (e.g., smartphone or smartwatch), backend token issuers and the actual resources like vehicles in car sharing or baggage storage in airport scenarios.

1.2 Structure of the deliverable

Each chapter X from 2 to 6 is devoted to a component (the one associated to Task T8.(X-1)). Each of these component chapters X is organized as follows. Chapter X.1 is dedicated to the description of the component, its role and its architecture. Chapter X.2 is dedicated to the description of the workflow associated to the component, that is, how it interacts with other components in the E-CORRIDOR context. Chapter X.3 is dedicated to the current status of the development and the integration of the component. Chapter X.4 contains a discussion on the compliance of the component with the requirements. Finally, Chapter X.5 contains a work plan for testing and final maturation of the component.

After these component chapters, this deliverable contains a last chapter, which is dedicated to the conclusion (Chapter 7). The executive summary, this introductive chapter (Chapter 1) and the conclusion (Chapter 7) are written by the WP8 leader (CEA). Each component chapter (Chapters 2 to 6) is written by the task leader partner associated to the corresponding component.

2 Privacy Aware Seamless Multimodal Authentication – Task 8.1

To support a seamless multimodal authentication, this task aims at designing a multi-factor authentication (MFA) able to exploit a set of biometric-based authentication mechanisms along with contextual (such as location) and behavioral (such as activity recognition) information. To ensure the users privacy a token-based solution is adopted. Each source of information exposes only the minimum set of information required for the access control and a proof of the performed authentication.

To achieve such a goal two main sub-components are required: an engine able to manage the authentication analytics and a reasoner to process the tokens to validate the quality of the multi-factor authentication in accordance with the policy specified by the transportation entities in each step involved in a passenger's journey.

2.1 Component description

The approach adopted by the PASMA (Privacy Aware Seamless Multimodal Authentication) component foresees the exploitation of the authentication mechanisms available in the *analytics toolbox* of the Information Analytics Infrastructure (IAI) subsystem to build an advanced security service in the ASI. A wide set of identification and authentication analytics has been designed through a variety of Machine Learning (ML)/Artificial Intelligence (AI) techniques aided by biometric-based sensors (from the ones available in the smartphone to the ones installed on cars or self-service kiosks). This approach allows a flexible definition of the (biometric) factors that will be involved in the MFA according to the preferences of users and transportation service providers. Different use cases may cover different scenarios and be easily accommodated by the PASMA component. For instance, some passengers would like to fully manage their authentication process through BYOD (Bring Your Own Device) technologies whereas other passengers may feel comfortable in using biometrics for authentication but do not want to use their devices (or simply their smartphones do not meet the minimum technical requirements).

From an architectural standpoint the PASMA component is constituted by the following modules:

- **Engine**: from the desired combination of MFA, it is in charge of managing and orchestrating the authentication analytics based on passwords, single biometrics or other legacy authentication mechanisms. The engine interacts through a REST API with the requested authentication analytics available in the E-CORRIDOR framework to run the subcomponents and to forward the partial results to the Reasoner.
- **Reasoner**: It exploits the expressive capacity of logic-based theories and the efficiency of answer set programming. The module takes in input the authentication-tokens generated by the analytics part of the MFA and performs runtime stream reasoning to infer the quality of the performed authentication. To that end the reasoner includes also the timestamp of the event, as well as spatial and temporal relations describing the used authentication touchpoints. Moreover, additional context attributes such as status of the environment (e.g., number of people in the sensor area, luminosity level) and of the user (e.g., use of wheelchair, number of baggage) can be included.

– **Authentication analytics**: are the building blocks of the MFA. Authentication analytics available in the IAI toolbox exploit a mix of behavioral, location and contextual information. Examples of these include gait analysis, facial recognition, activity recognition, and driver characterization. The PASMA component manages and orchestrates the execution of such authentication analytics according to the workflow specified in the MFA.

A high-level design of the architecture of the PASMA component is represented in Figure 3. The authentication analytics constituting the central layer are selected and their composition is specified on a case-by-case basis according to the requirements of the MFA (i.e., the scenario specified by the pilot). Instead, engine and reasoner modules are functionally the same in each scenario, requiring only a simple customization through a configuration script.

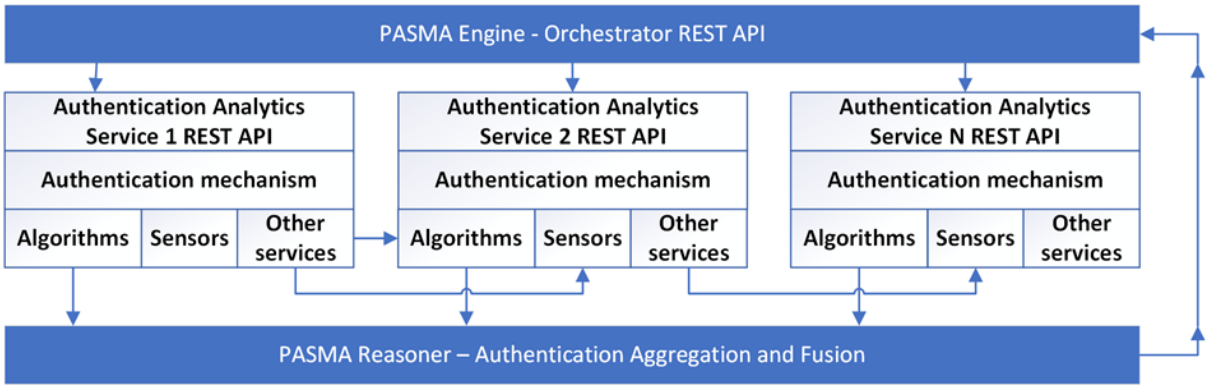

Figure 3: Privacy aware seamless multimodal authentication (PASMA) component: high-level design and example of authentication based on three factors.

The reasoning engine is based on the Event Calculus (EC) formalism to handle concurrent, indirect, and context-dependent events, as well as non-deterministic effects as such events. To this end, it can carry out temporal projection and abductive reasoning so that a track of contextual events and their effects can be inferred. Events and their effects are considered to update in an incremental way the authentication context of passenger, evaluate the tokens and enforce the decision. The inference rules are specified in the EC formalism by using predicates defined in the OWL ontology language (OWL [https://www.w3.org/OWL/]).

2.2 Workflow description

The internal workflow of the PASMA module is presented in Figure 4. The first step foresees the identification of the desired MFA according to the requirements of the application scenario (e.g., the MFA can be realized through a facial recognition at a kiosk or via mobile and a subsequent gait-based authentication while the passenger walks in a smart tunnel). Then, the workflow corresponding to the MFA is executed by sending a series of requests to basic authentication analytics (steps 2 and 3.x). In step 4, attributes from each of the single factor authentication information are aggregated by the reasoner that provides in output a decision concerning the quality of the performed process (e.g., if the facial recognition was performed in an environment with low luminosity the confidence on the overall authentication process may be affected). If the result of MFA process matches the desired quality, the authentication token is generated (step 5).

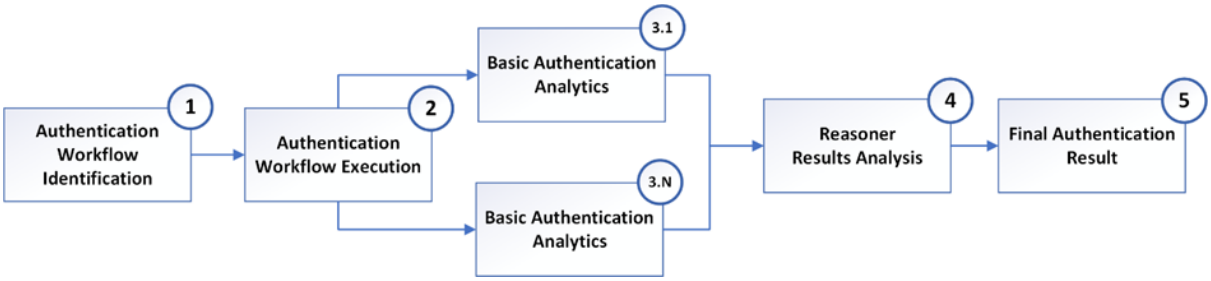

Figure 4: A high-level overview of the sequential steps performed by the PASMA.

Internally, each authentication service exploited by the PASMA component executes a four steps process, as reported in Figure 5. First, a *ground truth* is generated. According to the considered authentication it can be generated by requesting the user to issue an identity document or more generally to perform an enrollment process. Then, when there is a need for authenticating the user, appropriate sensors collect data and extract relevant features (steps 2 and 3). Finally, a ML/AI-based classifier is in charge of classifying the collected information and providing a response on the authentication process.

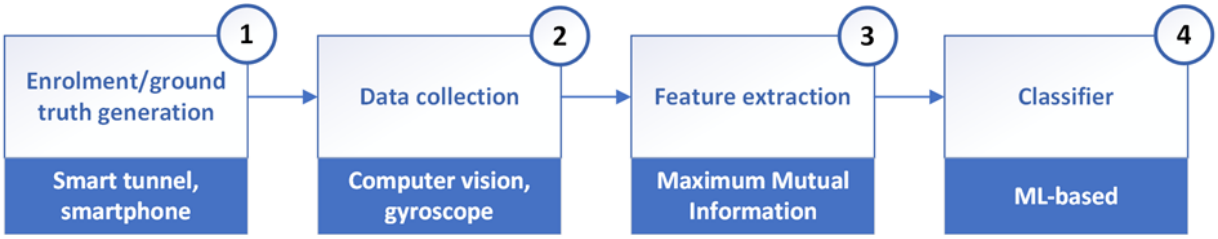

Figure 5: General workflow for the authentication analytics exploited by the PASMA component.

2.3 Current status

At the time of writing this deliverable, the PASMA component is still being finalized. The current version of the engine is containerized and exposes a REST API to interact with the ASI subsystem. A set of initial tests with a sample set of the authentication analytics available in the IAI toolbox have been performed successfully.

Currently, ontology and inference rules are being defined for the reasoner considering the information that can be collected and provided in output by the analytics.

An example of the targeted MFA according to the scenarios expressed in the AT pilot is represented in Figure 6.

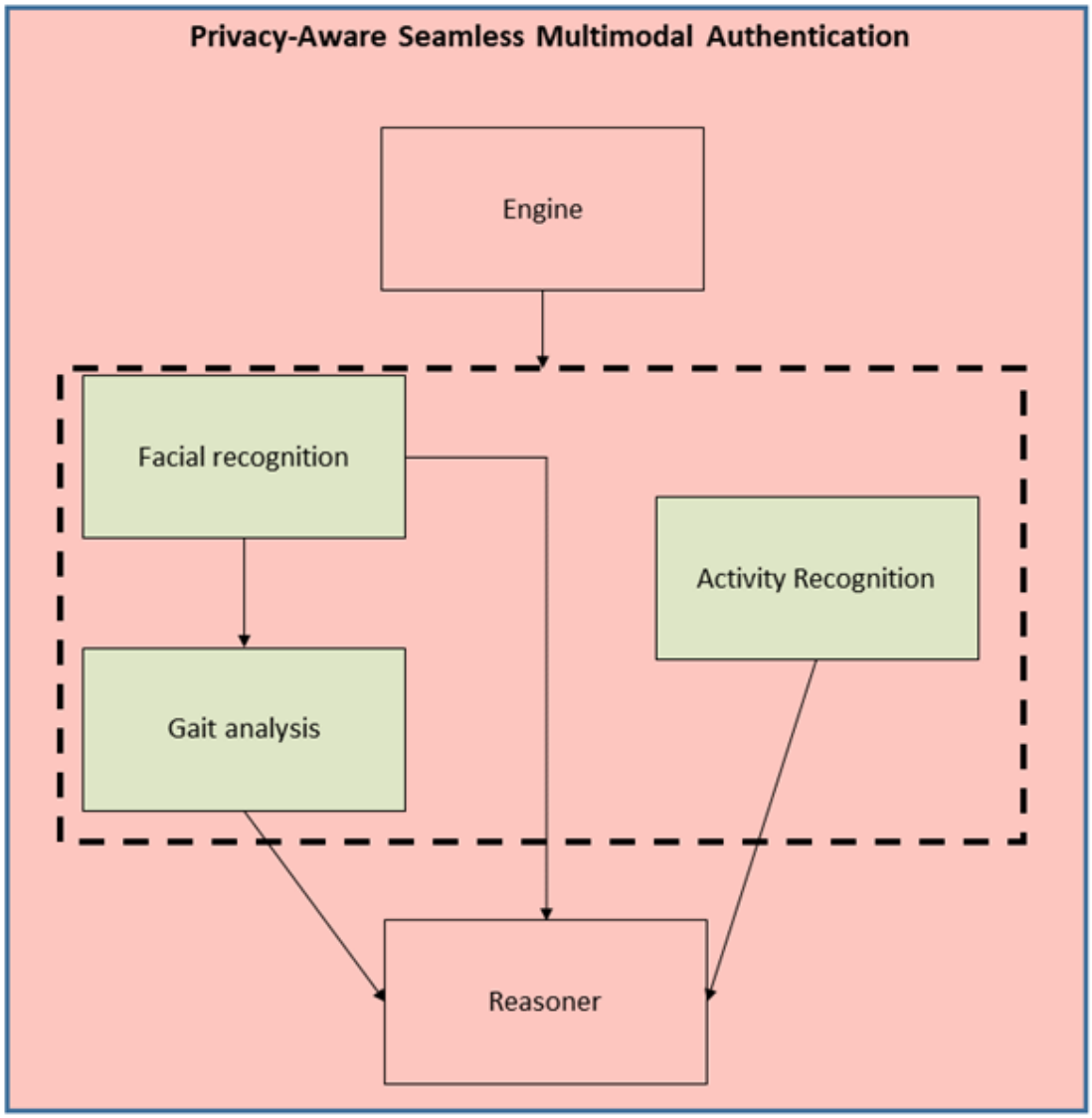

Figure 6: Example of the PASMA component instantiated for the scenarios expressed by the AT pilot.

2.4 Compliance with requirements

Table 1: Compliance with requirements for Task 8.1.

In order to fulfil Platform Requirement(s)	*Requirement*	*Priority*	*Solution*
E-CORRIDOR-DA-04 E-CORRIDOR-DA-05 E-CORRIDOR-DA-06	Authentication mechanisms exploit multiple sensors and share results (i.e., tokens) to increase quality and reliability of the process	MUST	The component leverages the process performed by single-factor authentication analytics and coordinate their execution through standard OpenAPI specifications.

E-CORRIDOR-Ope-04	Sensors and analytics expose input and output in a standard fashion (codified through API, template or guideline) to ease interoperability	MUST	All the analytics in the IAI toolbox expose a standard interface (the IAI API). The parameters exposed by the authentication token and processed by the reasoner of the PASMA component will be codified in a JSON format.
E-CORRIDOR-Per-02 E-CORRIDOR-Per-03	The identification process should be performed in a timely fashion to allow a frictionless user experience	SHOULD	To improve the user experience while using the MFA, the individual analytics are orchestrated by the PASMA in a series and parallel composition to avoid the introduction of any delay.

2.5 Work plan for testing and final maturation

Current efforts are oriented towards the following steps:

1. definition of a minimum set of common parameters provided in output by each authentication service (e.g., confidence level, timestamp)
2. finalizing the implementation of the OpenAPI to support the Service Discovery and Gateway of the ASI subsystem
3. OWL-based specification of the ontology used by the reasoner
4. definition of inference rules to perform the contextual reasoning
5. further refinement of the initial MFA scenarios defined in the pilots (and potential extension with new ones)
6. testing of the PASMA component along with other services offered in the pilots (i.e., the generated authentication token will allow the user to receive a service offered by the transportation service provider).

Tests will be performed considering the Airport-Train (AT) pilot environment. In the considered scenarios the transportation service provider can identify different set of MFA to accommodate security requirements and passenger preferences on the identity information used in the authentication process.

3 Continuous Behavioral Authentication – Task 8.2

Passenger's journeys are inherently multimodal. Moreover, within the same transportation multiple entities are in charge of verifying the passenger's identity at different steps. For example, by considering only the airport, there are several touchpoints (e.g., check-in, baggage drop, boarding gate) each requiring a new authentication. Avoiding to request the same identification and travel document multiple times is a factor that can contribute to improve the passenger experience. This task aims at exploiting the authentication token representing his/her behavioural fingerprint (built thanks to the analytics designed in WP7 and the multi-modal authentication of T8.1), to keep the passenger continuously authenticated with the transportation environment.

3.1 Component description

From the time the user (either passenger or driver) plans and reserves her/his multi-modal journey, to the time when she/he reaches destination, interactions with services offered by different providers are performed. This scenario underlines the need to re-authenticate the user with each of the involved stakeholders. By considering the passenger experience, continuous and automatic authentication is a better solution than re-authenticating the user at each step of her/his journey. Authentication tokens exchanged between security domains belonging to a federated environment can achieve that goal.

The designed solution is built around the EU eIDAS (electronic IDentification, Authentication and trust Services) framework enabling digital identities and electronic signatures with the same legal validity of paper documents used for the corresponding transactions in the "physical world". In the E-CORRIDOR scenario, it is used to support a pan-European identity management. Such a Federated Identity Management (FIdM) solution is based on standard protocols (such as SAML) and allows a verification of the passenger's identifiers against national registries.

By adopting an eIDAS compatible identity management, a few benefits are brought to both users and transportation operators (e.g., car sharing, train, airport):

- Interoperability and compatibility across borders: thanks to the legal, operational and semantic compatibility in the EU single market
- Error reduction in the user/passenger's files: as the self-declared identities are verified against government agencies these can be considered error free

To quantify the impact of such benefits e.g., in the airport business, it is estimated that incorrect data costs over € 650 million annually to the airlines, e.g., due to fines and repatriation costs [https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Studies+and+supporting+documents?preview=/84416364/116588829/eIDASeID_Aviation.pdf]. On the passenger's perspective if the records are correct and aligned with the different services accessed by the passenger, less time is required at the touchpoints for the identification.

From a technical perspective, the eIDAS framework adopts the SAML (Security Assertion Markup Language) standard to exchange authentication and authorization information between security domains. The exchanged security tokens (signed and encrypted) contain assertions with user's identifier, authentication status and attributes.

3.2 Workflow description

As in each FIdM model, three main logical entities are involved in the system: user, service provider (SP) and identity provider (IdP). The SPs are in charge of providing access to (either public or private) online services, whereas the IdPs store, manage and verify the identities. In the E-CORRIDOR scenario, the transportation entities mainly act as SP leveraging the trust services offered by the IdPs running in a different domain.

One scenario considered in the multi-modal travel foresees a user having a digital account with a transportation entity validated in a given country and willing to access to services perhaps (but not necessarily) located in a different member state. For instance, the passenger considered in the AT pilot (please see D2.2) may have an account with the airport authenticated with eIDAS and wants to use some services offered by the train entity on the second leg of her/his journey. By adopting a FIdM approach, there will be no need for the passenger to create a new account and will therefore experience a better service being continuously authenticated with the transportation infrastructure.

Figure 7 represents the workflow of our component. A user with credentials in a given domain tries to access to a service (requiring authentication) available in a new domain. Instead of requesting new credentials, the service reaches the home domain of the user (e.g., where the user was previously authenticated in the previous leg of her/his journey) by contacting the proxy service through the connector (steps 1 and 2). The identity provider of the user's home domain can then verify her/his identity and can later approve the request (steps 3 and 4). Finally, the user can access to the service thanks to the received authentication token.

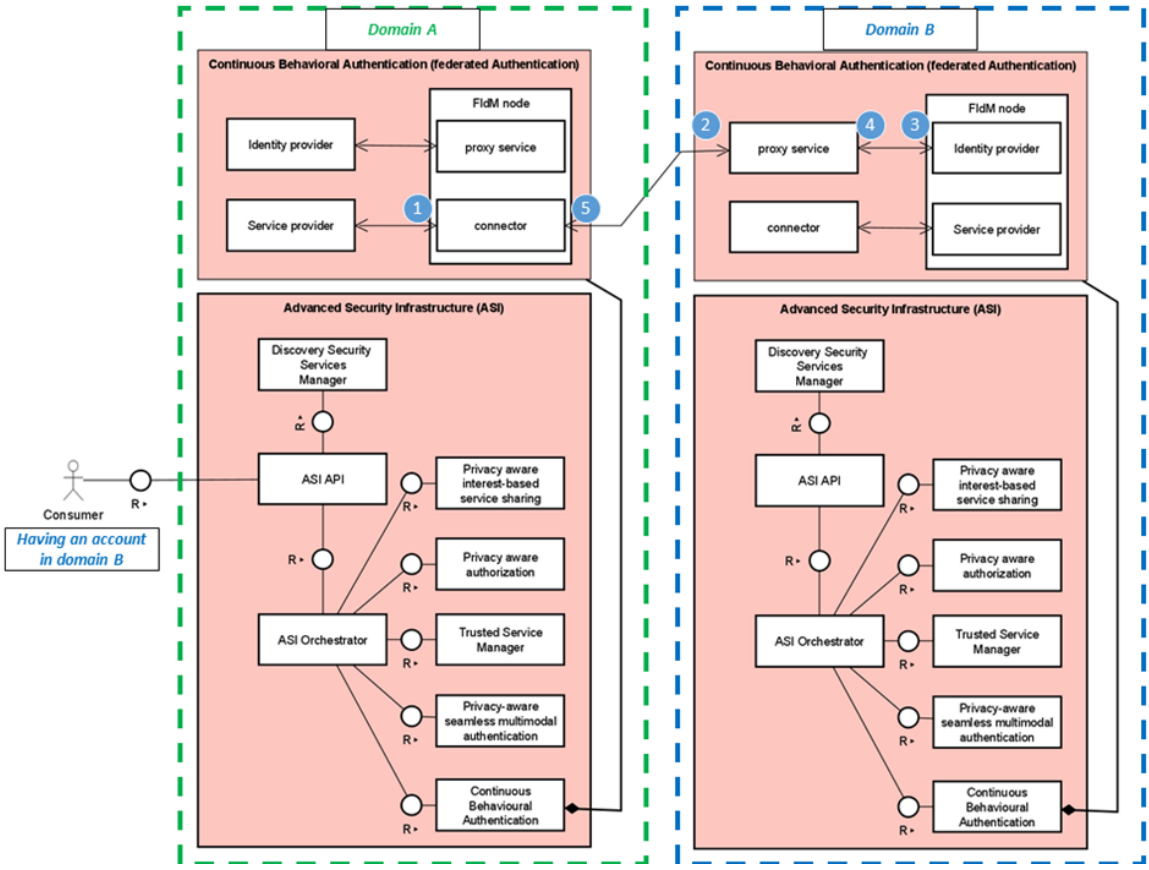

Figure 7: The workflow describing the authentication in domain A of a user coming from domain B.

3.3 Current status

Unfortunately, the current version of the eIDAS framework does not have native support to specific attributes required in the transportation sector (e.g., passport or visa) and for derived identity solutions (e.g., biometrics). In our component we are extending the reference integration package (pre-release version 2.6 [https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/eIDAS-Node+Integration+Package]) provided by the Connecting Europe Facility (CEF) to support the above-mentioned sector specific attributes.

Our initial effort has been devoted to the simulation of the most generic scenario consisting of two member states, and the user willing to access any service hosted in a country and domain different from her/his own. At the time of writing this deliverable, our continuous authentication service has been designed and the current implementation containerized and shared with the project consortium through the Nexus repository.

As the service already runs stand-alone, pilot partners can then start using this component to identify further scenarios in addition to the one mentioned above and currently under customization for the AT pilot. From the exposed OpenAPI the user can login once and remain connected with the infrastructure through the exchange of token-based messages.

3.4 Compliance with requirements

Tableau 2: Compliance with requirements for Task 8.2.

In order to fulfil Platform Requirement(s)	*Requirement*	*Priority*	*Solution*
E-CORRIDOR-Sec-IS-06 E-CORRIDOR Use-01	Stakeholders adopt standard protocols for authentication and authorization in their own security domains (OIDC, OAuth, SAML).	MUST	Sub-components adopt SAML for exchanging information on user's authentication status and attributes.
E-CORRIDOR Per-02	Multi-modal transportations belong to the same Circle of Trust (CoT) created through bi-lateral or peer-to-peer agreements.	MUST	The designed solution is based on the FIdM. Moreover, since our module is based on the eIDAS framework, the component potentially supports a wide range of compatibility with external services.
E-CORRIDOR-Sec-IS-06 E-CORRIDOR Use-01	The analytic-based user identification systems adopted by the stakeholder in their security domains need to expose models and information as SAML assertions.	MUST	We plan to exploit the token generated by the muli-modal and multi-factor authentication of task T8.1.

3.5 Work plan for testing and final maturation

Current effort is oriented at the integration of the service in the ASI subsystem, in particular to make the service reachable by the ASI gateway. Then, the identified transportation specific attributes will be included considering inputs collected in the pilots (and any additional one following the ongoing discussions). Moreover, the authentication token generated in T8.1 will be included in the workflow. Integration and test with demo environments of the services running in the transportation environment (e.g., reservation, check-in) will be used to validate the component in the AT pilot.

4 Privacy Aware Interest-Based Service Sharing – Task 8.3

Multimodal cross-border transport services use profile matching to help customers from a country find the right service located in another country with similar attributes (e.g., interest, location, background, etc.). However, privacy concerns often hinder customers from enabling this functionality. Some confidential customer data faces the risk of hacking, leaking or exposure of their personal information & location privacy. Based on this, we propose our Privacy Aware Interest-Based Service Sharing, which allows customers to match their interest with others without revealing their real interest and profiles, and vice versa. To limit the risk of privacy exposure, only minimum information about interest attributes of the users is extracted, with prevention of real profile attributes. It is secure and almost prevents from hacking profile of users.

For instance, suppose that a passenger has a connection flight, and she has some free time that she would like to spend going to a restaurant. In particular, the passenger wishes to know which are the available restaurants within the airport that match some criteria, such as the cost, waiting time to be served, type of menu and so on. However, the passenger does not want to provide her interest details to the service provider. Therefore, she can use the Interest-Based component to know the available restaurants.

4.1 Component description

To achieve its functionality, this component provides two distinct cryptographic services allowing manipulating data in a privacy-preserving way. The first one is based on fully homomorphic encryption (FHE). The other is based on two-party computation (2PC). Actually, the implementation of each of these two services can be seen as two distinct components.

4.1.1 Fully homomorphic encryption based sharing service

This subcomponent provides homomorphic encryption schemes. Fully Homomorphic encryption (FHE) is a recent cryptographic method that allows performing computations directly on encrypted data, without the need of decrypting it. As such, the encryption schemes possessing homomorphic properties can be very useful to construct privacy preserving protocols, in which the confidential data remains secured not only during the exchange and the storage but also for the processing. In the context of data outsourcing and cloud computing, homomorphic encryption is a mechanism that helps to protect data from intrusions from the cloud provider itself. The service provider (cloud) processes the received data homomorphically and sends the encrypted result to the end user, owner of the homomorphic secret key.

In real world cloud applications using FHE encryption, one or several entities interact with the cloud and top-reserve the privacy of each user; their data is sent encrypted over the cloud. The service provider processes the received data homomorphically and sends the encrypted result to an end user (owning the FHE parameters, and hence its secret key). The latter one decrypts the result using its own decryption key. Here, the service provider can compute almost any function over the encrypted data and acts transparently with respect to each entity using only public information and homomorphically encrypted data.

In order to address the practicality issues, we dispose nowadays of several tools and methods to bring to reality homomorphic-based cloud applications. There are several FHE schemes quite efficient (each one with its advantages and disadvantages) as well as several open-source libraries implementing it (e.g., SEAL[1], PALISADE[2] or TFHE[3]). Moreover, there exists a

theoretical framework (Chimera) allowing switching between these different cryptosystems in order to choose the most appropriate for various parts of the computation in the homomorphic domain. The CEA team has worked on the design, development and maintenance of the open-source Cingulata[4] compiler environment, the first operational tool of this kind. The integration of TFHE (standing for Fast Fully Homomorphic Encryption over the Torus and belonging to the 3rd generation of FHE schemes) into Cingulata compilation chain was realized in June 2019. As such, Cingulata offers the possibility to execute Boolean circuits either with BFV cryptosystem (and thus the execution is dependent of the multiplicative depth) or with TFHE (only *13mn* to perform a gate evaluation) techniques for the E-CORRIDOR project and an added – value of enhanced privacy – protecting framework. Developing and adopting Cloud – first deployment strategy, the secure sharing approaches based on homomorphic encryption help ensuring data confidentiality while allowing secure processing.

4.1.2 Two-party computation based data sharing service

To keep private the pieces of information of the parties involved in this component, the Interest-Based 2PC adopts the secure Two-Party Computation (2PC) technique. We recall that in a secure two-party computation, two parties exist (Alice and Bob), each holding some private data x and y, respectively. The goal of secure two-party function computation is allowing Alice and Bob to jointly compute the outcome of a function g(x, y), without disclosing to the other party the own input. The straightforward way to solve the above problem would be to have a TTP to which Alice and Bob securely send the data, and to have the TTP compute g(x, y) and separately send the out- come to Alice and Bob. The business in secure two-party computation amounts securely compute g(x, y) without the need of a TTP.

4.2 Workflow description

The following picture shows how FHE-based service sharing and 2PC-based service sharing are both provided to the E-CORRIDOR framework as a double task component of the ASI. It also gives a very high-level description of the internal architecture of both of these sub-components.

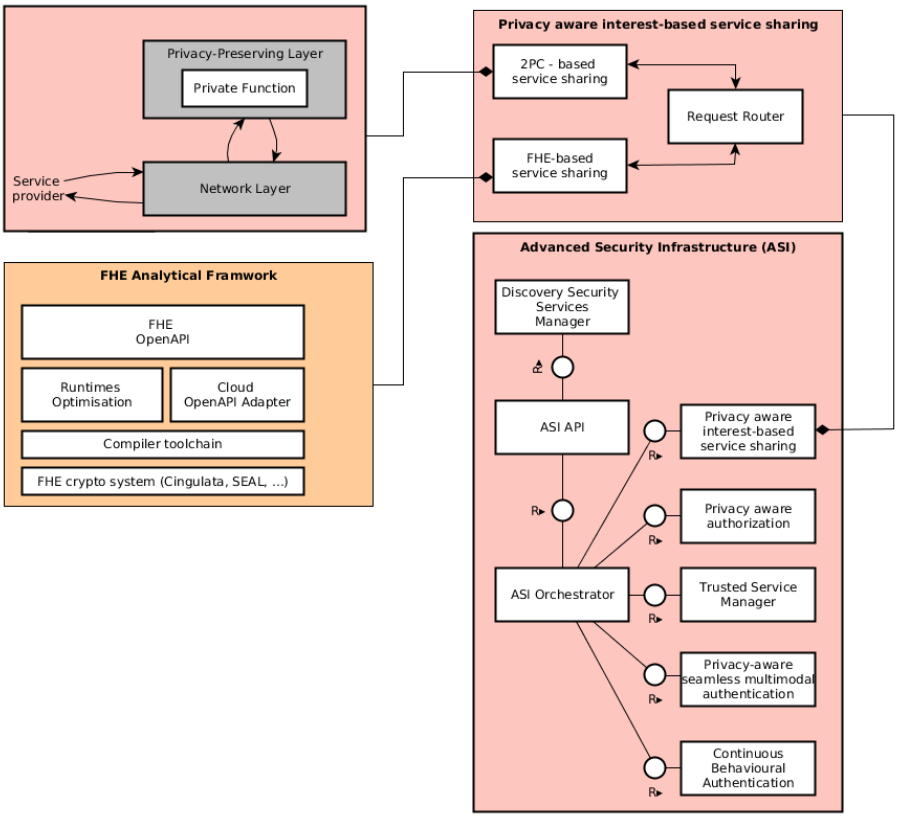

Figure 8: The technology components 2PC and FHE for privacy aware interest-based service sharing integrated in the ASI of the E-CORRIDOR framework.

4.2.1 Workflow for fully homomorphic encryption based data sharing service

In the E-CORRIDOR project, FHE technology will allow firstly to strengthen the security of data privacy and to respect privacy-aware data sharing in three pilots, secondly to guarantee trustworthy for eWallet use case of S2C pilot, finally to provide FHE-based validation service for providing a service of proving information in the pilot of Car Sharing in Smart City. The FHE-based validation services can be applied for the driver's license, e.g. a proof that the driving license has been validated by a mobility provider, a proof of address, mobility profile etc. other proof of information which are required by various transport providers and national regulations. To do so, the E-CORRIDOR framework provides the suitable environment to perform efficient computation over encrypted data: the distributed architecture for multi servers dedicated to FHE technology with load balancing features.

Figure 8 shows how the Privacy Aware Interest-based Service sharing component integrated into the E-CORRIDOR framework and in particular in its Advanced Security Infrastructure (ASI). The Request Router component allows redirect request to right FHE analysis – based service sharing. In the FHE – based service sharing feature, it composes a FHE analytics framework that is configured for FHE analysis cluster but it can be simplified for deployment in a simple server. This framework has 4 layers, the first layer is FHE cryptosystem like BFV, CKKS, TFHE, on top of this we have compiler toolchain like Cingulata, SEAL … Before applying for Cloud Open API, the 2 layers for runtimes optimization and API adapter play the important role for FHE adaptation.

In order to illustrate how FHE cryptosystem based data sharing service works in details, a simple interest matching example is briefly discussed. Initially, all keys are generated such as

public key, private key, etc. Given a set of interests, this set will be transformed into a table or a vector the same for each user's interest table, then the table will be transformed into a binary vector. The bottom line idea is subtracting 2 encrypted binary vectors under analysis. If the encrypted result vector contains a zero value then this interest is the same for both users. In practice, pattern searching uses several techniques to reduce the size of the output cipher-texts and improve performance.

Data type of the set of interests will depend on the type of function to be run on the analytic. The input data could be a string or integer number before transforming into binary vectors. For instance, given a set of interests (reading, running, swimming, tennis) and 2 users, one who likes reading and swimming has a binary vector [1;0;1;0] the other has a binary vector [1;1;1;1]. The result vector after running the algorithm is [0;-1;0;-1], this means both users has 50% the same interests.

4.2.2 Workflow for two-party computation based data sharing service

In this component, there are two main stakeholders involved:

- *A Service Provider*
- *A Prosumer*

The Prosumer aims to run a particular service offered by the Service Provider. When running a service both parties involved wish to keep their data private. In particular, the offered service will make use of the prosumers' interests.

A scenario that can be considered refers to the AT pilot where passengers involved in a multimodal transportation move from, for instance, a first part of the travel done by train to the second part, which involves a connection flight. The passenger has some free time to spend to go to a restaurant before the departure. When the passenger is approaching the airport, she will be able to use her smartphone to run an interest-based service that uses the 2PC technique to keep private the involved data. The service provider hosting at the airport side will allow the passenger to know all the restaurants that match the passengers' interests.

Table 3: Set of interests that a passenger can consider

Menu	It considers the type of restaurant, for instance American, Italian and others
Location	How far from the passenger position. For instance, restaurants in range of 200 meters
Cost	It expresses the type of restaurant in terms of costs. For instance, a fast-food or an expensive restaurant
Time to wait	It approximately indicates the maximum amount of time to wait until the passenger is served

Table 3 shows the list of interests that a passenger can set up before running the service. For each interest, a passenger can provide her degree of preferences and these on will be matched

in a private manner with the information available by the service provider.

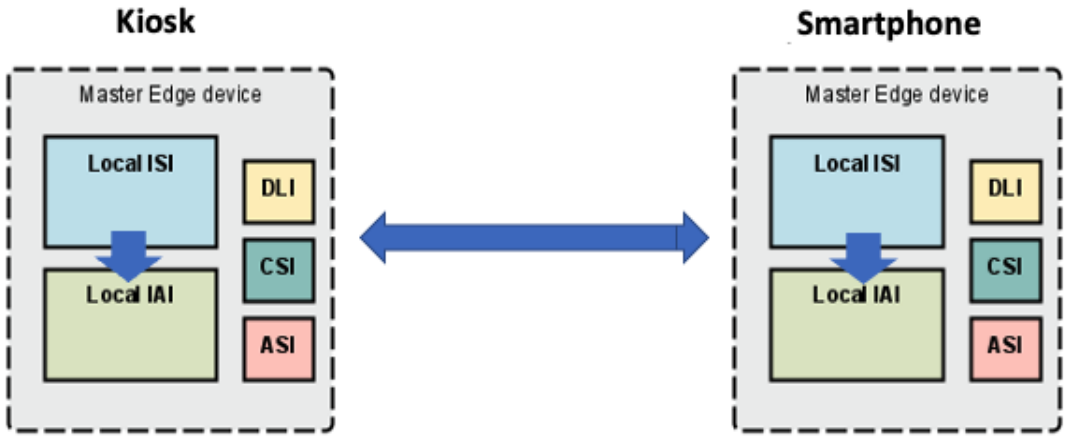

Figure 9: Interest-based 2PC service between a Kiosk and Smartphone.

In Figure 9, we show an interaction between a Kiosk, which resides at the airport side and acts as Service Provider party, and a passenger's smartphone. All data related to the passenger's interests and the available restaurants are first stored in the Local ISI. Then, when the analytic that involves the 2PC – based service sharing component is run, the 2PC technique is triggered, as it is available within the Advanced Security Infrastructure (ASI), see Figure 8.

4.3 Current status

At the moment when we write this document, three cryptographic algorithms have been implemented and tested for (respectively) fully homomorphic encryption, decryption, and evaluation for the FHE-based component. The implementation of APIs is in progress, in order to make these FHE services available for the integration in the ASI infrastructure.

The evolution of the 2PC component is seeing its implementation within the AT Pilot aiming at providing custom services to passengers depending on their interested. The corresponding analytic that uses this component is illustrated in T7.3 of the D7.2. Here, seen the strong interest of the pilot to this component, we are in the process of customizing the 2PC – based service sharing to provide services to passengers based on their interests.

The 2PC – based service sharing component is at the moment working as standalone component and its integration with the AT Pilot and the E-Corridor framework is in progress. The current implementation is written in JAVA and it is based on CBMC- GC [34].It is composed of two main parts: the compiler that translates functions written in "C" into garbled circuits, and the interpreter that is able to execute compiled functions [39]. Thus, CBMC-GC offers a very flexible high-level language that allows developers to express a wider range of functions compared to simpler techniques, which for instance only focuses on simple private matching operations.

To work with passengers' smartphones, we have extended and adapted CBMC- GC to work with Android OS. In Figure 10, we show the main window of the app for Android OS. Moreover, our version of CBMC- GC extended to work as 2PC – based service sharing is able to work on a scenario that foresees the usage of, for instance, two devices based on Android O.S., or in a hybrid case in which only a device with Android O.S. is involved plus the use of an Edge node or Cloud node that supports the JAVA virtual machine.

Figure 10: 2PC-based service main window.

4.4 Compliance with requirements

Table 4: Compliance with requirements for T8.3.

In order to fulfil Platform Requirement(s)	*Requirement*	*Priority*	*Solution*
E-CORRIDOR-DS-09	Prosumers may require running analytics expressing conditions to preserve confidentiality over the shared data.	MUST	The adoption of 2PC- based and FHE- based sharing services will allow prosumers to preserve confidentiality over the shared data.
E-CORRIDOR-DA-04 E-CORRIDOR-DA-05 E-CORRIDOR-DA-06	Sensor network data, user profile and results of the user data analytics are shared among multiple security areas and mode of transportations (stakeholders) to reduce shadow zones and increase the reliability of the authentication in the multi modal	MUST	Once user profile and user interest are both homomorphically encrypted by the FHE-based component, the intersection between them can be homomorphically evaluated. The result of this evaluation can be used in secure protocols to allow or

	environment.		not data sharing
E-CORRIDOR-DA-11 E-CORRIDOR-DM-04	Prosumers may require running analytics preserving the nature of their sensitive data against untrusted parties. In this case, 2PC or FHE technologies may be adopted.	SHOULD	The adoption of 2PC- based and FHE- based sharing services will allow prosumers to run analytics in a privacy-preserving way. This will be the case of the AT Pilot for instance
E-CORRIDOR-DM-03	Prosumers may require that some shared data, e.g., those ones that contain sensitive information, will be encrypted.	MUST	2PC- based and FHE- based sharing services will allow prosumers to encrypt sensitive data before running the analytic
E-CORRIDOR Ope-y02	Privacy aware Interest-Based analytics will be available at the edge of the E-CORRIDOR framework.	MUST	2PC- based and FHE- based sharing services will work on the EDGE exploiting its portable framework

4.5 Work plan for testing and final maturation

For now, the FHE cryptographic algorithms are implemented, current effort is therefore spent to implement and test the services layer (APIs).

Another effort is oriented to the improvement of the 2PC – based service sharing component and, in particular, to its development and customization for the AT pilot analytic. Moreover, we are working on the integration of the component as service in the ASI subsystem to make the service reachable by the ASI gateway.

In the next period, we are also going to integrate the FHE-based services into the ASI framework. Finally, these services will be dockerized and integrated into the E-Corridor framework.

Regarding the 2PC-based sharing component for the next period, we will progress on the maturation of the component to properly work as Android application with support of the CBMC-GC framework. In this way, this component will be able to work both at the producer side and at the edge of the E-corridor framework.

1https://github.com/microsoft/SEAL

2https://github.com/gchq/Palisade

3https://github.com/tfhe/tfhe

4https://github.com/CEA-LIST/Cingulata

5 Privacy Aware Authorization – Task 8.4

This component provides a privacy-aware authorization service based on ciphertext-policy attribute-based encryption (CP-ABE). A CP-ABE scheme permits to encrypt a message in a way that allows decryption only under some conditions on attributes of the user that pretends to decrypt. For example, one can suppose that a user can decrypt a message only if these attributes include ((‘CEA’ or ‘CNR’) and (‘Computer Science’)). This technique needs a trusted third part that extracts individual secret keys from both the attributes of their owners, and a master secret key.

We focus on the workflow of this component used to address a use-case from Air-Train pilot, which involves passenger’s attribute-based authorisations for transactions with transport companies. Depending on the value of user’s attributes such as pass boarding, location, or nationality, a passenger will be able or not to decrypt a token send by the company. This token will be necessary to start the transaction. We assume that these passenger’s attributes are extracted by the trusted authority from passenger’s documents, and distributed to all the companies.

5.1 Component description

This component implements a Ciphertext-Policy Attribute-Based Encryption (CP-ABE) scheme from Bethencourt, Sahai and Waters [47].

CP-ABE needs a trusted third part that extracts individual secret keys from the attributes of their owners. This extraction algorithm needs a master secret key owned by this third party. It is associated to a master public key, necessary to encrypt messages in addition with a Boolean combination of attributes. The Boolean combination of attributes is called a (attribute-based) policy. It can also be seen as a public encryption key.

Formally speaking, this component implements four algorithms **Setup**, **Extract**, **Encrypt** and **Decrypt** that provide the following services:

1) **Setup** takes no input. It sets up the necessary parameters and permits to construct a master secret key MSK and its associated master public key MPK;

2) From the master secret key MSK and a set S of attributes, **Extract** constructs an individual private key ASK;

3) **Encrypt** takes in input a message PT, the master public key MPK, a policy APK, and outputs a ciphertext CT.

4) **Decrypt** takes in input a ciphertext CT and an individual private key ASK, and outputs:

- a plaintext PT if S matches with APK, S being the set of attributes from which ASK has been extracted, and APK being the policy from which PT has been encrypted ;

- a notification of forbidden decryption if S does not match with APK (with the same definitions for S and APK).

Here, we say that an attribute set S matches with a policy APK if the boolean combination APK of attributes comes true when evaluated by replacing all attributes of S by 1 and all other attributes by 0. For example for S = (‘CEA’, ‘Mathematics’) and APK= ((‘CEA’ or

'CNR') and ('Computer Science')), S does not match with APK because ((1or 1) and (0)) is 0.

Formally speaking, the decryption of CT = **Encrypt**(PT, MPK, APK) with ASK = **Extract**(MSK, S) is allowed if and only if S matches with APK.

5.2 Workflow description

5.2.1. High-level description

In order to make this component running in the E-CORRIDOR framework, a protocol has been designed in the context of the use-case **AT-UC-07** of Air-Train Pilot.

This use-case concerns attribute-based authorization for a transaction between a passenger and a transport company, for example in a duty-free shop. Depending on the value of user's attributes such as pass boarding, location, or nationality, a passenger will be able or not to decrypt a token sent by the company. This token will be necessary to start the transaction. The mechanism of the following transaction is not in our concern and is then not a part of the protocol.

The stakeholders of this protocol are of three kinds : passengers, companies, and a trusted third part, named as the Certification Authority (CA), which is necessary in the context of using attribute-based encryption mechanisms (see §5.1).

We consider that these stakeholders have access to classical cryptographic algorithms provided by the CSI component of E-CORRIDOR. In particular, we assume that they have access to a public key infrastructure, allowing them to verify signatures from each other in a classical (not attribute-based) way.

This protocol can be decomposed into four parts:

(1) The CA runs the Setup;

(2) A company is added among the stakeholders;

(3) A passenger is added among the stakeholders;

(4) A passenger asks a company for a transaction, and is allowed or not to make it, depending on if he can or not decrypt a token sent by the company.

The algorithm (1) is run by the CA one time before anything else. Then, protocols (2), (3) and (4) are run when necessary.

5.2.2. A more detailed description

Now, let us detail each of these protocols.

(1) Setup: The CA runs **ABE.Setup** and gets a master secret key MSK and its associated master public key MPK.

(2) Adding a company: The CA signs MPK and sends it to a company. The company verifies the signature and keeps MPK.

(3) Adding a passenger: From MSK and the attributes of a passenger, the CA runs **ABE.Extract** to extract an individual secret key ASK for this passenger. From a signed key exchange, the CA and the passenger share then a (classical) secret symmetric key K. Then, the CA encrypts ASK with K, signs it and sends it to the passenger. Finally, the passenger verifies the signature, decrypts ASK, and keeps it.

(4) Authorizing a transaction: A passenger asks a company for a transaction. The company then runs **ABE.Encrypt** to encrypt a token with a policy APK depending of the kind of the requested transaction. The company signs this encrypted token and sends it to the passenger. The passenger verifies the signature and runs **ABE.Decrypt** to dcrypt the token. He can do it only if its attributes match with the policy APK. Else, he has no access to this token and the transaction cannot happen.

5.2.3. Key management

The following table summarizes information about all the keys needed by the different stakeholders to execute this protocol. The names of the keys in the first column are written in black for the keys to be instantiated and in blue for the keys with a unique instance.

Table 5: Addressing AT-UC-07 with ABE: key management.

key	Function	associated algorithm	Owner	generation	Sending
K	Encryption of ASK	Symmetric encryption	Each passenger has a different one. The CA has the one of each passenger.	Secret sharing between the passenger and the CA	Never send
PK	Verification of the signed data at reception	Signature	Each passenger has each company's one and the one of the CA, the companies have the CA's one, the CA have each passenger's one.	PKI	PKI
SK	Signature of data before sending	Signature	Each stakeholder (passenger, company, CA) has a different one	PKI	PKI
MPK	Encryption with access policy (combined with APK).	**ABE.Encrypt**	Only one MPK. Each company has it.	**ABE.Setup** run by the CA.	Signed by the CA, and then sent by the CA to the company.
MSK	Extraction of ASK from the	**ABE.Extract**	The CA. Only one MSK.	**ABE.Setup** run by the CA.	Never sent

	list of the attributes of a passenger.				
APK	Encryption with access policy (combined with MPK).	**ABE.Encrypt**	The company. One per access policy to consider.	The company	Never sent
ASK	Attribute-based decryption	**ABE.Decrypt**	Each passenger has his own ASK.	**ABE.Extract** run by the CA each time a new passenger is added.	Encrypted by the CA with K, then signed by the CA, then sent by the CA to the passenger.

5.2.4. Security considerations and discussion about why using ABE

We end up §4.2 by some remarks considering the security of this protocol and the justification of using ABE.

- *Remark 1: By opposition to a hypothetic non-attribute-based version, this protocol allows companies to give (or not) an access for a passenger to a transaction without knowing the identity of the passenger (the identities of the passengers being only known by the CA).*

- *Remark 2: Compared with a version that would use only a basic public key infrastructure instead of attribute-base encryption mechanisms, this protocol reduces the number of the keys that a company has to store. Indeed, there is no need for a key per passenger, but only one per access policy and the master key. An access policy can cover different kinds of transaction protocols, so that there is no need for many keys.*

- *Remark 3: This protocol is no resistant to collusions between different passengers. It needs a security model in which a passenger has neither interest to make a transaction for another, nor to allow another passenger to make a forbidden transaction.*

5.3 Current status

The development of the ABE services of this component is still in progress.

The integration of the component to the ASI and the E-CORRIDOR framework has not started yet.

5.4 Compliance with requirements

Table 6: Compliance with requirements for T8.4.

In order to fulfil Platform Requirement(s)	*Requirement*	*Priority*	*Solution*
E-CORRIDOR-DS-09	Prosumers may require running analytics expressing conditions to preserve confidentiality over the shared data.	MUST	The adoption of ABE-based services allows a fine access control, which can provide confidentiality on encrypted data under required conditions.
E-CORRIDOR-DA-04 E-CORRIDOR-DA-05 E-CORRIDOR-DA-06	Sensor network data, user profile and results of the user data analytics are shared among multiple security areas and mode of transportations (stakeholders) to reduce shadow zones and increase the reliability of the authentication in the multi modal environment.	MUST	Attribute-based encryption allows broadcasting encrypted data in a way such that only the authorized entities can decrypt it. That allows secure sharing among multiple areas and mode of transportations.
E-CORRIDOR-DA-11 E-CORRIDOR-DM-04	Prosumers may require running analytics preserving the nature of their sensitive data against untrusted parties. In this case, 2PC or FHE technologies may be adopted.	SHOULD	Whilst 2PC and FHE technologies allow computations directly on encrypted data, ABE-based services provide a fine access control. It allows users to encrypt data in a way such that only authorized servers can decrypt it before computation.
E-CORRIDOR-DM-03	Prosumers may require that some shared data, e.g., those ones that contain sensitive information, will be encrypted.	MUST	ABE-based service will allow prosumers to encrypt sensitive data.

E-CORRIDOR Ope-y02	Privacy aware Interest-Based analytics will be available at the edge of the E-CORRIDOR framework.	MUST	ABE- based service will work on the EDGE exploiting its portable framework.

5.5 Work plan for testing and final maturation

Current effort is spent to make the ABE services available. Once they will be, the component will be dockerized and turned into an OpenAPI Swagger project. Tests will be realized in stand-alone. Then, an effort will be made to integrate it in the ASI infrastructure. The component will be tested while running in the ASI once it will be able to run in it.

Regarding the implementation of the protocol described in §5.2 for having a demonstration of the component working in a practical context, one-to-one meetings with the lead of Air-Train pilot (WP2) will be organized from now, in order to identify the involved partners and their expected contributions. Once the component integrated in the associated workflow in action, final tests and demonstrative videos of the component running in a pilot context should follow.

6 Secure Identity Management / Trusted Service Manager – Task 8.5

Note: The component was previously called Trusted Identity Provider (TrIP) in D8.1. To easier distinguish this component from the Identity Manager of the Common Security Infrastructure that is used as an admin interface for the managing the Data Sharing Agreements (DSAs), it is renamed to Trusted Service Manager (TSM).

In this task a secure identity management system is developed. The system provides an edged security layer to the E-CORRIDOR framework. The layer can be used by all other pilots to achieve a comprehensive identity management solution across the whole project. The security is bootstrapped from hardware roots of trust that are provided by the underlying Trusted Service Manager (TSM). The main features of the TSM is the secure distribution of credentials to establish strong identities in the participating entities.
The TSM is instantiated for the eWallet use case S2C-US-01: Shared mobility eWallet (Log in) for the S2C pilot. In this use case, the overall goal is to simplify multimodal journeys by employing a SSO framework and data sharing through the eWallet. This allows travelers to store their personal data in one place and give service providers fine granular access to necessary authentication data without registering and authentication with multiple service providers.
For this, the TSM builds the basis for both an identity provider and a eWallet database server. In short, the identity provider issues authorization tokens to the mobility providers to access the traveller's eWallet.
The remainder of this chapter is dedicated to a detailed component and workflow description as well as a report about the current state and compliance with the E-Corridor requirements. The chapter is concluded with a work plan for testing and final maturation.

6.1 Component description

The system model for the instantiated TSM is shown in Figure 11. As introduced in D8.1, the TSM is part of the Advanced Security Infrastructure (ASI) of the E-Corridor framework. It advertises its API through the Discovery Security Service Manager of the ASI and is accessible via ASI orchestrator.

In its instantiated version for the eWallet use case, two independent TSMs instantiations are used to secure both an authentication as well as a eWallet database server. The authentication server is used to issue authorization tokens that can be used to access the eWallet.

Thus, the relevant entities for the instantiated eWallet use case are the S2C pilot mobility providers (E1), e.g., car sharing service of Clem or the bus on demand service by Nemi, and the two TSM-backed servers of the identity provider (E2) and the eWallet (E3). The interaction between the entities is as follows. Mobility providers and travellers register with the identity provider (1). For the travellers, the identity provider will securely transmit the user data to the eWallet server where the data is stored (2). After this initial registration step, the user can from now on log in from any participating mobility provider that will redirect to the identity provider.

We instantiated the TSM with a Trusted Platform Module (TPM) as root of trust since they are standard hardware on modern servers and widespread. Thus, they can be directly used without modifying the hardware. Our previous analysis (D8.1) has shown that they are feasible to be used for the intended use case and provide string security guarantees that fulfill the defined requirements.

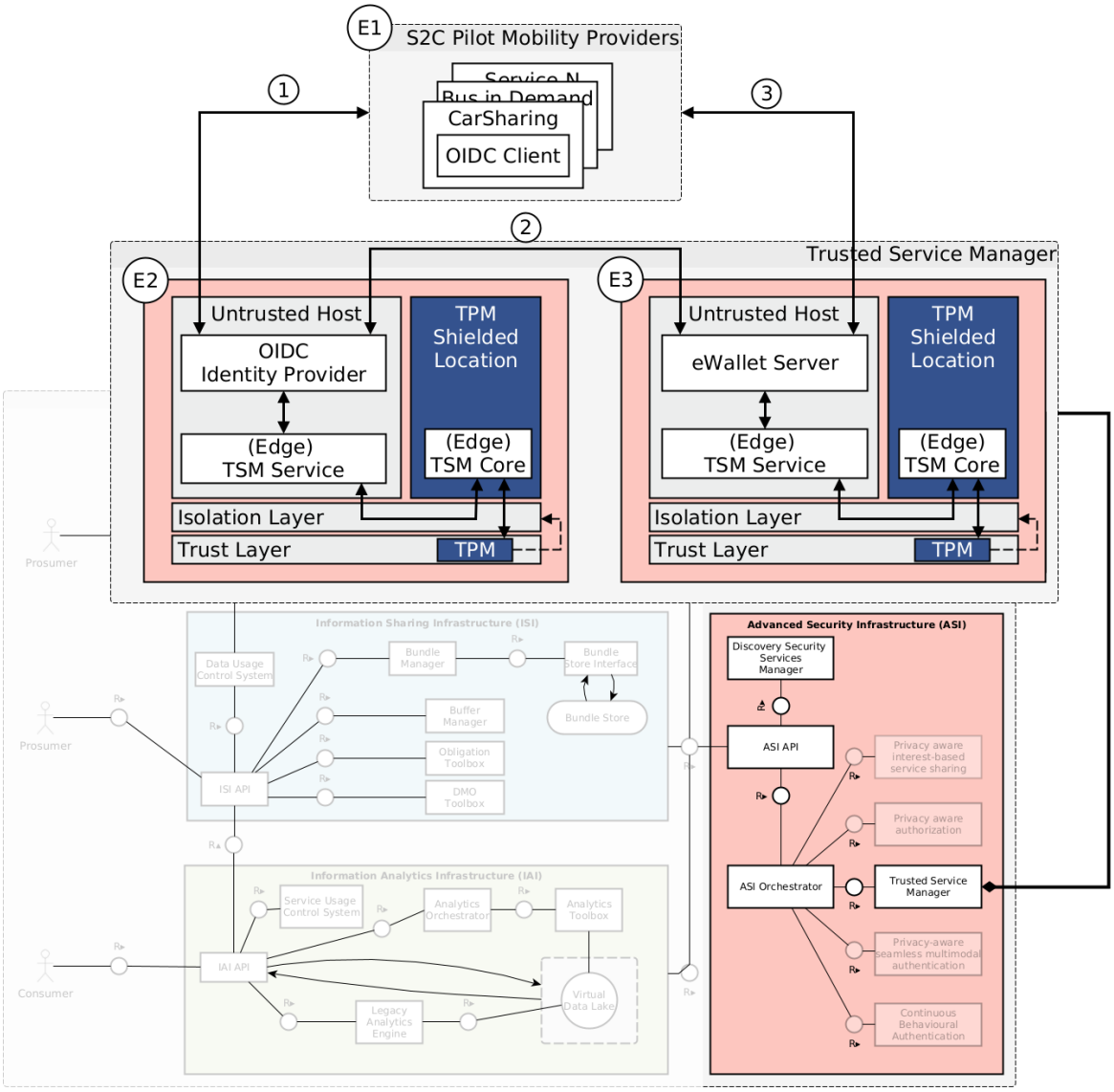

Figure 11: Instantiated Trusted Service Manager for the eWallet Use Case.

Moreover, for the selection of the high-level federated access and identity management solution, OpenID Connect (OIDC) was chosen since it best meets the requirements for SSO, fine granular access scope for the eWallet, and integration with the TPM as Hardware Root of Trust (RoT). Additionally, it was already used in the majority of the mobility providers of the S2C pilot so that minimal adaptations are necessary to implement the eWallet use case.

We made a standard-conform extension of the OIDC standard by using asymmetric cryptography to sign the access token and defining new authorization scopes that are aligned to the requirements of the eWallet use case. The corresponding security-sensitive private keys are securely stored within the shielded location of the TPM and by design cannot leave it. In addition, the security-critical signature generation and verification operations are completely handled within the TPM. Additionally, the necessary certificates are also securely stored in the shielded location of the TPM so that they cannot be exchanged by unauthorized entities.

The S2C pilot providers implement the OIDC client. Among other things, the OIDC client provides an interface to register their service as well as their customers with the OIDC server.

The customers can then use the OIDC interface as Single-Sign-On solution to the mobility providers and to access the eWallet.

The corresponding workflows are detailed in the following section.

6.2 Workflow description

The workflow can be subdivided into the four phases 1.) system provisioning, 2.) mobility provider and traveller registration, 3.) SSO, and 4.) eWallet interaction. The following sections and diagrams give a high-level introduction about the detailed workflow.

6.2.1 System Provisioning

Within the provisioning phase, the TSMs create and exchange their cryptographic identities (keys and certificates) with the help of the TPM. For this, first the unique provisioning certificates are read out from each TPM. With these secure end-to-end channels can be established with the TPMs. This is used to create the necessary application identity keys. These keys are created in such a way that they are bound to the respective TPM and the security-sensitive part of the key (private key) cannot leave the shielded location of the TPM. The correct creation of the keys (TPM bound keys) can be cryptographically verified with the TPM where the TPM can use its identity keys to certify the correct creation data of the keys with a signature. With the corresponding public keys, digital certificates are created and securely exchanged between the TSMs. The certificates are securely stored (write-protected) in the non-volatile memory of the other TPM. From now on, secured TPM-backed channels (e.g., TLS) can be established between the TSMs. The provisioning keys can be used later on to update the application keys if necessary.

6.2.2 Mobility Provider and Traveller Registration

During the registration phase, both the mobility provider and the traveller register with the OIDC identity provider. The mobility providers declare which data they will need from future travellers to use their services. Moreover, they retrieve the digital certificate of the identity provider so that they can later verify the issued tokens for the SSO procedure. The personal data of the travellers are securely sent to the eWallet server where they are stored in separate databases. For the secure channel the application identity keys are used to establish a TLS channel.

6.2.3 Single Sign On

After a user is registered with the identity provider, he can use SSO for registered mobility providers as follows. The user wants to access a service that a mobility provider offers, e.g., book a vehicle or a bus. If not logged in already, the user is redirected to the identity provider with the scope required to use the said service, e.g., a valid driving license to book a car. The user gives username and password and the mobility provider gets the authorization code from the identity provider. The mobility provider uses the authorization code to request the ID token. The identity provider creates the ID token with user ID (UID) and email and creates a corresponding signature with the TPM. Both IDToken and its signature are sent to the mobility provider. The mobility provider verifies the signature and uses the email and UID to log in the user.

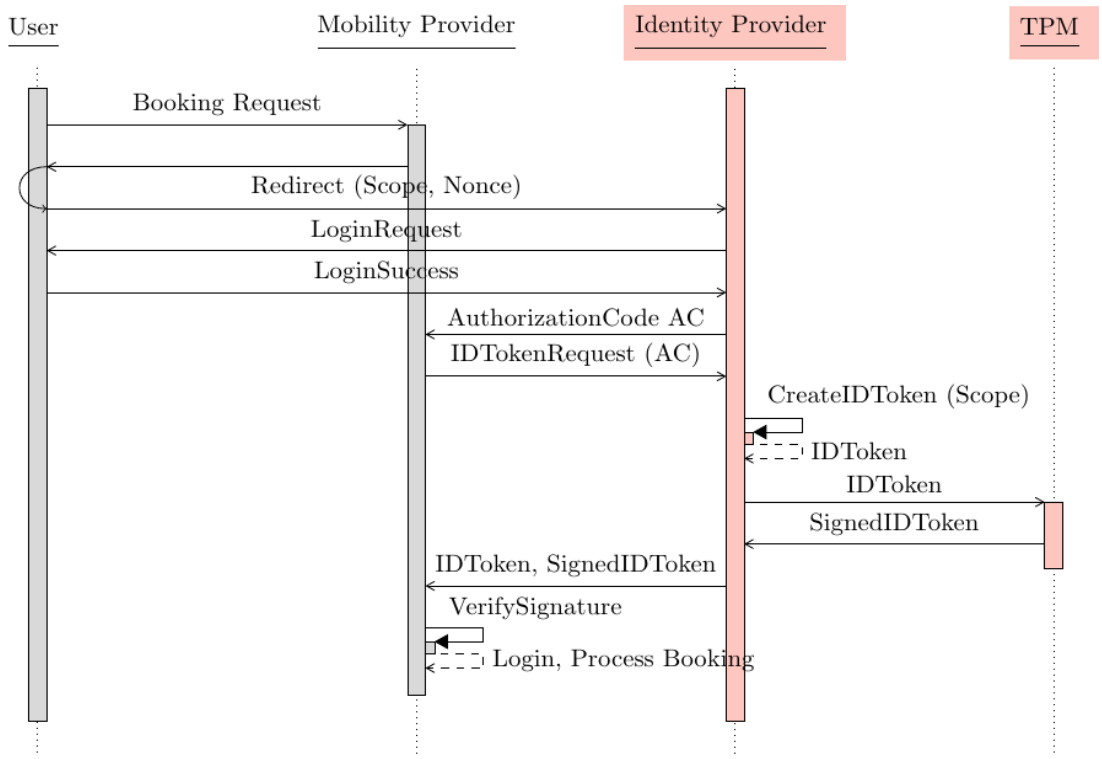

Figure 12: Enhanced OIDC Authorization Code Workflow for SSO.

6.2.4 eWallet Interaction

For interacting with the eWallet, the mobility provider can forward the ID token for authentication either to retrieve or on behalf the traveller update data in the eWallet.

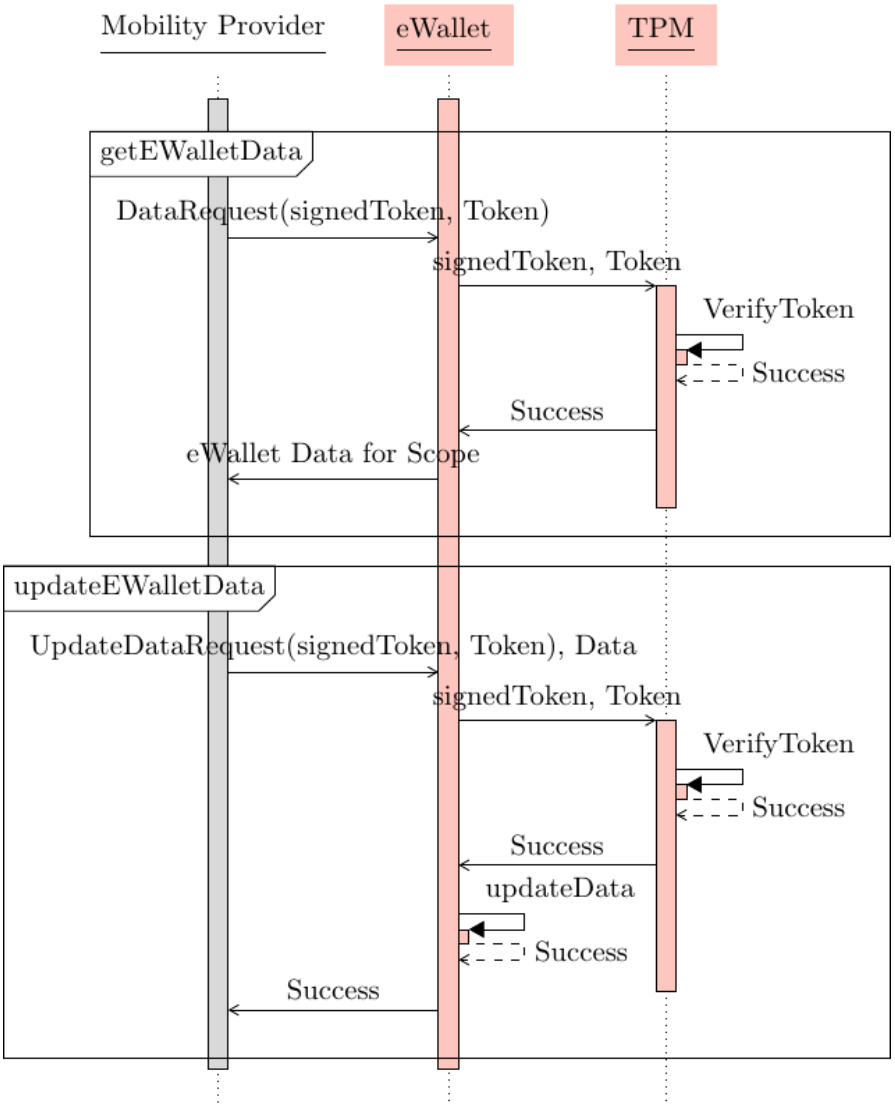

Figure 13: Enhanced OIDC Authorization Code Workflow for eWallet Access.

6.3 Current status

The basic functionality of the identity provider as well as the eWallet service is implemented. This includes already the standard-conform extension of the OIDC standard regarding the extended scopes as well as the change to asymmetric cryptography for signing the tokens. A standalone version with mocked clients is already running locally. The services are dockerized in containers.

Regarding the integration into the E-Corridor framework, the containers are uploaded to the E-Corridor CI. Current work is done to integrate the services into the ASI framework. In particular to advertise its API through the ASI Discovery Security Service Manager.

6.4 Compliance with requirements

Table 7: Compliance with requirements for T8.5.

In order to fulfil Platform Requirement(s)	*Requirement*	*Priority*	*Solution*
E-CORRIDOR-Sec-IS-02	E-CORRIDOR stores data encrypted at-rest to preserve confidentiality and privacy	COULD	TSM uses a hardware-based RoT, e.g., TPM2.0, to secure its identities. The secure identities could be used to derive additional keys that may be used for further use cases. Such a use case would be the instantiation of secure storage to store data encrypted at rest.
E-CORRIDOR-Sec-IS-03	E-CORRIDOR protects data in-transit (e.g., using TLS protocol) with encrypted channels to collect (e.g., upload) or deliver data (e.g., read), allowing to preserve confidentiality, privacy and authenticity.	COULD	TSM uses a hardware-based RoT, e.g., TPM2.0, to secure its identities. The secure identities could be used to derive additional keys that may be used for further use cases. Such a use case could be the establishment of secure channels to secure data in transit, e.g., by using TLS.
E-CORRIDOR-Sec-IS-04	E-CORRIDOR employs data integrity measure over the shared data.	COULD	TSM uses a hardware-based RoT, e.g., TPM2.0, to secure its identities. The secure identities could be used to derive additional keys that may be used for further use cases. Such a use case could be the integrity protection of shared data.
E-CORRIDOR-Sec-IS-05	E-CORRIDOR uses capabilities to evaluate the integrity of the running framework.	COULD	TSM uses a hardware-based RoT, e.g., TPM2.0, to secure its identities. The TPM2.0 has capabilities to

			store integrity data. It could be used to store integrity values of the framework.
E-CORRIDOR-Sec-IS-06	E-CORRIDOR provides its API functionalities after performing authentication and authorisation steps by using standard protocols (e.g., OpenID Connect, OAuth2).	COULD	TSM uses a hardware-based RoT, e.g., TPM2.0, to secure its identities. The secure identities could be used to derive additional keys that may be used for further use cases. Such a use case could be to secure tokens of standard authentication and authorization protocols (e.g., OpenID Connect, OAuth2)
E-CORRIDOR-Use-01	E-CORRIDOR uses standard authentication protocols (e.g. OpenID Connect, OAuth2, SAML, eIDAS).		
E-CORRIDOR-Use-02	E-CORRIDOR usage allow seamless authentication by leveraging Single-Sign On (SSO) authentication schemata.		

6.5 Work plan for testing and final maturation

Current effort is spent to integrate the service with the ASI framework. In particular, integration is done to make the service available by the ASI Discovery Security Service Manager. Currently, full TPM integration is only done locally but not yet dockerized or integrated with the E-Corridor framework. Moreover, current research is done to secure the eWallet database with the help of the TPM.

7 Conclusions

This document presented the status of the first maturation of the advanced security component, whose goal is to provide the advanced cryptographic services required to provide security and privacy of the E-CORRIDOR platform. The implementation of these services takes in account the requirements already established at M12 in D8.1. For each task, we specified the status of the associated components, the compliance with these requirements, and we gave a work plan for final maturation and testing.

The following table summarizes the status of all the services that ASI should provide:

Table 8: WP8 status per service.

Service	Task	Available in stand-alone	Integration in the ASI infrastructure	Pilot scenarios and workflow	Integration in a pilot context
Multimodal authentication	T8.1	Yes but to be finalized	Almost done	Yes	In progress
Contextual reasonner	T8.1	In progress	No	Yes	No
Continuous behavioural authentication	T8.2	Yes	In progress	Yes	In progress
FHE for interest-based service sharing	T8.3	Yes but to be finalized	Yes (FHE), in progress (interest-based sharing)	Yes	No
2PC for interest-based service sharing	T8.3	Yes	In progress	Yes	In progress
ABE for privacy aware authorization	T8.4	In progress	No	Yes	No
Secure identity management	T8.5	Yes	In progress	Yes	In progress

These services have various degrees of maturation. Most of them are (at least partially) already available in stand-alone versions, some of them are containerized, and some of them are available as OpenAPI projects in order to prepare their integration in the ASI infrastructure. A current effort is made to realize this integration through regular one-to-one meetings with the task leaders, as well as the integration of the ASI in the E-CORRIDOR framework through inter-workpackages meetings.

Discussions are also in progress with pilot workpackages' teams in order to customize these services and integrate them for use in pilot contexts. In addition to the finalization of the advanced cryptographic solutions, the next months will be devoted to their integration in the ASI E-CORRIDOR framework, and to validation and final maturation. Among other things, this goal will be intended by means of continuing the regular intra-workpackage and inter-workpackages regular meetings that we have already initiated for software integration.

8 Reference

[1] A. K. Jain, A. A. Ross et K. Nandakumar, Introduction to Biometrics, Boston, MA: Springer, 2011.

[2] M. Singh, R. Singh et A. Ross, «A comprehensive overview of biometric fusion,» *Information Fusion,* vol. 52, pp. 187-205, 2019.

[3] P. C. Cattin, D. Zlatnik et R. Borer, «Sensor fusion for a biometric system using gait,» chez *Conference Documentation International Conference on Multisensor Fusion and Integration for Intelligent Systems. MFI 2001 (Cat. No.01TH8590)*, 2001.

[4] R. Wang et D. Tao, «Context-Aware Implicit Authentication of Smartphone Users Based on Multi-Sensor Behavior,» *IEEE Access,* vol. 7, pp. 119654-119667, 2019.

[5] J. Mason, R. Dave, P. Chatterjee, I. Graham-Allen, A. Esterline et K. Roy, «An Investigation of Biometric Authentication in the Healthcare Environment,» *Array,* vol. 8, p. 100042, 2020.

[6] R. Mandeljc, S. Kovačič, M. Kristan et J. Perš, «Tracking by identification using computer vision and radio,» *Sensors (Basel),* vol. 13, pp. 241-273, 2012.

[7] Y. Li, B. Zou, S. Deng et G. Zhou, «Using Feature Fusion Strategies in Continuous Authentication on Smartphones,» *IEEE Internet Computing,* vol. 24, pp. 49-56, 2020.

[8] J. Yang, J.-y. Yang, D. Zhang et J.-f. Lu, «Feature fusion: parallel strategy vs. serial strategy,» *Pattern Recognition,* vol. 36, pp. 1369-1381, 2003.

[9] E. Maler et D. Reed, «The Venn of Identity: Options and Issues in Federated Identity Management,» *IEEE Security and Privacy,* vol. 6, pp. 16-23, 2008.

[10] M. Kang et A. Khashnobish, «A Peer-to-Peer Federated Authentication System,» chez *2009 Sixth International Conference on Information Technology: New Generations*, 2009.

[11] M. H. K. a. A. Khashnobish, «A Peer-to-Peer Federated Authentication System,» chez *Sixth International Conference on Information Technology: New Generations*, 2009.

[12] N. Naik et P. Jenkins, «Securing digital identities in the cloud by selecting an apposite Federated Identity Management from SAML, OAuth and OpenID Connect,» chez *2017 11th International Conference on Research Challenges in Information Science (RCIS)*, 2017.

[13] R. Shere, S. Srivastava et R. K. Pateriya, «A review of federated identity management of OpenStack cloud,» chez *2017 International Conference on Recent Innovations in Signal processing and Embedded Systems (RISE)*, 2017.

[14] S. Rieger, «Using Federated Identities to Access IP-Protected Web Resources in Multi-customer Environments,» chez *2010 Fifth International Conference on Internet and Web Applications and Services*, 2010.

[15] T. Komura, Y. Nagai, H. S., A. M. et K. Takahashi, «Proposal of Delegation Using Electronic Certificates on Single Sign-On System with SAML-Protocol,» chez *2009 Ninth Annual International Symposium on Applications and the Internet*, 2009.

[16] O. Boehm, J. Caumanns, M. Franke et P. O., «Federated Authentication and Authorization: A Case Study,» chez *2008 12th International IEEE Enterprise Distributed Object Computing Conference*, 2008.

[17] T. Reimer, P. Abraham et Q. Tan, «Federated Identity Access Broker Pattern for Cloud Computing,» chez *2013 16th International Conference on Network-Based Information Systems*, 2013.

[18] E. Samlinson et M. Usha, «User-centric trust based identity as a service for federated cloud environment,» chez *2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT)*, 2013.

[19] G. E., M. Zamani, J. Ab Manan et P. A., «A survey on security issues of federated identity in the cloud computing,» chez *4th IEEE International Conference on Cloud Computing Technology and Science Proceedings*, 2012.

[20] J. Köhler, S. Labitzke, M. Simon, M. Nussbaumer et H. Hartenstein, «FACIUS: An Easy-to-Deploy SAML-based Approach to Federate Non Web-Based Services,» chez *2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications*, 2012.

[21] G. Whitson, «Understanding OAuth: What Happens When You Log Into a Site with Google, Twitter or Facebook,» 24 05 2014. [En ligne]. Available: https://lifehacker.com/5918086/understanding-oauth-what-happens-when-you-log-into-a-site-with-google-twitter-or-facebook.

[22] A. Rasiwasia, *A Framework To Implement OpenID Connect Protocol For Federated Identity Management In Enterprises*, Luleå University of Technology, Department of Computer Science, Electrical and Space Engineering, 2017.

[23] W. Contributors, «eIDAS,» [En ligne]. Available: https://en.wikipedia.org/w/index.php?title=EIDAS&oldid=1006881918. [Accès le 12 04 2021].

[24] AGID - Agenzia per l'Italia Digitale, «The Italian eIDAS-Node,» [En ligne]. Available: https://www.eid.gov.it/nodo-eidas-italiano.

[25] G. Hillenius, «Denmark pre-selects suppliers for next-generation eID,» 2018. [En ligne]. Available: https://joinup.ec.europa.eu/collection/egovernment/news/eidas-ready.

[26] Federal Office for Information Security, «eIDAS Notification of the German eID,» [En ligne]. Available: https://www.bsi.bund.de/EN/Topics/ElectrIDDocuments/German-eID/eIDAS-notification/eIDAS_notification_node.html.

[27] E. Commission, «European Commission,» [En ligne]. Available: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eIDAS-Node+version+2.5?preview=/325353777/325353812/eIDAS-Node%20Installation%20and%20Configuration%20Guide%20v2.5.pdf.

[28] WSO2 Identity Server, «Electronic Identification, Authentication and Trust Services Regulation,» [En ligne]. Available: https://docs.wso2.com/display/IS570/Electronic+Identification%2C+Authentication+and+Trust+Services+Regulation. [Accès le 15 April 2020].

[29] N. N. B. P. a. Y. S. Dahlia Malkhi, "Fairplay - A Secure Two-Party Computation System," *13th Security Symposium Security 04,* 2004.

[30] N. N. B. P. a. Y. S. D. Malkhi, «The Fairplay project.,» *http://www.cs.huji.ac.il/labs/danss/Fairplay.*.

[31] N. N. B. P. Assaf Ben-David, «FairplayMP - A System for Secure Multi-Party Computation,» *ACM Computer and Communications Security Conference,* 2008.

[32] F. M. P. S. D. A. Gianpiero Costantino, «An implementation of secure two-party computation for smartphones with application to privacy-preserving interest-cast,» *Proceedings of the 18th annual international conference on Mobile computing and networking,* vol. https://doi.org/10.1145/2348543.2348607, p. 447–450, 2012.

[33] V. K. a. M. R. David Evans, A Pragmatic Introduction to Secure Multi-Party Computation,, NOW Publishers, 2018.

[34] «https://www.cprover.org/cbmc/,» CBMC Project.

[35] A. S. a. B. Waters, "Fuzzy Identity Based Encryption," *In Advances in Cryptology – Eurocrypt, Springer,* vol. 3494 of LNCS, p. 457–473, 2005.

[36] J. S. P. a. J. N. F. Myong H. Kang, "Access control mechanisms for inter-organizational workflow," *In SACMAT '01: Proceedings of the sixth ACM symposium on Access control models and technologies,* Vols. New York, NY, USA. ACM Press., p. 66–74, 2001.

[37] N. L. a. W. H. W. Jiangtao Li, "Automated trust negotiation using cryptographic credentials," *In ACM Conference on Computer and Communications Security,* p. 46–57, 2005.

[38] C. G. a. A. Silverberg, "Hierarchical id-based cryptography.," *In ASIACRYPT*, p. 548–566, 2002.

[39] S. A. a. P. Taylor., «Cryptographic Solution to a Multi Level Security Problem.,» *In Advances in Cryptology – CRYPTO,* 1982.

[40] e. a. N. Ragouzis, «Security Assertion Markup Language (SAML) V2.0 Technical Overview,» *Committee Draft 02,* n° %1http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html, 2008.

[41] e. a. N. Sakimura, «OpenID Connect Core 1.0 incorporating errata set 1,» n° %1https://openid.net/specs/openid-connect-core-1_0.html, 11/8/2014.

[42] Shibboleth consortium, «The Shibboleth Project,» n° %1 https://www.shibboleth.net/about-us/the-shibboleth-project/, 2021.

[43] e. a. A. Nadalin, «WS-Trust 1.4,» *OASIS Standard incorporating Approved Errata 01,* n° %1http://docs.oasis-open.org/ws-sx/ws-trust/v1.4/errata01/ws-trust-1.4-errata01-complete.html, 04/25/2012.

[44] C. K. a. M. McIntosh, «Web Services Federation Language,» *WS-Federation,* n° %1http://docs.oasis-open.org/wsfed/federation/v1.2/ws-federation.html, p. Version 1.2, 05/22/2009.

[45] S. S. a. J. A. M. Z. A. Khattak, «A study on threat model for federated identities in federated identity management system,» *International Symposium on Information Technology, Kuala Lumpur, Malaysia,* n° %1doi: 10.1109/ITSIM.2010.5561611., pp. 618-623, 2010 .

[46] D. Clegg et R. Barker, Case Method Fast-Track: A RAD Approach, Addiso-Wesley, 1994.

[47] Bethencourt, J., Sahai, A. and Waters, B. (2007) Ciphertext-Policy Attribute-Based Encryption. 2007 IEEE Symposium on Security and Privacy (SP'07), Oakland, CA, 20-23 May 2007, 321-334. https://doi.org/10.1109/SP.2007.11

A Appendix

A.1 Definitions and Abbreviations

Term	Meaning
ABE	Attribute-Based Encryption
AMB	Airport Managing Body
ASI	Advanced Security Infrastructure
AT	Air-Train
BFV	Barkerski-Fan-Verkauteren
BYOD	Bring Your Own Device
CA	Certification Authority
CBP	Customs and Border Protection
CEA	Commissariat à l'Energie Atomique et aux Energies Alternatives
CKKS	Cheon-Kim-Kim-Song
CoT	Circle of Trust
CP	Ciphertext Policy
CP-ABE	Ciphertext-Policy Attribute-Based Encryption
DSA	Data Sharing Agreement
EASA	European Aviation Safety Agency
ECCSA	European Centre for Cybersecurity in Aviation
ESTA	Electronic System for Travel Authorization – US
ETA	Electronic Travel Authorization – Australia and Canada
ETIAS	EU Travel Information and Authorization System
EU	European Union
eIDAS	Electronic Identification, Authentication and trust Services
eWallet	Digital wallet
FHE	Fully Homomorphic Encryption
FIM	Federated Identity Management
GDPR	EU General Data Protection Regulation
H&S	Hub and Spoke
IATA	International Air Transport Association
IdP	Identity Provider
IDS	Intrusion Detection System
IFE	In-Flight Entertainment

IIoT	Industrial Internet of Things
ISI	Information Sharing Infrastructure
M2M	Machine to Machine
MoSCoW	Must have, Should have, Could have, and Won't have but would like
NEXTT	New Experience Travel Technologies
NFR	Non Functional Requirement
OIDC	OpenID Connect
P2P	Peer-to-Peer
PKI	Public Key Infrastructure
PRM	People with Reduced Mobility
RFID	Radio-frequency identification
SAML	Security Assertion Markup Language
SIM	Secure Identity Management (System)
SSO	Single Sign-On
SSR	Special Service Request
TEE	Trusted Execution Environment
TFHE	Torus FHE (Fully Homomorphic Encryption over the Torus)
TPM	Trusted Platform Module
TSM	Trusted Service Manager
TTP	Time-Triggered Protocol
UML	Unified Modeling Language
US	United States of America
2PC	Two-Party Computation